Harmonizing People, Processes, and Technology for Robust Cybersecurity

D6.3 Cybersecurity Policy Toolkit v1

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D6.3 Cybersecurity Policy Toolkit v1		
Work Package	WP6 Title		
Contractual due date	31/12/2025	**Actual submission date**	18/12/2025
Type	R	**Dissemination Level**	PU
Lead Beneficiary	KETYAK		
Responsible Author	Research Team (KETYAK)		
Contributions from	IANUS, DSA, BYTE		

Funded by the European Union

ECCC

Funded by the European Union under Grant Agreement no. 101158555 and supported by the European Cybersecurity Competence Centre (ECCC). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	30.09.2025	Initial Deliverable structure	Research Team (KETYAK)
0.4	28.11.2025	Final draft ready for internal review	Research Team (KETYAK)
0.5	10.12.2025	Peer review	Evangelos Michos, Demetris Antoniou (IANUS)
0.6	11.12.2025	Peer review	George Achilleos (DSA)
0.7	11.12.2025	Final draft addressing comments from internal review	Research Team (KETYAK)
0.8	16.12.2025	Final quality check	Eleni Keliri (eBOS)
0.9	17.12.2025	Final draft addressing comments from Quality Check	Research Team (KETYAK)
1.0	18.12.2025	Final version ready for submission	Violeta Vasileva (MAG)

Disclaimer

The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

Contents

1 Executive Summary 7
2 Introduction 8
2.1 Mapping CYberSynchrony Outputs 8
2.2 Linkage to other project outputs 9
2.3 Deliverable Structure 10
3 Methodological Approach 11
3.1 Toolkit Design Principles 12
3.2 Guidelines for Use and Integration into Organizational Processes 15
3.3 Policy Update and Document Control Procedure 16
4 Security Policies and Standards 17
4.1 Tool 1 - Information Security Strategy 18
4.2 Tool 2 - Information Security Governance Policy 28
4.3 Tool 3 - Risk Management Policy & Methodology 37
4.4 Tool 4 - Asset Management Policy 62
4.5 Tool 5 - Supplier and Third-Party Management Policy (TPS) 69
4.6 Tool 6 - Access Control Policy 76
4.7 Tool 7 - Vulnerability and Patch Management Policy 92
4.8 Tool 8 - Network Security Policy 103
4.9 Tool 9 - Systems & Applications Security Policy 112
4.10 Tool 10 - Data Protection Policy 123
4.11 Tool 11 - Acceptable Use Policy 132
4.12 Tool 12 - Human Resources Security, Training & Awareness Policy 139
4.13 Tool 13 - Physical Security Policy 149
4.14 Tool 14 - Incident and Event Management Policy 158
4.15 Tool 15 - Business Continuity and Disaster Recovery Policy 167
5 Supporting Tools and Templates 177
5.1 Document Completion Guide 177
5.2 Measure Effectiveness Evaluation Procedure 177
5.3 Statement of Applicability (SoA) 177
5.4 Asset-Based Risk Assessment Workbook 177
5.5 Impact Assessment Templates (BIA, Impact Assessments) 177
5.6 Checklists and Compliance Mappings 178
6 Implementation and Monitoring 179
6.1 Compliance and Control Mechanisms 179
6.2 Performance Indicators and Effectiveness Measurement (KPIs, Metrics) 179
6.3 Control and Audit Procedures 179
7 Conclusions 180
8 References 181
Annex I: Summary (from Grant Agreement) 182
Annex II: Consortium Members 183

© CYberSynchorny, 2024

List of Figures

Figure 1 EU Legislative Landscape 14
Figure 2 Organizational Chart 30
Figure 3 Risk Scoring Criteria 48
Figure 4 Process Flow Diagram 53

List of Tables

Table 1 Adherence to CYberSynchrony's GA 9
Table 2 Links to other Project Outputs/Work 10
Table 3 Cybersecurity Incident Management Framework 11
Table 4: Policy Tools to NIS2 requirements mapping 13
Table 5 Implementation 25
Table 6 Information Processing Owners / System Access Owners 33
Table 7 Compliance with Legal and Regulatory Obligations 35
Table 8 Definition of Roles and Responsibilities 44
Table 9 Risk Analysis Criteria 46
Table 10 Impact Criteria 47
Table 11 Risk Acceptance Criteria 50
Table 12 Asset Inventory 54
Table 13 Threat Catalogue 56
Table 14 Vulnerability Catalogue 57
Table 15 Risk Impact 60

© CYberSynchorny, 2024

Acronyms and abbreviations

ABBREVIATION / TERM	DESCRIPTION
AM	ASSET MANAGEMENT
AI	ARTIFICIAL INTELLIGENCE
BCP	BUSINESS CONTINUITY PLAN
BIA	BUSINESS IMPACT ANALYSIS
BOD	BOARD OF DIRECTORS
CAPA	CORRECTIVE AND PREVENTIVE ACTION MECHANISMS
CCTV	CLOSED-CIRCUIT TELEVISION (SECURITY CAMERAS)
CDP	LEGAL ACT OF CYBERSECURITY TOOLKIT OF THE DIGITAL SECURITY AUTHORITY OF CYPRUS
CEO	CHIEF EXECUTIVE OFFICER
CERT	COMPUTER EMERGENCY RESPONSE TEAM
CISO	CHIEF INFORMATION SECURITY OFFICER
CMP	CHANGE MANAGEMENT PROCEDURE
D	DELIBERABLE
DMZS	DE-MILITARIZED ZONES
DPIA	DATA PROTECTION IMPACT ASSESSMENT
DPO	DATA PROTECTION OFFICER
DRP	DISASTER RECOVERY PLAN
DSA	DIGITAL SECURITY AUTHORITY OF CYPRUS
ENISA	EUROPEAN UNION AGENCY FOR CYBERSECURITY
EU	EUROPEAN UNION
GDPR	GENERAL DATA PROTECTION REGULATION
GRC	GOVERNANCE, RISK, AND COMPLIANCE
HR	HUMAN RESOURCES
IAM	IDENTITY AND ACCESS MANAGEMENT
ICT	INFORMATION COMMUNICATION TECHNOLOGY
INFOSEC	INFORMATION SECURITY AUTHORITY
IOT	INTERNET OF THINGS
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

© CYberSynchorny, 2024

IT	INFORMATION TECHNOLOGY
L	LEVEL
KPIS	KEY PERFORMANCE INDICATORS
MFA	MULTI-FACTOR AUTHENTICATION
ML	MACHINE LEARNING
MTTR	MEAN TIME TO RESPOND
NDA	NON-DISCLOSURE AGREEMENT
NIS	NATIONAL INTELLIGENCE SERVICE
NIS2	NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2
NTP	NETWORK TIME PROTOCOL
RFP	REQUEST FOR PROPOSAL
RM	REQUIREMENT
RPO	RECOVERY POINT OBJECTIVES
RTO	RECOVERY TIME OBJECTIVES
SDLC	SOFTWARE DEVELOPMENT LIFE CYCLE
SOC	SECURITY OPERATIONS CENTER
SSO	SINGLE SIGN-ON
T	TASK
TA	AWARENESS AND TRAINING
TPS	THIRD-PARTY MANAGEMENT POLICY
VPN	VIRTUAL PRIVATE NETWORK
WP	WORK PACKAGE

© CYberSynchorny, 2024

1 Executive Summary

CYberSynchrony aims to deliver a holistic modular framework that enhances cybersecurity preparedness, coordination, and resilience across Member States. The project integrates technological, operational, and human-factor components to support strategic planning, threat intelligence sharing, incident response, regulatory alignment, and cybersecurity capacity building.

The D6.3 Cybersecurity Policy Toolkit draws upon requirements identified in earlier Work Packages, the regulatory landscape analysis, and the operational needs of participating Organizations. It is designed to be scalable, adaptable, and compatible with European directives and standards.

The Toolkit provides Organizations with a harmonised suite of cybersecurity policies, governance templates, procedural guidelines, and compliance structures aligned with EU regulatory frameworks, including NIS2, GDPR, and ISO/IEC 27001. The toolkit supports public-sector entities, competent authorities, and cross-border cybersecurity ecosystems.

© CYberSynchorny, 2024

2 Introduction

This Deliverable D6.3 presents Version 0.1 of the Cybersecurity Policy Toolkit developed under WP6 of the CYberSynchrony project. The purpose of the toolkit is to provide a structured, standardised set of cybersecurity policies and supporting tools aligned with the project's objectives and the needs of stakeholders involved in cybersecurity governance and operations.

The CYberSynchrony Policy Toolkit is a combination of operational cybersecurity policy tools applied by the Digital Security Authority of Cyprus (DSA) and the Hellenic National Intelligence Service for hands-on management of national cybersecurity.

Digital Security Authority (DSA) is an independent governmental agency in Cyprus responsible for implementing the European NIS Directive, focusing on bolstering cybersecurity levels for essential services and critical infrastructures across various sectors. Tasked with enhancing the nation's cybersecurity posture, DSA collaborates with other agencies to develop legislative frameworks, promote research, foster cooperation between entities, and protect critical information infrastructure. In CYberSynchrony, DSA acts as a regulatory and policy expert, ensuring alignment with European and national cybersecurity standards. Moreover, DSA supports the development of educational content based on its deep understanding of cybersecurity protocols. DSA's expertise with critical infrastructure guides the optimization of sector-specific cybersecurity policy measures and tools.

The Centre for Technological Support, Development, and Innovation (KETYAK) of the National Intelligence Service (NIS) of Greece focuses on applied research and bolstering of the NIS capabilities through essential scientific tools and coordination in research projects. Hellenic NIS serves as: (a) the National Computer Emergency Response Team (CERT) assisting in cyberattack prevention, response and recovery, (b) the INFOSEC National authority offering advice, instructions and technical assistance to government agencies in matters of communication - information security and (c) the operator of the Hellenic government Security Operations Center (g-SOC) providing administrative and technical support to public sector in cybersecurity. In CYberSynchrony, KETYAK, given its expertise in applied research, technological support, and deep collaboration with academic and research institutions, serves as a bridge between practical applications and academic research. KETYAK also provides practical insights into the development of proactive cyber tools and strategies, leveraging its experience in countering cyber threats against national security, ensuring that the solutions developed are holistic, cutting-edge, and cater to real-world cybersecurity challenges.

The fifteen (15) Tailored Cybersecurity Policy Tools are adaptable and ready/easy-to-use, enabling security officers to obtain, adjust and update their policies to the dynamic nature of the cyber landscape, ensuring the security of their organization. All policies are in compliance with national, EU and international standards and legal frameworks.

Any Organization can easily and directly adopt and implement the present CYberSynchrony Policy Tools by inserting their individual name in the field: [Organization Name].

2.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony‘s Grant Agreement (GA) commitments, as extracted from the formal deliverable and task description, in respect to their outputs and work to be performed.

© CYberSynchorny, 2024

Table 1 Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.3	Cybersecurity Policy Toolkit v1	All	A Toolkit providing access to stakeholders to up-to-date Cybersecurity Policies and Regulations.
TASKS			
T6.5	Tailored Cybersecurity Policy Tools	Chapter 3 Sections 3.1-3.3 Chapter 4 Sections 4.1-4.15	The development of adaptable to the dynamic cybersecurity framework policy tools and templates by following a methodology relied on NIS2 and national cybersecurity authorities

2.2 Linkage to other project outputs

As an initial version, D6.3 focuses on the development of an adaptable policy toolkit to enhance organizations inAl critical sectors design their cybersecurity frameworks in alignment with the evolving EU digital space. To this end, D6.3 is built on the outputs of WP2 'CYberSynchrony Ecosystem requirements and Use Case definition' on:

(1) Review the current cybersecurity landscape and identify potential threats.

(2) Capture and detail the specific needs and requirements of end-users.

(3) Create a robust and adaptable design for the CYberSynchrony ecosystem.

Concerning the linkages of D6.3 with the progressive Tasks and Deliverables of WP6 'Cybersecurity Consciousness: Empowering Society Through Awareness (CYBERWISE) and Cybersecurity Standardization and Compliance Reinforcement (CYBERGOPLUS) is designed to exchange feedback (receive-deliver) on:

(4) Adjust the Policy Toolkit on the technical and procedural specifications of CYberSynchrony Platform and Pervasive Cybersecurity Awareness Platform. The platform will allow users to access and purchase the Policy Toolkit on the Modular Framework through their interaction with a tailored layout, user interface and navigation.

(5) Integrate policy toolkit module into the CYberSynchrony Training Plan and the Immersive Cybersecurity Game, offering an integrated training experience on the legislative and policy framework of EU to address the evolving cybersecurity landscape.

(6) Adapt to Real-time Compliance Oversight Tool that monitors the alignment of the end-users with the CYberSynchrony policy standards, ensuring that policy deviations are rectified immediately, minimizing potential security risks.

In addition, D6.3 exchanges feedback with WP8 'Integration, Demonstration, and evaluation Tasks' on:

(7) Integrate the Policy Toolkit in the Use Cases Planning to define the requirements analysis, framework architecture design, and technical specifications for the testing and demonstration of CYberSynchrony platform components.

© CYberSynchorny, 2024

(8) Test Policy Toolkit throughout the demonstration of Use Case 1 (UC1) CyberHealth Security for Digital Healthcare'.

(9) Test Policy Toolkit throughout the demonstration of Use Case 2 (UC2) Public Administration'.

(10) Test Policy Toolkit throughout the demonstration of Use Case 3 (UC3) 'Universities'.

Table 2 Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP2	T2.1 T2.2 T2.3 T2.4	D2.1	Cybersecurity landscape and threat analysis, end-user requirement analysis and use case definition – Initial version.
WP2	T2.1 T2.2 T2.3 T2.4	D2.2	Cybersecurity landscape and threat analysis, end-user requirement analysis, use case definition, and CYberSynchrony Framework – Final version.
WP6	T6.1	D6.1	Cyber Awareness Platform v1
WP6	T6.2 T6.3 T6.4	D6.2	Gamified Training Modules v1
WP6	T6.6 T6.7	D6.4	Compliance Monitoring v1
WP8	T8.1 T8.2 T8.3 T8.4	D8.1	CYberSynchrony Integration Blueprint & Use Case Portfolio v1

2.3 Deliverable Structure

The structure of this Deliverable is organized as follows:

- **Chapter 1:** Executive Summary
- **Chapter 2:** Introduction
- **Chapter 3:** Methodology for the development of policies.
- **Chapter 4:** Detailed presentation of the fifteen (15) cybersecurity policies.
- **Chapter 5:** Supporting tools and templates.
- **Chapter 6:** Implementation and monitoring framework.
- **Chapter 7:** Technical formatting specifications.
- **Chapters 8–9:** Conclusions and references.

© CYberSynchorny, 2024

3 Methodological Approach

The development of the Cybersecurity Policy Toolkit is based on a multi-layered methodological framework designed to ensure full compliance, comprehensive documentation, and alignment with Organizational needs. The approach combines international standards, regulatory requirements, and practical implementation considerations to support Organizations of varying size and maturity.

All policy tools derived from the Digital Security Authority of Cyprus (DSA) and the National Intelligence Service (KETYAK) contain practices and procedures employed in the field by security officers to support national cybersecurity.

The fifteen (15) core policy tools that synthesize the Toolkit are deployed in a progressive and escalated procedure covering the entire Cybersecurity Policy Cycle:

Table 3 Cybersecurity Incident Management Framework

CYBERSECURITY POLICY TOOLKIT	
TOOL No	**POLICY**
Tool 1	Information Security Strategy
Tool 2	Information Security Governance Policy
Tool 3	Risk Management Policy & Methodology
Tool 4	Asset Management Policy
Tool 5	Supplier and Third-Party Management Policy (TPS)
Tool 6	Access Control Policy
Tool 7	Vulnerability and Patch Management Policy
Tool 8	Network Security Policy
Tool 9	Systems & Applications Security Policy
Tool 10	Data Protection Policy
Tool 11	Acceptable Use Policy
Tool 12	Human Resources Security, Training & Awareness Policy
Tool 13	Physical Security Policy
Tool 14	Incident and Event Management Policy
Tool 15	Business Continuity and Disaster Recovery Policy

The policy toolkit applies to all organizations that belong to the critical Sectors of Annex I of NIS2 (Network and Information Systems Directive 2): [3]

1. Energy
2. Transport
3. Banking
4. Financial market infrastructures
5. Health
6. Drinking water
7. Wastewater

© CYberSynchorny, 2024

8. Digital infrastructure
9. ICT service management (business-to-business)
10. Public administration
11. Space

Any specific sector (e.g. health, public administration, digital infrastructure) shall follow its internal, national and EU policies and procedures for the adoption of cybersecurity policies. As an indication, Tool 2 'Information Security Governance Policy' outlines the decision-making tree and proceedings for the uptake of the Toolkit within the organization.

Upon the procedural integration, any Organizations can implement the CYberSynchrony Tools by inserting their individual name in the field: [Organization Name].

The 15 cybersecurity policies shall be reviewed and updated at regular and ad-hoc intervals to align with the evolving EU cybersecurity landscape. Tool 2 indicates the review policy.

3.1 Toolkit Design Principles

The design of the Toolkit is guided by a set of core principles:

Compliance with Standards and Regulations

The Toolkit incorporates requirements and best practices from key international, European, and national frameworks, including:

- **C.D.P. 389/2020 (Cybersecurity Toolkit of the Digital Security Authority of Cyprus)** [1]
- **Hellenic National Intelligence Service (NIS) Cybersecurity Policies** [2]
- **NIS2 (Network and Information Systems Directive 2)** [3]
- **ENISA Cybersecurity Standards** [4]
- **GDPR (General Data Protection Regulation)** [5]
- **CRA (Cyber Resilience Act)** [6]
- **ISO/IEC 27001:2022 (information security management systems)** [7]

In a specific approach, relying on the operational use of the fifteen tools by national cybersecurity authorities, the fifteen tools are aligned with:

- **Cybersecurity Risk-Management Measures of Article 21 of NIS2:** [3]

(a) Policies on risk analysis and information system security.
(b) Incident handling.
(c) Business continuity, such as backup management, disaster recovery, and crisis management.
(d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
(e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.
(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.
(g) Basic cyber hygiene practices and cybersecurity training.
(h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
(i) Human resources security, access control policies and asset management.

© CYberSynchorny, 2024

(j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

The specific policy tools developed are further mapped to the NIS2 requirements:

Table 4: Policy Tools to NIS2 requirements mapping

Tool ID	Policy Tool Name	Addressed NIS2 (Article 21) Requirement
Tool 01	Information Security Strategy	(a) Policies on risk analysis and information system security
Tool 02	Information Security Governance Policy	(a) Policies on risk analysis and information system security
Tool 03	Risk Management Policy	(a) Policies on risk analysis and information system security
Tool 04	Asset Management Policy	(i) Asset management
Tool 05	Human Resource Security Policy	(i) Human resources security
Tool 06	Access Control Policy	(i) Access control policies
Tool 07	Vulnerability and Patch Management Policy	(e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
Tool 08	Network Security Policy	(g) Basic cyber hygiene practices and cybersecurity training
Tool 09	System and Application Security Policy	(g) Basic cyber hygiene practices
Tool 10	Data Protection and Cryptography Policy	(h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption
Tool 11	Acceptable Use Policy	(g) Basic cyber hygiene practices
Tool 12	Supplier Relationship Security Policy	(d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
Tool 13	Incident Management Policy	(b) Incident handling
Tool 14	Information Security Assurance & Audit Policy	(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
Tool 15	Business Continuity & Disaster Recovery Policy	(c) Business continuity, such as backup management and disaster recovery, and crisis management

© CYberSynchorny, 2024

- **ENISA Cybersecurity Standards on:** [4]
  (a) Cyber Threats
  (b) EU incident response and cyber crisis management
  (c) Market
  (d) Product Security and Certification
  (e) Risk Management
  (f) Skills and competences
  (g) State of cybersecurity in the EU
  (h) Vulnerability Disclosure

- **European Union Legislative Landscape:** [8]

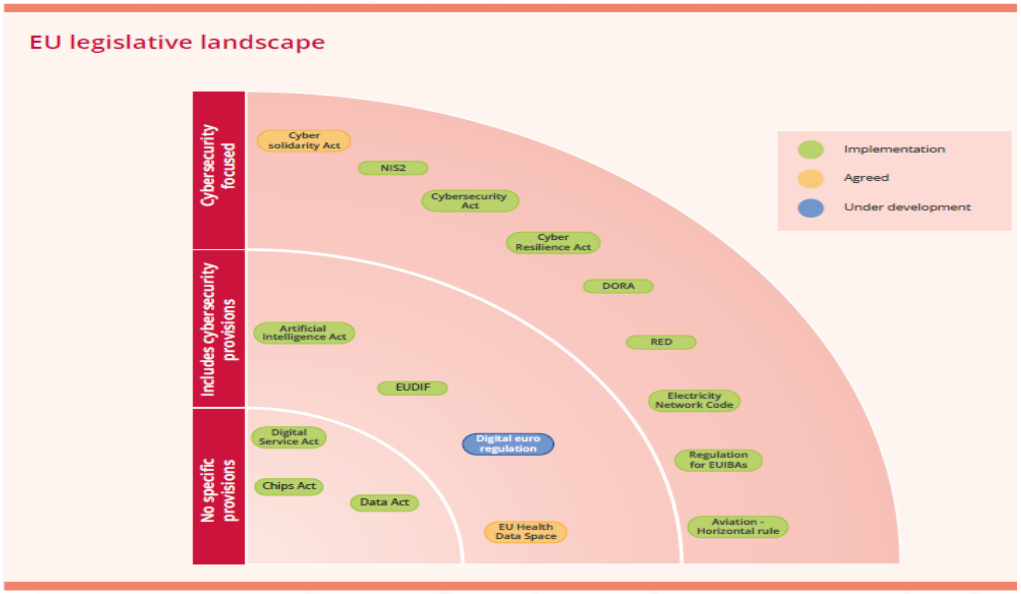

Figure 1 EU Legislative Landscape

Adaptability

Each policy is structured so it can be tailored to:

- the national cybersecurity framework
- the size of the Organization,
- its cybersecurity maturity level,
- its operational context and scope.

This ensures that the Toolkit is applicable to both small and large entities.

Clarity and Efficiency

The policies are written in a concise and structured manner to support clear interpretation and immediate application without unnecessary complexity.

Integration into Organizational Processes

Cybersecurity is treated as an embedded component of Organizational governance and day-to-day operations. The Toolkit promotes integration with existing processes, such as:

- Governance and compliance,
- IT and operations,
- HR and procurement,
- Enterprise risk management.

© CYberSynchorny, 2024

Reusability and Maintainability

All policies follow a common structure, enabling easy maintenance, versioning, and extension as Organizational needs evolve.

3.2 Guidelines for Use and Integration into Organizational Processes

For effective adoption and implementation of the Toolkit, the following steps are recommended:

1. **Formal approval by senior management**, establishing the policies as authoritative internal requirements.
2. **Integration into operational procedures** across functions (IT, HR, procurement, operations).
3. **Staff training and awareness**, ensuring personnel understand and can apply each policy.
4. **Clear communication channels** for reporting, clarification, and policy-related feedback.
5. **Continuous evaluation of effectiveness**, supported by monitoring mechanisms and periodic assessments.

While the policies in this toolkit are designed as universal baselines, specific sectors must tailor the content to address their unique regulatory and operational environments. The following guidelines provide concrete examples for the CYberSynchrony pilot sectors:

- **Healthcare (Use Case 1):**
    - **Asset Management (Tool 4):** Customization must explicitly classify Electronic Health Records (EHR) and IoMT devices (e.g., insulin pumps, pacemakers) as "Critical Assets."
    - **Access Control (Tool 6):** Policies should define strict "Break-Glass" procedures, allowing emergency access to patient records during life-critical incidents, a requirement unique to medical environments.
    - **Data Protection (Tool 10):** Must explicitly reference GDPR Article 9 (Special Categories of Personal Data) and national health data laws regarding patient confidentiality.
- **Public Administration (Use Case 2):**
    - **Information Security Strategy (Tool 1):** The strategic objectives should emphasize the "Continuity of Essential Public Services" (e.g., water, civil registry) as a primary goal.
    - **Incident Management (Tool 13):** Reporting procedures must be customized to include mandatory notification timelines to national CSIRTs or Digital Security Authorities, as required for Operators of Essential Services (OES).
    - **Supplier Relationship (Tool 12):** Due diligence clauses should focus heavily on the integrity of software used for citizen digital identity platforms.
- **Academia and Research (Use Case 3):**

© CYberSynchorny, 2024

- **Acceptable Use Policy (Tool 11):** This policy requires significant adaptation to accommodate "Open Science" principles, defining acceptable boundaries for high-performance computing (HPC) usage and personal device (BYOD) connections on campus networks.

- **Vulnerability Management (Tool 7):** Patching schedules should be adjusted to account for "Research Freeze" periods, ensuring that security updates do not disrupt long-running computational experiments.

- **Data Protection (Tool 10):** Customization should distinguish between administrative data (Student PII), which requires strict locking, and research data, which may require open publication.

Furthermore, the adoption of policies and procedures should follow a *risk-based approach*; where each organization is expected to assess the risks applicable to their context and operations and implement the appropriate measures to reduce risk and increase operational resilience. As such, it is expected that organizations that opt to make use of these policies do so with the understanding that they require adaptation to the organizational context.

3.3 Policy Update and Document Control Procedure

Document management is an essential quality assurance mechanism. The procedure includes:

- **Designation of a Policy Owner** (responsible for content) and a **Policy Custodian** (responsible for maintenance and distribution).
- **Annual review**, or review triggered by significant Organizational, technological, or regulatory changes.
- **Version control mechanisms** to track modifications and ensure consistency.
- **Documented revision history**, recording all updates and justifications.
- **Retention of previous versions** to maintain traceability and compliance records.

© CYberSynchorny, 2024

4 Security Policies and Standards

This chapter presents a detailed description of the 15 core security policies included in the Cybersecurity Policy Toolkit. Each policy has been developed to provide clear, actionable guidance and to support Organizations in establishing a structured and comprehensive cybersecurity framework aligned with international best practices and regulatory requirements. All Tools contain separate policy templates implemented by the Digital Security Authority of Cyprus and the Hellenic National Intelligence Service. The present CYberSynchrony Policy Toolkit is a synthesis of progressive policy templates providing a holistic cybersecurity approach to stakeholders.

© CYberSynchorny, 2024

4.1 Tool 1 - Information Security Strategy

[Organization Name]

INFORMATION SECURITY STRATEGY

© CYberSynchorny, 2024

Table of Contents

1. Introduction .....
   1.1 Purpose .....
2. Scope .....
3. Alignment of the Information Security Strategy with the Business Strategy .....
4. Key Strategic Pillars of Information Security .....
   4.1 Governance and Compliance .....
   4.2 Risk Management Process .....
   4.3 Information Security Framework .....
   4.4 Monitoring and Incident Response .....
   4.5 Training and Awareness .....
   4.6 Adoption of Technological Innovations in Cybersecurity .....
   4.7 Supplier and Third-Party Management .....
5. Legislative Acts .....
6. Performance Metrics and Monitoring .....
7. Implementation Plan for Strategic Information Security / Cybersecurity Interventions (Example) .....
   7.1 Justified Allocation of Budget and Resources for Plan Implementation .....
8. Top Management Commitment .....
9. Review .....
10. References .....

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

[Organization Name] establishes an **Information Security Strategy** that sets out the long-term objectives and high-level approach for managing information security, with the aim of mitigating related risks. The Strategy ensures that information security efforts are aligned with the mission, objectives, regulatory and other requirements of [Organization Name], while at the same time enhancing resilience against evolving threats.

This is achieved through the implementation of advanced cybersecurity practices, staff training and awareness, ongoing risk analysis, and continuous improvement of Organizational and technical information security measures.

More specifically, the strategic objectives are to:

- Align the information security strategy with the Organizational objectives of [Organization Name] by embedding relevant security controls into business processes, thereby supporting the strategic goals of [Organization Name].
- Mitigate risks through a structured risk assessment process that identifies, evaluates, and prioritizes information security risks and ensures the implementation of appropriate measures to reduce their impact on the operations of [Organization Name].
- Ensure compliance with relevant legislation, regulations (e.g. NIS2 Directive), and applicable good practices and standards.
- Promote a culture of training and awareness, fostering a strong sense of responsibility for security matters across [Organization Name].
- Leverage advanced technologies and methodologies to enhance the effectiveness of security controls. The target state includes full integration of advanced information security measures into all aspects of [Organization Name]'s business activities.
- Ensure continuity of operations by building capabilities for effective detection, response, and recovery from security incidents.
- Establish mechanisms for regular review and improvement of Organizational and technical security measures in order to address emerging threats and vulnerabilities in [Organization Name]'s systems.
- Develop close relationships and collaboration with third parties (e.g. suppliers) to strengthen cybersecurity across [Organization Name]'s entire supply chain.

© CYberSynchorny, 2024

2. Scope

This Strategy applies to all assets, infrastructure, personnel, and processes of the Organization, including the following:

- **Human resources** (employees and third parties/suppliers) who have access to or interact with information systems.
- **Information assets** relating to significant categories of data, whether stored, processed, or transmitted, include sensitive, personal, and business-critical information.
- **Policies, procedures, and other workflows** related to information management.
- **Technical infrastructure**: hardware, software, other IT systems and applications, networks, and cloud-based environments and services.
- **Physical assets and facilities** that host critical information, such as data centers and other buildings and locations where [Organization Name] operates.

3. Alignment of the Information Security Strategy with the Business Strategy

The Information Security Strategy is a critical component of the Organization's overall business strategy and must remain aligned with the mission and strategic objectives of [Organization Name]. Integrating information security and cybersecurity into business strategy strengthens productivity, coordination, and coherence of efforts, thereby enhancing the overall resilience and security posture of the Organization.

Information security should not be treated as a standalone function but as a key enabler of Organizational success. It must protect critical data and systems while supporting innovation and operational efficiency.

During the strategic planning process, the results of information security and cybersecurity risk assessments must be considered to support better planning of future needs and initiatives.

To ensure that the Strategy remains current, the alignment between the Information Security Strategy and the business strategy must be periodically assessed and updated where necessary. In addition, the Information Security Strategy should be developed in close collaboration with the business units of the Organization to ensure mutual support and improved overall performance.

4. Key Strategic Pillars of Information Security

The documented Strategy describes, in detail, specific security objectives, the approach to security and risk management, and the means for validating the effectiveness of the Strategy through key performance indicators (KPIs).

To record and prioritize objectives, [Organization Name] has adopted the Cybersecurity Maturity Model as a practical tool for guidance, self-assessment, planning, and continuous improvement of its security posture. The Model helps [Organization Name] determine where it aims to be within the next three to five years in terms of maturity for each category and subcategory.

The prioritization of Information Security Strategy objectives and high-level security goals, as well as the related implementation actions, are organized as follows:

© CYberSynchorny, 2024

4.1 Governance and Compliance

- Definition of roles and responsibilities for information security/cybersecurity within [Organization Name].
- Development and implementation of a cybersecurity policy framework. The Information Security Strategy is reflected in the information security policy.
- Development and adherence to relevant policies, procedures, standards, and guidelines.
- Monitoring compliance with regulatory and other obligations.
- Strengthening monitoring and reporting mechanisms for cybersecurity-related policies.

Opportunities: Cooperation with experienced information security/cybersecurity providers, strengthening internal expertise, potential compliance with international standards such as ISO 27001 or other relevant standards, and increased customer confidence in [Organization Name].

Constraints: Limited budget for ongoing investment in new technologies, high cost of compliance, difficulty in attracting specialized experts, and the constantly evolving cyber threat landscape.

Linkage: Reference to the "Information Security Governance Policy".

4.2 Risk Management Process

- Development of a risk assessment and management framework for [Organization Name], including processes for identifying, analyzing, evaluating, and mitigating potential threats and vulnerabilities.
- Definition of key tools and methodologies to be used for risk management.

Opportunities: Better-informed and faster decision-making, competitive advantage, improved efficiency through optimized processes, and encouragement of innovation and growth.

Constraints: Budget, staffing, and expertise limitations; incomplete, inaccurate, or unavailable data; challenges in maintaining relevance due to the rapidly changing cybersecurity and threat landscape; and resistance to change.

Linkage: Reference to the "Risk Management Policy" and to the "Asset-Based Risk Assessment Workbook" (Asset Register and Risk Assessment Tool).

4.3 Information Security Framework

- Establishment of an effective and documented Information Security Management System (ISMS) to protect information from threats (internal or external, intentional or accidental).

Opportunities: A structured approach for identifying, assessing, and mitigating cyber risks; improved protection of critical assets and reduced exposure to attacks; and enhanced compliance.

Constraints: Resource limitations for maintaining a comprehensive security framework; complexity; resistance to change; and the need to maintain relevance in a changing cyber threat environment.

Linkage: Reference to the "Information Security Policy".

4.4 Monitoring and Incident Response

- Development of a comprehensive incident response plan and, where appropriate, establishment of a monitoring capability or Security Operations Center (SOC) for continuous monitoring and rapid response to cyberattacks.

© CYberSynchorny, 2024

- Training teams to identify and respond effectively to security incidents.
- Training of specialized staff and formation of dedicated teams for efficient incident management.
- Conduct post-incident reviews to improve future response.

Opportunities: Minimization of operational disruption; use of advanced tools and techniques for detection and handling of cybersecurity incidents; and improved trust among stakeholders of the Organization.

Constraints: Shortage of specialized personnel capable of managing advanced tools and minimizing operational disruption; time-consuming testing and training; and high volume of alerts, many of which may be false positives.

Linkage: Reference to the "Incident and Event Management Policy".

4.5 Training and Awareness

- Conduct of periodic training sessions for employees and other relevant stakeholders.
- Organization of awareness campaigns on cybersecurity risks and security topics to promote best practices.
- Exercises and simulations (e.g. phishing simulations and other drills) to strengthen Organizational readiness.
- Documentation of specific measures for staff training and awareness.

Opportunities: Increased staff awareness of cybersecurity issues; improved ability of personnel to identify and respond to cyber threats; better work performance and productivity; improved acceptance of and adaptation to change; and development of future in-house specialists with advanced skills.

Constraints: Limited budget for training programmes, staff reluctance to participate, and the need to continuously update training content to keep it relevant.

Linkage: Reference to the "Human Resources Security, Training & Awareness Policy".

4.6 Adoption of Technological Innovations in Cybersecurity

- Investment in and deployment of state-of-the-art cybersecurity technologies, including advanced threat detection and prevention tools.
- Integration of Artificial Intelligence (AI) and Machine Learning (ML) for analysis of large data volumes (big data) to detect cyberattacks.
- Development of architectures such as Zero Trust and Defense in Depth to strengthen network security.
- Integration of security-by-design principles into system and application development.

Opportunities: Support from national resources for resilience; collaboration with operators of critical infrastructure for sharing best practices; development of specialized teams to protect emerging technologies; and enhanced capability to respond to attacks targeting critical infrastructures.

Constraints: Persistent cyber threats; high cost of implementing advanced technologies; and the need for continuous staff training.

4.7 Supplier and Third-Party Management

- Documentation of policies that define how cybersecurity risks arising from suppliers and other third parties are managed.
- Definition of contractual requirements, including compliance with the Organization's information security policies.
- Conduct of regular assessments and audits of third-party security practices.

© CYberSynchorny, 2024

- Monitoring of third-party access to the Organization's systems and data to ensure continuous compliance and risk mitigation.

Opportunities: Improved expertise and efficiency through the use of external providers offering specialized skills and technologies, cost savings without the need for major upfront investment by the Organization; and flexible, scalable solutions.

Constraints: Risks relating to data security and privacy; dependence on a single provider; limited control and visibility over external providers' processes and security measures; and contractual and legal challenges.

Linkage: Reference to the "Supplier and Third-Party Management Policy".

5. Legislative Acts

For the successful implementation of the Information Security Strategy, it is essential to consider the main legislative acts governing cybersecurity and information protection.

Continuous monitoring of these legislative acts ensures that the Organization remains compliant with new requirements and provides the necessary protection and flexibility in the field of information security and cybersecurity.

6. Legislative Acts

To measure the effectiveness of cybersecurity, [Organization Name] defines specific Key Performance Indicators (KPIs) linked to the strategic objectives outlined above.

Through regular reports submitted to senior management, appropriate visibility is provided regarding information security performance and areas requiring improvement. This facilitates progress monitoring and evaluation of the achievement of the intended outcomes.

To measure the effectiveness of the Information Security Strategy, the following indicative metrics may be monitored:

1. Development and Implementation of a Cybersecurity Policy

- Level of compliance with the internal cybersecurity policy.
- Time to respond to emerging cybersecurity threats.
- Results of compliance audits.

2. Development of Critical Monitoring and Incident Response Capabilities

- Percentage reduction in successful cyberattacks on applications and data.
- Success in restoring critical infrastructures after an attack.
- Time to detect and respond to critical cybersecurity incidents.
- System availability time and recovery time after disruptions.

3. Promotion of Staff Training and Awareness

- Participation and completion rate of staff in cybersecurity training programmes.
- Success rate in staff security examinations or assessments.

4. Adoption of Technological Innovations for Cybersecurity

- Success in deploying innovations such as IoT and AI to enhance cybersecurity.

© CYberSynchorny, 2024

7. Implementation Plan for Strategic Information Security / Cybersecurity Interventions (Example)

Below is an example implementation plan for strategic interventions related to Information Security / Cybersecurity, which has been approved by the Top Management of [Organization Name] and reviewed at least annually.

Table 5 Implementation

No.	Cybersecurity Project	Start Date	Completion Date	Owner/Responsible Unit	Required Resources	Evaluation Method
1	Strengthening Anti-Phishing Programmes			IT Department	Budget, Staff, Training	Performance Recording, Evaluation Criteria
2	Staff Training on Cyber Threats			Human Resources	Training Material, Instructors	Attendance Monitoring, Training Evaluation
3	Network Security Upgrade			Network Department	Detection Tools, Technical Staff	Achievement of Defined Objectives, Network Security Assessment
4	ISO 27001 Compliance Assessment			Cybersecurity Department	Specialists, Assessment Tools	Compliance Verification, Identification of Gaps
5	Implementation of Zero Trust Architecture			Cybersecurity Department	Technological Resources, Staff Training	Implementation Analysis, Results Evaluation

7.1 Justified Allocation of Budget and Resources for Plan Implementation

The allocation of budget and resources for implementing the initiatives in the Implementation Plan for Strategic Information Security / Cybersecurity Interventions must be based on justified investments aligned with the prioritized objectives and the results of risk assessments. For each intervention, at least the following elements should be documented in a dedicated report:

1. Priority Analysis:

- Assessment of the criticality and impact of each cybersecurity objective.
- Understanding the risk level and required resources for each objective.

2. Investments:

- Allocation of budget according to the importance of each cybersecurity objective.
- Prioritization of investments in objectives with higher risk or criticality.

3. Risk Assessment:

- Evaluation of the risks associated with each cybersecurity objective.
- Documentation of the resources required to reduce these risks.

4. Efficiency Evaluation:

- Definition of measurable performance indicators and KPIs for each investment.
- Continuous evaluation of investment effectiveness and adjustment of resource allocation accordingly.

© CYberSynchorny, 2024

5. Flexibility for Handling Emergencies:

- Maintaining flexibility in the budget to address unexpected cybersecurity incidents.
- Establishment of contingency plans for rapid response to emerging threats.

6. Continuous Review and Updating:

- Periodic review of requirements and priorities.
- Updating resource allocation based on developments in the cybersecurity landscape.

8. Top Management Commitment

The actions identified for implementation under the Strategy are supported by top management through the provision of resources, knowledge, and time. The management of [Organization Name] is committed to promoting and supporting the implementation of the Information Security Strategy in order to protect information and ensure its confidentiality, integrity, and availability.

As noted above, top management demonstrates its commitment to cybersecurity through the following key commitments:

1) Support and Resources:
   Provision of the necessary financial, human, and technological resources for the implementation of cybersecurity policies and measures.
2) Promotion of Cybersecurity Policies:
   Development, approval, and enforcement of cybersecurity policies, as well as compliance with them.
3) Staff Awareness:
   Provision of training and awareness activities for staff regarding cybersecurity threats.
4) Continuous Assessment and Enhancement:
   Regular evaluation of cybersecurity measures and implementation of improvements where required.
5) Crisis Management:
   Development and maintenance of a strong crisis management capability in the event of a cyberattack.
6) Cooperation with External Bodies:
   Pursuit of close cooperation with external bodies and authorities for information sharing and joint response to cybersecurity challenges.

This commitment is a fundamental pillar in ensuring a reliable, secure, and resilient information environment for the Organization and all involved stakeholders.

9. Review

To ensure the successful implementation and management of the Information Security Strategy, a systematic and continuous lifecycle for this document must be applied, including:

- Periodic review of cybersecurity objectives, in order to verify ongoing alignment with developments in the cybersecurity domain. As part of this process, a review of the relevant elements should take place at least annually, and any changes should be implemented through the established change management process.

© CYberSynchorny, 2024

- Definition of responsibilities and roles for reviewing and updating the Strategy, clearly assigning accountabilities to all parties involved.
- Validation of the effectiveness of actions through performance indicators directly linked to the Organization's objectives.
- Reporting to Top Management via a formal mechanism that communicates review results, performance of implemented actions, and the derived indicators.

10. References

Category	ID	Measure	Objective of the Measure
Strategy	STR1	Strategy for Information Security	To establish an information security strategy that defines high-level objectives and approach to mitigate security risks.
Governance	GOV1	Roles and Responsibilities for Information Security	To define roles and responsibilities for information security within the Organization.
Governance	GOV2	Compliance with Legal and Regulatory Obligations	To ensure compliance with all applicable legal and regulatory obligations regarding network and information security.
Governance	GOV3	Information Security Policies, Standards, Guidelines, Procedures	To establish information security policies, standards, guidelines, and procedures that reflect the information security strategy.

© CYberSynchorny, 2024

4.2 Tool 2 - Information Security Governance Policy

[Organization Name]

INFORMATION SECURITY GOVERNANCE POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
   1.1 Scope
2. Organizational Chart (Example)
3. Information Security Roles and Responsibilities
   3.1 Roles and Responsibilities of Top Management
   3.2 Network and Information Systems Security Officer (NIS Officer)
   3.2.1 Minimum Responsibilities of the NIS Officer
   3.2.2 Position of the NIS Officer within the Organization
   3.3 Business Continuity and Disaster Recovery Officer
   3.4 Information Processing Owners / System Access Owners
   3.5 Chief Information Security Officer (CISO)
   3.6 Information Security Analysts
   3.7 Security Awareness Trainer
   3.8 Steering Committee
4. Compliance with Legal and Regulatory Obligations
5. Review
6. References

© CYberSynchorny, 2024

1. Introduction

Purpose

This document defines the Information Security Governance of [Organization Name].

Information Security Governance includes, among other things, the Statement of Applicability of the K.D.P. 389/2020 Framework, as well as the Organizational Chart of [Organization Name].

It subsequently includes the Organization's Obligations regarding Information Security, as well as the Roles and Responsibilities of the Network and Information Systems Security Officer, the Business Continuity and Disaster Recovery Officer, and the Information Processing Officers or holders of access to the information processing systems of [Organization Name], as referenced in Decision K.D.P. 389/2020.

It further includes the central repository of the legal, regulatory, supervisory, and contractual obligations related to network and information security that [Organization Name] is required to comply with.

[Organization Name] aims to conduct its activities professionally, applying high standards in the provision of services, both internally and externally.

1.1 Scope

This policy applies to all employees of [Organization Name] who have access to Organizational information and information systems, including all stages of the information lifecycle (storage, transmission, processing, and disposal/destruction).

2. Organizational Chart (Example)

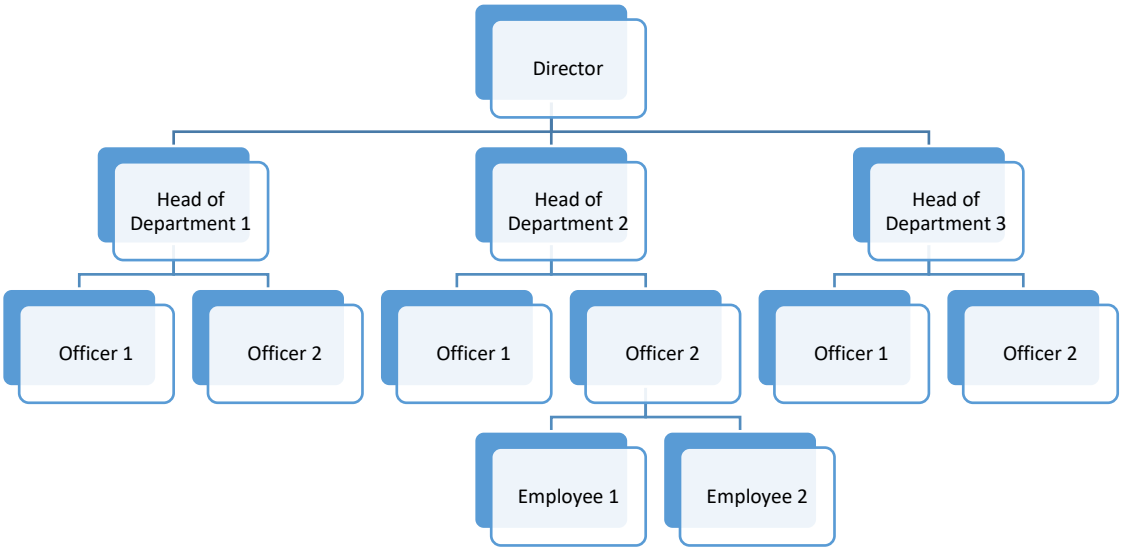

Figure 2 Organizational Chart

Note: Each Organization may define only those roles that align with its needs and structure and may omit roles that are not applicable. Additionally, depending on the Organization's size, it may not be feasible to appoint separate individuals for each role. In such cases, more than one role may be assigned to a single individual, provided that no conflict of interest arises between those roles.

© CYberSynchorny, 2024

3. Information Security Roles and Responsibilities

[Organization Name] maintains a distinct Organizational unit responsible for the security of its networks, systems, and information. Roles and responsibilities are clearly defined in order to avoid conflicts of duties, as depicted in the Organizational chart.

[Organization Name] has assigned clear cybersecurity roles, duties, and responsibilities for all staff. These are reviewed periodically to ensure their continued suitability. The Organization identifies, assesses, and addresses any occurrence of conflicting duties.

3.1 Roles and Responsibilities of Top Management

Roles and responsibilities for Top Management, the Board of Directors (BoD), and Steering Committees vary according to the nature of the Organization, its sector, and its structure. Indicative roles and responsibilities include:

Top Management

1. Chief Executive Officer (CEO)

- Defines the overall strategy and direction of the Organization.
- Is responsible for achieving business objectives.
- Represents the Organization externally.

2. President

- Chairs the meetings of the Board of Directors.
- Works closely with the CEO on the development and implementation of strategic initiatives.

3. Executive Management Team

- Implements decisions of Top Management.
- Manages the operational aspects of the Organization.

Board of Directors (BoD)

1. Board Members

- Oversee the activities of Top Management.
- Establish policies and monitor strategic direction.

2. Chair of the Board

- Chairs the Board meetings.
- Represents the Board to Top Management.

Steering Committee

1. Chair of the Steering Committee

- Leads meetings and coordinates the activities of the Steering Committee.
- Collaborates with Top Management to implement specific strategies.

2. Members of the Steering Committee

- Advise on issues related to their domain of expertise.
- Work with Top Management on the implementation of programmes and initiatives.

© CYberSynchorny, 2024

The interaction and cooperation between these levels is a critical factor for decision-making, oversight, and the achievement of the Organization's objectives.

3.2 Network and Information Systems Security Officer (NIS Officer)

[Organization Name] has appointed a qualified and appropriately experienced Network and Information Systems Security Officer (NIS Officer) and has notified the relevant authorities of the officer's contact details.

- The NIS Officer is appointed on the basis of professional qualifications, and particularly on the basis of specialized knowledge in network and information systems security and the ability to fulfil the duties listed below (Minimum Responsibilities).
- The NIS Officer performs exclusively duties related to network, systems, and information security and is not engaged in other tasks. In the case of small Organizations, the NIS Officer may perform additional duties provided that no conflict of interest arises and taking into account the Organization's criticality level, and subject to approval by the Digital Security Authority.
- [Organization Name] has communicated the NIS Officer's contact details to the Digital Security Authority.
- [Organization Name] has ensured that candidates for the role of NIS Officer have been appropriately vetted so that the appointed individual can properly discharge their duties. The suitability of the NIS Officer is evaluated periodically.

3.2.1 Network and Information Systems Security Officer (NIS Officer)

The NIS Officer appointed by [Organization Name] has at least the following responsibilities:

- Inform and advise [Organization Name] and staff who have access to network and information systems about their obligations and other relevant legal and regulatory provisions.
- Monitor compliance with national or EU provisions on information security, and with [Organization Name]'s internal policies on network and information systems security.
- Provide advice on information security management and monitor performance in line with the Organization's risk management methodology and procedures.
- Collaborate with and act as the single point of contact for the Digital Security Authority on issues related to its competencies, including support for external audit activities and the provision of documents and information.
- Report to senior management on information security threats, vulnerabilities, and risks through formal and regular reports.
- Perform, at least annually, a risk assessment of networks, information systems, and essential services to identify significant weaknesses and vulnerabilities in network infrastructures.

3.2.2 Position of the NIS Officer within the Organization

[Organization Name] ensures that the NIS Officer:

a. Is appropriate and timely involved in all matters relating to network and information systems security.

b. Is supported by [Organization Name] in the performance of the duties described above (Minimum Responsibilities).

c. Does not receive instructions that conflict with the exercise of those duties and is not dismissed or penalized by [Organization Name] for performing them properly.

d. Reports directly to the highest management level of [Organization Name].

e. Is bound by confidentiality and professional secrecy in the performance of their duties.

© CYberSynchorny, 2024

f. Has access to the necessary financial and human resources, processes, and technical and Organizational measures to carry out the role and to support the Organization in complying with the obligations set by the Digital Security Authority.

g. Possesses appropriate knowledge, training, and experience consistent with the duties of the role and maintains that knowledge through regular professional development. The Digital Security Authority may issue guidance on suitable training and experience for the NIS Officer.

3.3 Business Continuity and Disaster Recovery Officer

The Business Continuity and Disaster Recovery Officer is responsible for the coordination and design of the Business Continuity Plan (BCP) and the Disaster Recovery Plan (DRP) in the event of disruption to the operations of [Organization Name].

The Officer is also responsible for distributing these plans to personnel involved in restoring critical business functions and operations. Specifically, the Officer is responsible for:

- Identifying and assessing critical business processes to be included in the BCP and DRP.
- Overseeing and coordinating:
    - risk assessments and impact analyses,
    - assessment of the adequacy and alignment of the plans with business objectives.
- Maintaining records of reviews and updates of the BCP and DRP and monitoring Organizational changes that may require their revision.
- Supervising the readiness of alternative recovery sites (where applicable) in terms of resources and applications.
- Identifying the incident causing the disruption to business and triggering the relevant plans (e.g. Incident and Event Management Policy, Crisis Management Plan, Disaster Recovery Plan).
- Designating an appropriate alternative location for the recovery of critical business functions, where relocation is required.
- Coordinating and overseeing the restoration of critical business functions and processes to ensure continuity of operations.
- Coordinating infrastructure and facilities security plans in case of relocation to alternative premises.
- Supervising the transfer and management of staff and necessary equipment to the alternative recovery site (where applicable).
- Managing human resources issues arising from the activation or testing of the BCP and DRP.
- Reviewing, testing, and revising the BCP and DRP.
- Planning and coordinating ongoing training and awareness activities for those involved in BCP and DRP implementation.

3.4 Information Processing Owners / System Access Owners

Table 6 Information Processing Owners / System Access Owners

Name and Surname	Title	Roles and Responsibilities	Relevant Access Rights

© CYberSynchorny, 2024

These individuals are responsible for specific information processing activities or hold access to information processing systems and must ensure appropriate use and protection of those systems and data.

3.5 Chief Information Security Officer (CISO)

The CISO, or Chief Information Security Officer, is a senior executive who oversees an organization's information, cybersecurity, and technology security. CISO's responsibilities include developing, implementing, and enforcing security policies aimed at protecting critical data. The exact duties vary depending on the Organization. Traditionally, CISO focuses on developing and leading the information security program. This includes protecting the Organization's assets, applications, systems, and technology, while also enabling and promoting business outcomes.

3.6 Information Security Analysts

Information Security Analysts are responsible for monitoring and analysing security systems. Their duties include:

- Monitoring Organizational networks for security breaches and investigating incidents.
- Using and maintaining security software (e.g. firewalls, encryption tools) to protect sensitive information.
- Performing vulnerability assessments on systems and networks.
- Researching current trends in information security.
- Preparing reports documenting metrics, attempted attacks, and security breaches.
- Developing security standards and best practices for the Organization.
- Proposing security improvements to management or senior IT staff.
- Designing and implementing security measures to protect Organizational networks and systems.
- Supporting end users in installing or learning new security products and procedures.
- Staying up to date with new attack methods and security techniques and evaluating new security technologies for their effectiveness.

3.7 Security Awareness Trainer

The Security Awareness Trainer is responsible for training and educating staff on security best practices. They develop training programmes and materials, promote awareness of threats, and emphasize the importance of complying with security policies. Their focus is on cultivating a secure cultural mindset within the Organization by improving employees' security awareness.

Other duties may include, but are not limited to:

• Training and managing technology-related risks in collaboration with the Organization's Management.

• Developing and implementing continuous user security training and awareness programmes.

• Building and leading the cybersecurity strategy and framework, with initiatives to safeguard the Organization's cyber assets and technology.

• Implementing and managing the governance, risk, and compliance (GRC) process.

• Conducting phishing tests to teach employees how to recognize such attacks.

• Performing practical analysis of common cyberattacks.

• Reporting to the highest levels of the Organization (the CEO and the board of directors, or equivalent).

• Developing, justifying, and evaluating cybersecurity investments.

© CYberSynchorny, 2024

3.8 Steering Committee

The Steering Committee, or another appropriate executive-level committee, should provide management with expectations, along with accountability, for overseeing, coordinating, and assigning responsibility for the effectiveness of the cybersecurity program. Cybersecurity expertise should be maintained within this Committee. If necessary, the Committee should engage external experts with the appropriate experience to assist with its oversight responsibilities.

The Committee should review assessment reports that describe the effectiveness of the cybersecurity program on a regular basis (e.g., at least annually). Recommendations for corrective actions should be discussed whenever required. The Committee should ensure that annual self-assessments evaluate the Organization's ability to meet defined cybersecurity requirements. The Committee should approve the prioritization of remediation activities, including the allocation of resources, based on the assessment results.

The Committee should be responsible for maintaining a process for the formal discussion and evaluation of potential costs associated with cybersecurity incidents and data breaches as part of the budgeting process. It should also ensure that management takes appropriate actions to address evolving cyber risks or significant cybersecurity issues.

4. Compliance with Legal and Regulatory Obligations

[Organization Name] maintains a central register of legal, regulatory, and contractual obligations relating to network and information security.

Table 7 Compliance with Legal and Regulatory Obligations

No.	Legislation / Regulation / Directive	Reference Number	Type	Date of Last Amendment
1	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)	2016/679	Regulation	04/05/2016
2	Law on Network and Information Systems Security (2020) and related Decisions	C.D.P. 389/2020	Law	21/08/2020
3	Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union	2022/2555	Directive	14/12/2022

Internal audits must be carried out at least annually to verify compliance with all relevant legislative, regulatory, and contractual requirements relating to network and information security.

Where non-compliance is identified, [Organization Name] must define and implement a compliance action plan.

5. Review

The owner of this policy is [Policy Owner Title], who is responsible for its implementation, maintenance, and review in line with the following guidelines:

- Significant changes within the Organization.

© CYberSynchorny, 2024

- Information security incidents or regulatory changes.
- Annual review to determine the need for:
    - improving the effectiveness of the policy
    - updating the policy due to technological or Organizational changes.

6. References

Category	ID	Measure	Objective of the Measure
Strategy	STR1	Strategy for Information Security	To establish an information security strategy that defines high-level objectives and approach for mitigating security risks.
Governance	GOV1	Roles and Responsibilities for Information Security	To define roles and responsibilities relating to information security within the Organization.
Governance	GOV2	Compliance with Legal and Regulatory Obligations	To ensure compliance with all applicable legal and regulatory obligations regarding network and information security.
Governance	GOV3	Information Security Policies, Standards, Guidelines, and Procedures	To establish information security policies, standards, guidelines, and procedures that reflect the information security strategy.

© CYberSynchorny, 2024

4.3 Tool 3 - Risk Management Policy & Methodology

[Organization Name]

RISK MANAGEMENT POLICY & METHODOLOGY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
   1.1. Purpose
   1.2. Scope
2. Risk Management Policy
   2.1. Asset Inventory
   2.2. Risk Register
   2.3. Risk Analysis and Evaluation
   2.4. Risk Treatment Plans
3. Review
4. References
5. ANNEX A – Risk Management Methodology
   5.1. Definition of Scope
   5.2. Purpose of Risk Assessment
   5.3. Definition of Roles and Responsibilities
   5.4. Identification of Assets
   5.5. Identification of Potential Vulnerabilities
   5.6. Identification of Potential Risks
   5.7. Identification of Types of Risks
   5.8. Identification of Risk Owners
   5.9. Identification of Existing Security Controls
   5.10. Risk Analysis Criteria
   5.10.1. Likelihood Criteria
   5.10.2. Impact Criteria
6. Risk Scoring Criteria
7. Risk Analysis / Evaluation Process
   7.1. Information Gathering
   7.2. Likelihood Assessment
   7.3. Impact Assessment
8. Risk Treatment
   8.1. Risk Acceptance Criteria
   8.2. Risk Appetite Policy
   8.3. Risk Treatment Strategies
   8.4. Selection of Risk Treatment Measures
   8.5. Implementation Plan for Network and Information Security Measures (Action Plan)
   8.5.1. Activities to be Included in the Action Plan
   8.5.2. Resource Requirements
   8.5.3. Assignment of Roles and Responsibilities
   8.5.4. Monitoring Effectiveness and Reporting
   8.5.5. Evaluation and Review of the Risk Treatment Plan
   8.5.6. Reporting and Continuous Improvement
   8.6. Statement of Applicability of the Framework
9. Risk Assessment and Treatment Procedure
   9.1. Process Diagram
   Annex B – Asset Inventory
   Annex C – Threat Catalogue
   Annex D – Vulnerability Catalogue
   Annex E – Risk Impact Criteria

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

This document includes indicative Policy Terms for the management of risks related to the assets and data of **[Organization Name]**, in accordance with the provisions of the Security of Networks and Information Systems (Security Measures for Operators of Essential Services and Operators of Critical Information Infrastructure) Decision of 2020 (K.D.P. 389/2020) and the Security of Networks and Information Systems (Cybersecurity Maturity Controls) Decision of 2024 (K.D.P. 245/2024).

The purpose of this document is to:
• Establish a structured approach to risk management by defining the risk assessment process, the risk analysis criteria, the risk acceptance criteria, and the Organization's risk appetite.
• Enhance Organizational resilience by minimizing exposure to information security/cybersecurity risks.
• Ensure alignment of risk management with the Organization's strategic objectives and regulatory obligations.
• Define roles and responsibilities for activities related to risk management.
• Support decision-making by providing a structured methodology for the assessment and treatment of risks.
• Promote a culture of awareness of information security/cybersecurity risks through continuous monitoring, training, and improvement.

1.2 Scope

The Risk Management Policy and Methodology applies to all departments and functions of **[Organization Name]**, regardless of geographical location. It includes the identification, assessment, treatment, monitoring, and communication of all risks that may affect the achievement of the Organization's objectives. More specifically, the scope covers:
• All critical activities, information systems, infrastructures, assets, and personnel required for the uninterrupted and secure operation of [Organization Name].
• All Organizational units, departments, and staff involved in risk-related decision-making processes.
• Third-party suppliers and partners who handle or process sensitive data or provide critical services.
• Issues related to compliance with regulatory requirements.

2. Risk Management Policy

[Organization Name] maintains a risk management methodology (see Annex A), which includes the process for managing information and network security risks, defines the criteria for analysing the likelihood and impact of risks, and sets out the risk treatment strategy (reduction, transfer, avoidance, or acceptance) in line with the risk appetite of [Organization Name]. The methodology is applied at least annually. It is agreed and supported by Top Management and other relevant stakeholders within [Organization Name]. In particular:

- Clear roles, responsibilities, and criteria have been defined for carrying out risk management, as well as the related records that must be maintained.
- Risk acceptance criteria have been defined, which take into account the Organization's objectives, operating context, and strategy.
- [Organization Name] records the results of the information and network security risk management process and provides these results to the Competent Authorities annually or upon request.
- Identified risks are prioritized according to the impact they may have on [Organization Name] in terms of the confidentiality, integrity, and availability of the affected assets.

- The methodology follows best practices and consists of distinct phases and detailed steps (context establishment, risk assessment – including risk identification, risk analysis, and risk evaluation – risk

© CYberSynchorny, 2024

treatment, risk recording and reporting, communication, monitoring, and review) to enable the effective conduct of risk assessment exercises.
- Where possible, [Organization Name] establishes and monitors specific performance indicators related to risk management.
- Where applicable, the methodology should follow the wider Enterprise Risk Management (ERM) methodology and feed into it based on its results.
- It is recommended that [Organization Name] appoints a person responsible for the overall management and monitoring of the risk management methodology.
- [Organization Name] must inform all involved parties (internal and/or external to [Organization Name]) whose activities are related to the Organization's risks, about the risk management methodology.

2.1 Asset Inventory

Within the risk management methodology, the identification of Assets must first be carried out by creating an inventory of systems, processes, and other important resources within [Organization Name], and by recording the dependencies and interdependencies between these assets, systems, and processes. This is done to clearly describe the context/environment in which the risk assessment will be performed. A clear definition of the context allows for better identification of risks.

Examples of Assets are included in Annex B of this document.

The purpose of the Asset Inventory is the continuous monitoring of the status and condition of the assets/equipment of networks, information systems, and essential services in terms of their operational capability and potential failures, as well as the application of any policies related to each asset type included in the inventory.

A key part of the risk assessment process is determining the value of an asset so that the impact of its loss is known. The absence of a defined asset value makes it more difficult to calculate the risks associated with that asset.

For more information, please refer to the "Asset Management Policy".

2.2 Risk Register

[Organization Name] maintains, and regularly updates, a register of threats, vulnerabilities, and risks for each asset, including threats originating from insiders, with the aim of effectively identifying, recording, and monitoring risks, in accordance with international best practices.

For each identified risk, there is at least one designated risk owner.

The risk register must include risks arising from:

- the human factor
- accidental or unlawful destruction
- loss
- alteration
- unauthorized disclosure of, or access to, information that is transmitted, stored, or otherwise processed
- other risks that could potentially affect essential economic and social functions
- threats such as remote spying, theft of equipment, theft of information or media, retrieval of recycled or discarded media, data input from untrustworthy sources, incorrect use of devices, illegal processing of data, sending or distributing malware, abuse of rights
- corresponding weaknesses such as insufficient staffing resources, staff acting with conflict of interest / lack of segregation of duties, lack of monitoring and oversight, partially defined policies, inability to enforce policies and procedures through technical measures, etc.

© CYberSynchorny, 2024

Risks must cover all possible categories of risk sources, regardless of whether they are under the control of [Organization Name]. In particular, for complex and critical risk scenarios, the methodology should be applied iteratively, initially at a high level and subsequently in more detail (drilling down), until the correct root cause is identified.

Where assumptions and groupings have been made, relevant documentation must exist showing how these assumptions and groupings arose and confirming that they are aligned with the broader operating context of [Organization Name].

If threats, vulnerabilities, or risks are identified as not applicable to the current environment of [Organization Name], the stakeholders must update the relevant register, indicating that the corresponding entry is no longer active, for historical purposes.

The threat, vulnerability, and risk register must be updated, taking into account information from the vulnerability recording and reporting process.

The identification of threats, vulnerabilities, and risks to which [Organization Name] is exposed must be carried out with the participation of as many internal stakeholders as possible.

It is recommended that [Organization Name] has a documented procedure, communicated to staff, for the ad-hoc reporting by personnel of identified threats, vulnerabilities, and risks to which [Organization Name] is exposed.

Regular completeness checks of the threat, vulnerability, and risk register must be carried out against authoritative international sources.

2.3 Risk Analysis and Evaluation

Risk analysis and evaluation are essential components of [Organization Name]'s risk management framework. This process includes identifying, assessing, and prioritizing risks based on their likelihood and potential impacts on assets, in relation to the confidentiality, integrity, availability, and authenticity of information and associated functions.

[Organization Name] carries out an analysis of information security risks related to its assets, taking into account different likelihood levels and impact scores.

Each risk must be identified and scored in order to assess the appropriate mitigation strategy.

The results of the risk analysis and evaluation must be recorded in the threat, vulnerability, and risk register maintained by [Organization Name].

Appropriate and adequate strategies must be defined for treating the analysed risks, including measures for preventing, detecting, and monitoring attacks by insiders – whether due to ignorance, negligence, or malicious or professional intent.

In assessing likelihood and associated impact, both independent and dependent events must be taken into account.

It is recommended that methods and forecasts are implemented to determine cascading risks and their impacts.

The analysis of risks to which [Organization Name] is exposed must be carried out with the participation of as many internal stakeholders as possible.

[Organization Name] must have a documented procedure, known to staff, for informing the responsible personnel in case an error or omission in the risk analysis is identified.

In determining the likelihood and impact of identified risks, any implemented controls (where they exist) must be taken into account.

© CYberSynchorny, 2024

The potential and selected strategies must be periodically reviewed by appropriately authorized stakeholders to determine whether they remain appropriate and effective for managing the respective risks for [Organization Name]. Changes related to technology, services, or new strategic partnerships must also result in a review of related strategies and decisions.

The owner of each risk must give their approval regarding the acceptance of the residual risk and the selected risk treatment strategy.

2.4 Risk Treatment Plans

[Organization Name] defines, through the implementation of specific plans, the actions required to treat identified risks, ensuring that their management is aligned with Organizational objectives and other compliance requirements. This document describes in detail the selected risk treatment options — such as mitigation, acceptance, transfer, or avoidance — together with assigned responsibilities, timelines, and required resources. Through the systematic implementation of risk treatment measures, Organizations can strengthen resilience, maintain operational continuity, and meet regulatory obligations.

To this end:

- [Organization Name] defines appropriate and sufficient risk treatment measures as part of the implementation of the risk treatment strategy defined in the risk assessment process, taking into account preventive measures, detection measures, and response measures from an administrative, technological, and physical perspective, in order to ensure, where appropriate, a multi-layered defence.
- Risk treatment plans take into account the security measures described in the relevant legislation.
- Risk treatment actions are recorded in a relevant log, which includes a description of the measures taken, their duration/validity, the person responsible for each security measure, the resources required, how the effectiveness of the actions will be tested, and the residual level of risk after the implementation of the actions.
- The outcome of risk treatment is recorded in [Organization Name]'s risk treatment plan.
- Risk treatment plans must be monitored in order to verify the effectiveness of the risk treatment measures implemented by [Organization Name]. The timeframe within which the Organization must implement the relevant actions is determined according to the criticality of the risk, as set out in the relevant procedure.
- To assess the completeness of the selected measures, regular comparison must be made with structured control sets (e.g. ISO 27002, ISO 27001 Annex A, ISO 27017, ISO 27011, etc.). If a control that can be implemented is identified, [Organization Name] must carry out the corresponding assessment by following the risk management steps, limited to the risks that this specific control can address.

Documents related to Risk Management must be reviewed and revised at planned regular intervals, at least annually, or in the event of significant changes in [Organization Name]'s environment, in order to ensure alignment with evolving risks and Organizational changes.

It is additionally recommended that they be re-evaluated in the context of recommendations arising from internal audits, in combination with annual risk assessments or other compliance audits or following the introduction of new regulations or relevant standards.

Finally, it is recommended that they be reviewed after significant security incidents or breaches, as well as after changes in the cybersecurity landscape due to emerging threats, geopolitical developments, or technological advances.

© CYberSynchorny, 2024

4. References

Category	ID	Measure	Measure Objective
Risk Management	RM1	Methodology	To establish a risk management methodology that reflects the Organization's risk assessment process, risk analysis criteria, risk acceptance criteria, and risk appetite policy.
Risk Management	RM2	Context	To prepare an inventory of assets, systems, and processes within the Organization.
Risk Management	RM3	Risk Identification	To identify threats, vulnerabilities, and risks to which the Organization's assets, systems, and processes are exposed.
Risk Management	RM4	Risk Analysis	To analyse information security risks in the context of assets based on different likelihood and impact levels.
Risk Management	RM5	Risk Evaluation	To evaluate information security risks based on the Organization's risk appetite and to define appropriate risk treatment strategies.
Risk Management	RM6	Risk Treatment	To define actions for treating information security risks.
Human Resources Security	HRS5	Protection from Insider Threats	To ensure protection against network and information security threats originating from within the Organization.

© CYberSynchorny, 2024

5. ANNEX A – Risk Management Methodology

5.1 Definition of Scope

As a first step, the scope of the risk assessment is identified and defined. Typically, this includes the departments of [Organization Name] and other business units of [Organization Name] that will be covered, based on business activities, geography, Organizational structure, or other relevant criteria.

5.2 Purpose of Risk Assessment

The purpose and reasons for conducting a risk assessment are to help [Organization Name] understand the extent of risk exposure and to manage that exposure. Additionally, by mitigating the risks highlighted during the assessment, the Organization will prevent and reduce costly security incidents and data breaches and avoid regulatory and compliance issues.

5.3 Definition of Roles and Responsibilities

Table 8 Definition of Roles and Responsibilities

Role	Responsibility
Network and Information Systems Security Officer	• Maintains an up-to-date information security risk register and risk treatment plan on behalf of the Organization.
Risk owner	• An appropriate manager shall be appointed as the owner for each identified risk. • Provides assurance that the risk is accurately assessed. • Provides assurance that appropriate risk treatment measures are proposed. • Ensures that the risk is communicated to the relevant parties. • Is responsible for ensuring that the implementation of risk treatment measures is completed within the agreed timelines. • Communicates updates as required.
Senior Management	• Responsible for reviewing information security risks that are considered significant or critical, to ensure that appropriate treatment measures are applied. • Responsible for ensuring that the necessary resources are available to support these activities.
Employees of [Organization Name]	• Are required to notify the Information Security Officer of any issues they become aware of that may constitute, indicate, or cause an information security risk. • Are required to support the implementation of all risk treatment measures deemed necessary by the Risk Owner or Senior Management.

Note: Each Organization may define only the roles that align with its needs and structure and may remove or modify roles that do not apply. Additionally, depending on the size of the Organization, it may not be feasible to assign separate individuals to each role. In such cases, the Organization may assign more than one role to the same individual, provided that no conflict of interest arises between these roles.

© CYberSynchorny, 2024

5.4 Identification of Assets

Assets are identified by creating an inventory of systems, processes, and other important resources within [Organization Name], as described in the Asset Management Policy.

The identification of potential threats is a key component of risk methodologies, with the objective of identifying risk sources that could exploit vulnerabilities and affect the Organization's assets. For each asset, threats that can reasonably be expected to apply and that have the potential to cause harm are identified. Threats may be internal or external and may arise from cyber-attacks, system failures, human error, natural disasters, or regulatory changes.

An initial list of typical threats is included in Annex C of this document and in other relevant standards such as ISO 27005, etc.

5.5 Identification of Potential Vulnerabilities

This process includes examining technical, operational, and Organizational aspects to identify gaps in security controls, system configurations, processes, and human factors. For each asset, the circumstances or characteristics that could be exploited by a specific threat are identified and described. A vulnerability does not cause damage by itself, but its presence may allow a threat event to harm an asset.

An initial list of typical vulnerabilities is included in Annex D of this document.

5.6 Identification of Potential Risks

The identification of potential risks involves analysing the interaction between threats and vulnerabilities to determine the potential negative impacts on essential functions and services provided by the Organization. Risks arise when a threat exploits a vulnerability. At this stage, risks arising from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, information that is transmitted, stored, or otherwise processed are taken into account.

5.7 Identification of Types of Risks

The types of risk that arise for each identified threat against each asset must be considered during the risk evaluation. These may include loss of confidentiality, integrity, availability, or authenticity of any asset. Depending on the nature of the asset, consequences may take many forms, including interruption or degradation of services, reduction in service quality, loss of business, reputational damage, or financial penalties, including fines.

Examples:

- **Confidentiality risks** – Threats that compromise the confidentiality of sensitive data by allowing unauthorized access.
- Examples: Data breaches, insider threats, weak encryption, insecure storage.
- **Integrity risks** – Risks that affect the accuracy, consistency, and reliability of data and systems. Examples: Data corruption, unauthorized modifications, malware (e.g. ransomware), software supply chain attacks.
- **Availability risks** – Threats that disrupt access to systems, networks, or services, leading to downtime. Examples: DDoS attacks, system failures, ransomware, hardware malfunctions, insufficient redundancy.
- **Authenticity risks** – Risks that hinder the authenticity and traceability of information, logging and auditing capabilities, and enforcement of security policies. Examples: Inadequate logging practices, lack of access controls, weak authentication mechanisms, insufficient forensic capabilities.

© CYberSynchorny, 2024

5.8 Identification of Risk Owners

The Organization identifies cybersecurity risk owners to ensure accountability and effective risk mitigation. A risk owner is the person or group responsible for managing a specific risk, overseeing treatment and mitigation actions, and ensuring compliance with security policies.

5.9 Identification of Existing Security Controls

Existing security controls are identified and assessed in order to determine whether they are effective. Criteria includes whether the control reduces the likelihood and/or impact of a threat event. The results of this assessment lead to a conclusion that control is effective, ineffective, or redundant.

5.10 Risk Analysis Criteria

To assess the risk for an asset and determine the appropriate treatment, the Organization examines threats and defines the factors used for assessing and prioritizing cybersecurity risks. A five-point scale is used to describe the likelihood that a risk will occur and the impact it is likely to have.

5.10.1 Risk Analysis Criteria

A five-point scale from 1 (Very Unlikely) to 5 (Certain) is used:

Table 9 Risk Analysis Criteria

Likelihood	Description	Summary
1	Very Unlikely	Has never occurred before and there is no reason to believe it is more likely now.
2	Unlikely	There is a possibility it may occur, but it is more likely that it will not.
3	Possible	On balance, the risk is more likely to occur than not.
4	Very Likely	It would be surprising if the risk did not occur, based on past frequency or current conditions.
5	Certain	It is already occurring regularly or there is reason to believe it is almost imminent.

5.10.2 Impact Criteria

Impact criteria are used to determine the extent of the consequences that may arise from a cybersecurity risk. They help assess risk severity across the following areas:

- Operational impact
- Financial cost
- Reputational damage / Loss of trust
- Legal, contractual, and Organizational compliance
- Health and safety

The impact level is assessed based on how much each of these areas would be affected if the confidentiality, integrity, availability, or authenticity of an asset were compromised. The highest of these impact ratings are used as the asset's criticality rating and subsequently in the risk assessment.

© CYberSynchorny, 2024

Detailed risk impact criteria are provided in Annex E of this document.

Table 10 Impact Criteria

Impact level		Impact Areas				
Impact Assessment	**General Description**	**Operational Impact**	**Financial Cost**	**Reputational / Trust Impact**	**Contractual & Regulatory Compliance**	**Health & Safety**
1	Negligible	No impact	Very little or none	No damage to reputation	No legal or regulatory impact	No impact on health and safety
2	Minor	Some localized disruption to normal business operations	Partial	Limited impact, easy to restore	Minor violation with possibility of correction	Small risk, no long-term consequences
3	Moderate	Able to deliver product/service with some difficulty	Undesirable but tolerable	Media coverage, some loss of trust	Violation that may lead to fines or investigations	Possibility of injury or significant stress
4	High	Business operations significantly crippled in key areas	Severe impact on revenue and/or profit	Extensive publicity, severe reduction in trust	Serious violation likely to lead to legal actions	Serious impact on personal safety
5	Very high	Out of operation, no service to customers	Unsustainable debt: Organization may cease to operate	Catastrophic damage to reputation, loss of key customers/partners	Legal sanctions affecting the Organization's ability to operate	Immediate danger to life or severe physical harm

The impact is assessed based on the categories above, as well as the level to which these areas would be affected if the confidentiality, integrity, availability, and authenticity of an asset were compromised (Impact Assessment).

The highest score across confidentiality, integrity, availability, and authenticity determines the criticality of each asset, which becomes the highest impact score. This highest impact score is then used in the risk assessment.

The overall impact level is scored by combining all five impact domains and the potential effect on the asset if any of the core security properties (CIAA) are compromised.

The detailed impact criteria are included in **Annex E** of this document.

6. Risk Scoring Criteria

© CYberSynchorny, 2024

The risk classification used is based on the score obtained by multiplying the likelihood of the risk occurring by the potential impact. Both scales range from 1 to 5 ; therefore the minimum possible score is 1, and the maximum is 25, as shown in the risk heat map above. The heat map is a visual tool used in risk management to assess and communicate the likelihood and impact of identified risks in an intuitive and easily understandable way. It displays risks in a matrix—typically with likelihood on one axis and impact on the other—using color coding to indicate the severity of each risk and to support the prioritisation of risks based on their probability of occurrence and their potential consequences for the Organization.

The risk heat map presented below illustrates the scales and enables us to prioritise the Organization's risks so that they can be addressed more effectively.

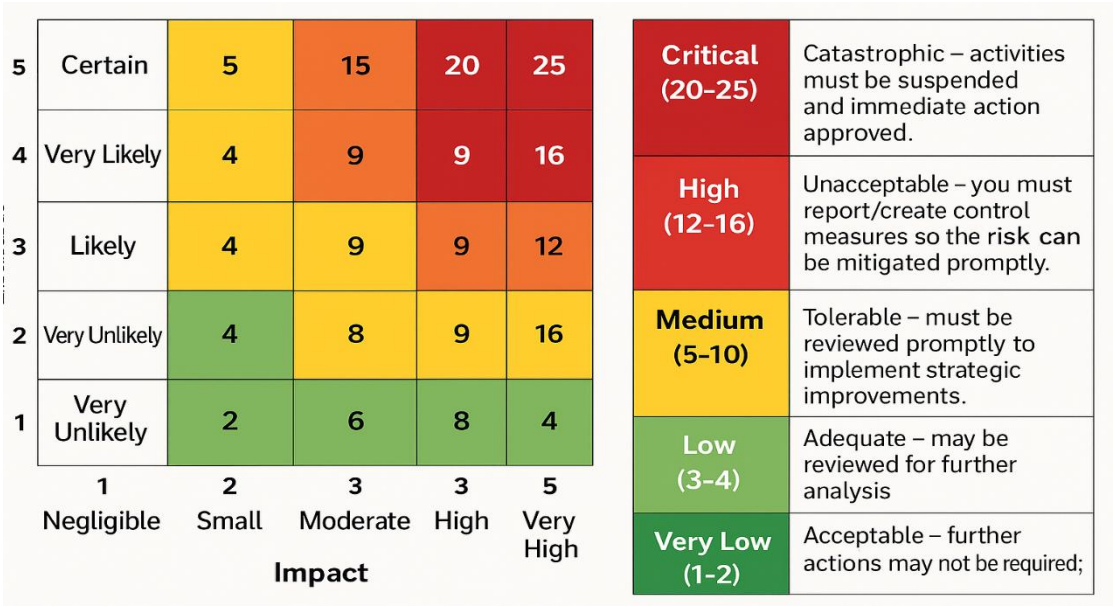

Figure 3 Risk Scoring Criteria

The matrix is divided into segments along the X-axis: Likelihood and Y-axis: Impact (e.g., Very Low to Critical).

The matrix is split into sections based on these categories, resulting in cells that represent combinations of likelihood and impact levels. The intersection of likelihood and impact provides the overall risk score, which determines the risk level classification.

Each risk will be assigned a classification based on its score as follows:

- CRITICAL – 20 to 25 (inclusive)
- HIGH – 12 to 16 (inclusive)
- MEDIUM – 5 to 10 (inclusive)
- LOW – 3 to 4 (inclusive)
- VERY LOW – 1 to 2 (inclusive)

Where:

Critical: Catastrophic – activities must be halted and immediate action must be approved.

High: Unacceptable – controls must be created or updated to mitigate the risk.

Medium: Tolerable – must be reviewed in due time to implement improvement strategies.

Low: Adequate – may be considered for further analysis.

© CYberSynchorny, 2024

Very Low: Acceptable – no further actions may be required, maintaining existing control measures is encouraged.

The rationale behind the likelihood and impact ratings assigned will be documented so that they can be reassessed at a later stage to determine whether they have changed significantly. This also helps ensure consistency and repeatability in risk assessments.

The matrix above shows the risk classifications, where green indicates an acceptable threshold, as the likelihood and/or impact is minimal.

Orange indicates a medium/moderate risk threshold, where both the risk and its impact are higher; therefore, addressing these risks is more important than those in the green range.

The red area indicates high-priority risks, as both the impact and likelihood are relatively high. The measures to mitigate these risks must be prioritised, and if they cannot be reduced, appropriate countermeasures must be in place.

The overall intention of the risk assessment and the proposed treatments is to reduce the risk classifications to a minimum acceptable level—that is, to reduce Very High, High, and Medium risks to Low or Very Low wherever possible. This is not always achievable, as sometimes, although the score decreases, the risk remains within the same classification. For example, a reduction in score from 16 to 10 means the risk still remains at a High level. The Organization may choose to accept these risks even though they remain high.

The priorities of the items in an action plan are determined by the highest priority level among the risks being addressed. For example, if three risks are being treated by a single action—one Medium and two Low—then the priority of that action will be Medium.

7. Analysis / Evaluation Procedure

7.1 Information Gathering

The Network and Information Systems Security Officer collects a substantial amount of information to ensure that the risk analysis is valuable and comprehensive. This information is obtained through the following available sources:

- Interviews with process owners
- Interviews with asset owners
- Interviews with application developers
- Interviews with security personnel
- Interviews with external security specialists
- Security incident logs
- Analysis of incidents occurring in other Organizations
- Previous risk assessments
- Etc.

7.2 Likelihood Assessment

An assessment of the likelihood of a threat occurring must be conducted. This should consider whether the threat has occurred in the past within the Organization or in similar Organizations in the same sector or location, as well as whether there is sufficient motivation, opportunity, and capability for the threat to materialise.

© CYberSynchorny, 2024

7.3 Impact Assessment

Finally, an assessment must be made of the impact that the loss of confidentiality, integrity, availability, or authenticity of an asset could have on the Organization. The method for evaluating impact is described in the "Risk Assessment Criteria" section of this procedure.

Risk Evaluation / Analysis is carried out at regular intervals.

8. Risk Treatment

For risks that exceed the Organization's acceptance threshold (based on the defined risk acceptance criteria), the available treatment options will be evaluated.

8.1. Risk Acceptance Criteria

This section defines the method the Organization uses to determine risk acceptance.

Risk acceptance is defined as a decision by which the Organization considers the presence of a risk to be acceptable and determines that no reduction or mitigation is required.

The Organization chooses to accept a risk based on the following conditions:

- The cost of mitigating the risk is greater than the value of the asset being protected
- The impact of compromise is low, or the value/classification of the asset is low

Risk Acceptance Framework:

Table 11 Risk Acceptance Criteria

Risk Level	**Level Required for Acceptance**
Very Low	Network and Information Systems Security Officer
Low	Network and Information Systems Security Officer
Medium	Network and Information Systems Security Officer
High	Director or Head of Operations (CEO or COO)
Very High	Board of Directors or other Senior Management body (e.g., Information Security Steering Committee)

When the Organization accepts a risk, it must still review it at least annually. Reasons for reviewing an accepted risk include:

- The value of the asset may have changed during the year
- The business value associated with the asset may have changed
- The strength of threats may have changed, resulting in a higher risk score
- The cost of mitigation may have changed, increasing the feasibility of mitigation or risk transfer

© CYberSynchorny, 2024

8.2. Risk Appetite

Risk Appetite: The level of risk the Organization is willing to accept in pursuit of its mission, strategy, and objectives before action is required.

Risk Capacity: The objective amount of loss the Organization can tolerate without jeopardising its continued operation.

8.3. Risk Treatment Strategies

The following strategies may be applied to address identified risks deemed unacceptable:

Reduction / Mitigation: Implement appropriate controls to reduce the likelihood and/or impact of the risk

Avoidance: Discontinue the activity associated with the risk

Transfer: Transfer the risk to another party, e.g., an insurer or supplier

Judgement will be exercised when selecting a course of action, based on a sound understanding of the circumstances surrounding the risk, such as:

- Business strategy
- Regulatory and legal considerations
- Technical considerations
- Commercial and contractual issues

The risk manager ensures that all relevant parties with an interest in or influence over the treatment of the risk are consulted.

8.4. Selection of Risk Treatment Measures

The document will be used as the starting point for determining the appropriate and sufficient measures needed to address the risks identified during the risk assessment.

When determining the measures, the Organization considers preventive, detective, and corrective controls. These measures may be categorised as administrative, Organizational, technological, or physical security measures.

If the measures defined in Annex III do not meet all requirements, additional measures may be applied.

8.5. Implementation Plan for Network and Information Security Measures (Action Plan)

Upon completion of the risk assessment, a detailed action plan must be developed for the implementation of information security measures as part of the overall risk treatment plan. This includes timelines, resource allocation, and role assignment. The action plan forms part of the wider risk management process and ensures that the Organization's information security posture aligns with identified risks and vulnerabilities.

8.5.1. Actions to be Included in the Action Plan

1. Develop a list of actions for each risk treatment strategy.

2. For each identified security measure, the following must be determined:

    I. What actions are required? (e.g., firewall installation, employee training)
    II. Who is responsible for implementation? (e.g., IT department, HR department, external partners)

© CYberSynchorny, 2024

III. What is the implementation timeline? (e.g., within 3 months)
IV. What resources are required? (e.g., budget for software/hardware acquisition, training costs, service procurement costs)
V. How will the action be validated? (e.g., penetration testing, vulnerability assessments)

8.5.2. Resource Requirements

For resource and budget allocation:

• Estimate the cost of required tools, technologies, training, and third-party services

• Allocate human resources with appropriate skills to implement the security measures

• Ensure necessary senior management support for ongoing funding, including long-term maintenance and monitoring of the implemented measures

8.5.3. Assignment of Roles and Responsibilities

To ensure accountability for each action:

• Appoint an action owner or a risk management team responsible for oversight

• Assign specialised tasks to security experts, IT staff, or external consultants

• Define a reporting and escalation procedure in case of issues

8.5.4. Monitoring Effectiveness and Reporting

After the implementation of the security measures, continuous monitoring and control are essential to ensure their effectiveness and to minimise residual risks. For this purpose, the Organization should:

• Consider the deployment of security monitoring tools (e.g., Security Information and Event Management – SIEM systems).

• Conduct regular vulnerability assessments, penetration testing, and IT security audits.

• Monitor the performance of the implemented controls to verify their proper operation.

8.5.5. Evaluation and Review of the Risk Treatment Plan

[Organization Name] is responsible for evaluating the effectiveness of the implementation.

[Organization Name] must conduct regular reviews and updates of the risk treatment plan to ensure that it remains effective in addressing new, evolving, and emerging risks and threats, as well as other operational needs.

Additionally, feedback should be provided to relevant stakeholders, and the plan should be adjusted as necessary to remain aligned with Organizational objectives.

8.5.6. Reporting and Continuous Improvement

A culture of continuous improvement should be promoted by enhancing policies, procedures, and technical solutions based on feedback and emerging threat landscape trends. This is achieved through regular reporting to the Organization's senior management on risk treatment progress, the implementation of security measures, and ongoing improvement initiatives, ensuring long-term security resilience.

8.6. Statement of Applicability

The Statement of Applicability will define the selected controls and will detail those that have been implemented, including descriptions of how they were applied and other supporting information.

© CYberSynchorny, 2024

In rare cases, certain controls may be excluded or deemed not applicable to the Organization. In such cases, the Statement of Applicability must document and justify the reasons for exclusion.

9. Risk Assessment and Treatment Procedure

9.1. Process Flow Diagram

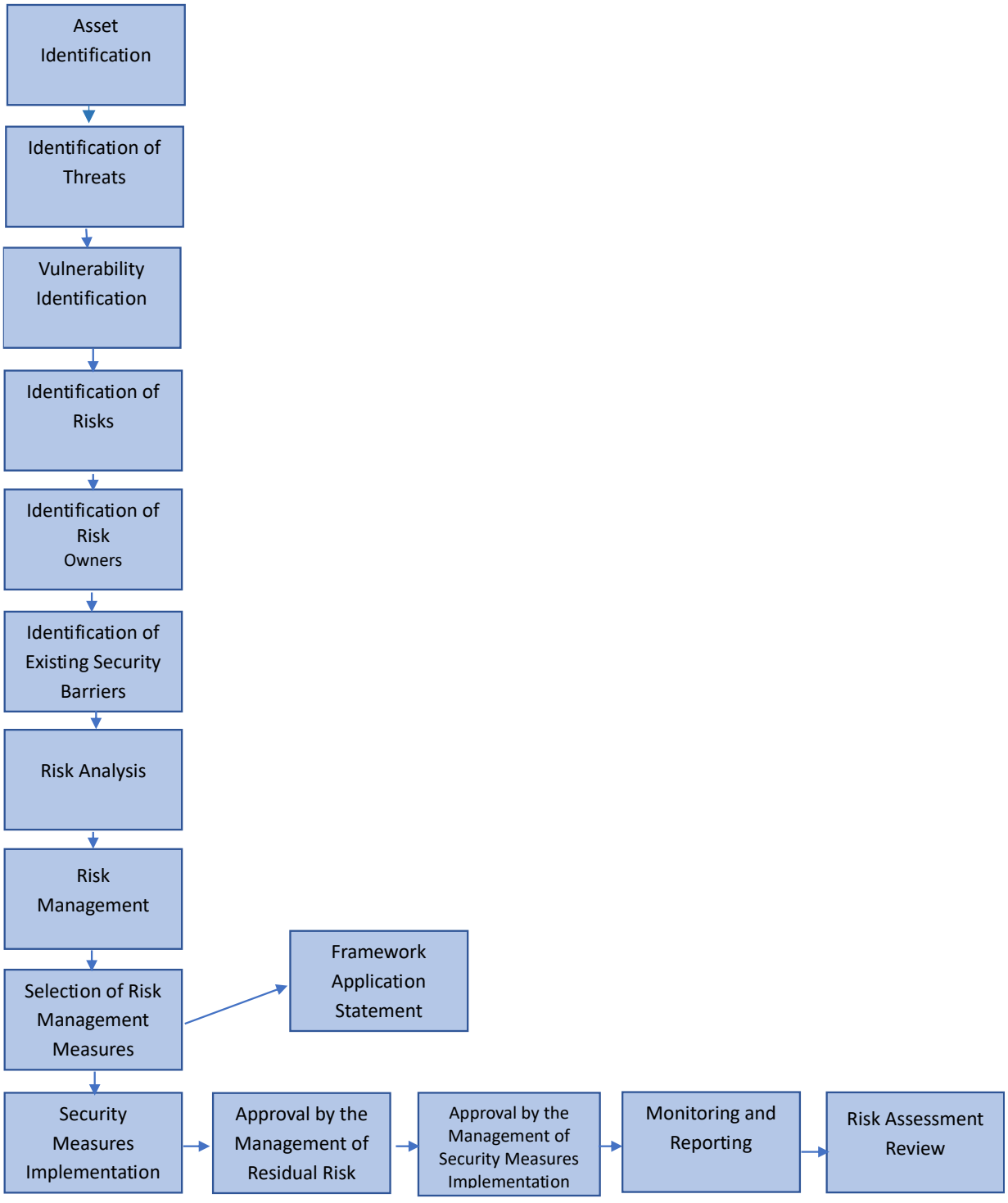

Figure 4 Process Flow Diagram

© CYberSynchorny, 2024

Annex B – Asset Inventory

Table 12 Asset Inventory

Asset Category	Sub-Category	Asset Item
Asset Category	Sub-Category	Asset Item
Information	Corporate	Budgets
		Corporate plans
		Corporate policies
	Health Services	Patient records – names, addresses, contacts
	Human Resources	Patient correspondence and complaints
		Employee records – address, Date of Birth, Insurance Numbers
		Employee expense claims
		Payroll information, including bank details
		Training records
		Recruitment information
		Leave / security clearance information
		Employee complaints / disciplinary records
		Workplace sickness / occupational health records
	Finance	Employment contract
		Accounting records – invoices, statements
	Procurement	Business bank account details
		Supplier contact details
		Procurement plans
	Legal	Commercial terms
		Supplier contracts
		Patient consent forms (overnight stay)
		Property leases
		Credit agreements
	Operations	Manuals for proper use of medical equipment
		Product specifications and material invoices
		Process and procedural documentation
		Organization-specific intellectual property
		Resource plans
	Audit & Compliance	Internal audit records
		External audit records
		Risk assessments
		Email
		Accounting
		Payroll system
		Custom software
		Intranet

© CYberSynchorny, 2024

Asset Category	Sub-Category	Asset Item
Software	—	Website
		Design software
		Office applications
		Marketing software
		Industry-specific applications
Equipment	—	Computer servers
		Networking equipment
		Personal computers
		Portable devices
		Mobile phones
Buildings / Location		
Services	—	Server rooms, including air-conditioning and power units
		Machinery
		Stock
		Vehicles
		Electricity supply
People	Key Resources	Water
		Network services
		Telephone services
		Owner / CEO
		Directors
Equipment	—	Knowledge holders
		Computer servers
		Networking equipment
		Personal computers
Other		

© CYberSynchorny, 2024

Annex C – Threat Catalogue

The following catalogue can be used as a starting point for creating a relevant list of threats that may apply to the information assets identified in the inventory.

Table 13 Threat Catalogue

Threat Category	Threat	Example
Human	Malicious outsider	Someone launches a denial-of-service attack on your e-commerce website
	Malicious insider	An employee or trusted third party gains access to information in an unauthorized way within your network
	Loss of key personnel	One or more individuals with essential skills or knowledge become unavailable, possibly due to prolonged illness
	Human error	An employee accidentally deletes the customer database
	Accidental loss	A manager loses a memory stick containing bank customer details
Physical	Fire	Your headquarters burns down due to an electrical fault
	Flood	A nearby river overflows and your headquarters becomes severely flooded
	Severe weather	No one can enter the office due to extreme weather conditions
	Earthquake	An earthquake affects the area of your headquarters and damages all your servers
	Lightning	All your servers are destroyed by a lightning strike on the data centre building
Technical	Hardware failure	A critical server experiences processor failure
	Software failure	Your financial system processes invoices incorrectly due to a software bug
	Virus / malicious code	A virus spreads across your network, blocking access to your data
Physical (Security)	Sabotage	A disgruntled former employee destroys equipment in your server room
	Theft	You arrive Monday morning to find that all your computers have been stolen
	Arson	Someone with a grudge against your Organization sets a fire during the night
Environmental	Hazardous waste incident	A truck carrying hazardous waste has an accident outside your office
	Power outage	The substation supplying your area has failed
	Gas supply failure	A suspected gas leak results in all supplies being shut off
Operational	Process failure	A new data transfer process does not handle unexpected scenarios, causing data loss or incorrect transmission
	Crime	A crime occurs in or near your office and the area is sealed off by the police

© CYberSynchorny, 2024

Annex D – Vulnerability Catalogue

Table 14 Vulnerability Catalogue

Type	Example Vulnerabilities	Example Threats
Hardware	Inadequate maintenance / defective installation of storage media	Breach of maintenance information system
	Lack of periodic replacement systems	Destruction of equipment or media
	Sensitivity to humidity, dust, pollution	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of effective configuration change control	User error
	Sensitivity to voltage fluctuations	Power loss
	Sensitivity to temperature fluctuations	Weather phenomenon
	Unprotected storage area	Theft of media or documents
	Lack of care during disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
	Known software defects	Abuse of rights
	No “logout” when leaving the workstation	Abuse of rights
	Disposal or reuse of storage media without proper wiping	Abuse of rights
	Lack of audit trails	Abuse of rights
	Incorrect assignment of access rights	Abuse of rights
	Widely distributed software	Data corruption
	Application programs run on outdated or wrong data	Data corruption
	Complex user interface environment	User error
	Lack of documentation	User error
	Incorrect configuration settings	User error
	Incorrect dates	User error
	Lack of identification and authentication mechanisms (e.g., user authentication)	Forged rights
	Unprotected password tables	Forged rights
	Poor password management	Forged rights
	No ability to disable unused services	Illegal data processing
	Immature or new software	Software malfunction
	Vague or incomplete specifications for programmers	Software malfunction

© CYberSynchorny, 2024

	Lack of effective change control	Software malfunction
	Uncontrolled downloading and use of software	Software tampering
	Lack of backups	Software tampering
	Lack of physical protection for building, doors, windows	Theft of media or documents
	No generation of management reports	Unauthorized equipment use
	End of Life / End of Support	Breach of system maintainability
Network	Lack of message sending/receiving proof	Repudiation of actions
	Unprotected communication lines	Eavesdropping
	Unprotected sensitive traffic	Eavesdropping
	Poor cable joints	Telecommunications equipment failure
	Single point of failure	Telecommunications equipment failure
	Lack of authentication of sender and receiver	Forged rights
	Insecure network architecture	Remote espionage
	Clear-text password transmission	Remote espionage
	Inadequate network management (routing resilience)	System overload
	Unprotected public network connections	Unauthorized equipment use
Personnel	Absence of staff	Violation of staff availability
	Inadequate recruitment procedures	Equipment or media destruction
	Insufficient security training	User error
	Incorrect use of software and hardware	User error
	Lack of security awareness	User error
	Lack of monitoring mechanisms	Illegal data processing
	Unsupervised external staff or cleaners	Theft of media or documents
	Lack of policies for correct use of telecommunications and messaging	Unauthorized equipment use
Location	Inadequate use of physical access controls for buildings and rooms	Equipment or media destruction
	Location in flood-prone area	Flooding
	Unstable electrical grid	Power loss
	Lack of physical protection of building, doors, windows	Equipment theft
Organization	Lack of formal user registration and deregistration processes	Abuse of rights
	Lack of access rights review processes (supervision)	Abuse of rights

© CYberSynchorny, 2024

	Lack of or insufficient security clauses in customer or third-party contracts	Abuse of rights
	No monitoring process for information processing facilities	Abuse of rights
	Lack of regular audits (supervision)	Abuse of rights
	Lack of risk identification and assessment procedures	Abuse of rights
	Lack of reporting of errors logged by administrator/operator logs	Abuse of rights
	Inadequate maintenance service response	Violation of system maintainability
	Lack of or insufficient Service Level Agreement	Violation of system maintainability
	Lack of change control process	Violation of system maintainability
	No formal ISMS documentation control process	Data alteration
	No formal process for supervising ISMS records	Data alteration
	No formal process for approving publicly available information	Unreliable data sources
	Inadequate allocation of information security responsibilities	Repudiation of actions
	Lack of business continuity plans	Equipment failure
	No email usage policy	User error
	Lack of procedures for software installation in operating systems	User error
	Lack of administrator/operator logs	User error
	Lack of procedures for classified information handling	User error
	Lack of information security responsibilities in job descriptions	User error
	Lack of or insufficient security clauses in employee contracts	Illegal data processing
	No disciplinary process for information security incidents	Equipment theft
	No formal mobile computing policy	Equipment theft
	No control of off-premise assets	Equipment theft
	Inadequate “clean desk & clean screen” policy	Theft of media or documents
	No facility authorization for information processing	Theft of media or documents
	Lack of monitoring mechanisms for security breaches	Theft of media or documents
	No regular management reviews	Unauthorized equipment use
	Lack of procedures for reporting security weaknesses	Unauthorized equipment use
	Lack of compliance procedures for copyright	Use of pirated or counterfeit software

© CYberSynchorny, 2024

Annex E –Risk Impact Criteria

Table 15 Risk Impact

Impact Level		Impact Areas				
Impact Rating	**General Description**	**A1. Operational Impact**	**A2. Financial Cost**	**A3. Reputational Damage**	**A4. Legal, Contractual & Organizational Compliance**	**A5. Health & Safety**
5	Very High	**Complete operational shutdown, severe impact on the Organization or critical infrastructure. Recovery requires extensive restoration procedures. Examples: Organization unable to operate due to cyberattack (e.g., ransomware); compromise of critical infrastructure (electricity grid, healthcare, financial institutions).**	**Creates a viability and capital adequacy issue.**	**Loss of revenue / cost impact resulting in a viability and capital adequacy issue requiring Board and regulatory intervention.**	**All stakeholder groups are affected. Significant degradation of trust and reputation across all related groups (e.g., customers, prospects, regulators, third parties). Example: cyberattack leading to potential Organizational collapse.**	**Severe legal or regulatory obligations threaten the Organization's existence and its ability to continue providing services. Example: international data breach with high fines and legal action.**
4	High	**Significant disruption of critical functions, major impact on productivity and service delivery. Examples: inability to access core systems across large parts of the Organization; major cyberattack affecting critical data or services.**	**Financial results seriously affected across multiple business areas.**	**Financial outcomes or costs significantly impacted, affecting several departments; require Board involvement.**	**Multiple stakeholder groups affected. Severe degradation of trust among key groups (e.g., private customers, corporate clients). Example: data breach involving customer data.**	**Obligations requiring special handling beyond standard procedures. Failure to address root causes may lead to significant losses or escalate into a "Critical" issue. Example: personal data loss affecting thousands of citizens.**

© CYberSynchorny, 2024

3	Moderate	**Moderate disruption affecting specific users or departments. Partial productivity reduction. Examples: outage of a system affecting certain employee groups; limited email or ERP outage.**	**Unable to absorb cost within existing departmental budget; requires senior management approval.**	**Loss / cost cannot be covered by existing budget allocations.**	**A specific stakeholder group is affected. Noticeable trust degradation among a defined group (e.g., corporate clients). May escalate to "High" depending on group size.**	**Obligations handled via existing processes but may still cause losses (e.g., penalties) and may strain third-party relationships.**
2	Low	**Minor operational disruption; systems remain functional. Easy restoration with limited delay.**	**Handled within existing budget.**	**Loss / cost addressed through allocated annual budget funds.**	**Trust degradation limited to an individual entity only (e.g., one private or corporate customer).**	**Limited obligations handled via standard processes; losses are minimal (e.g., minor penalties).**
1	Negligible	**No operational impact. Critical processes unaffected.**	**No direct loss / cost.**	**No direct revenue loss or immediate cost to repair any damage.**	**No immediate reputational impact to any entity or group.**	**No legal or compliance obligations.**

© CYberSynchorny, 2024

4.4 Tool 4 - Asset Management Policy

[Organization Name]

ASSET MANAGEMENT POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
1.1 Purpose
1.2 Scope
2. Asset Management Policy
2.1 Asset Lifecycle Management
2.2 Asset Recording and Monitoring Policy
2.3 Definition of Recording and Monitoring Parameters
3. Secure Disposal or Reuse of Assets
4. Review
5. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

This document defines the indicative Policy Terms for the management of assets belonging to [Organization Name], with the aim of establishing guidelines for the appropriate protection of the Organization's assets.

This policy establishes a structured approach for managing assets throughout their lifecycle, safeguarding them from cyber-related security threats, and ensuring compliance with legal and regulatory requirements. By maintaining accurate records and applying controls, the policy supports the Organization's ability to identify, prevent, and respond to cybersecurity risks.

The objectives of the Policy are summarised as follows:

- To create and maintain an accurate inventory (asset register) of all information assets, including ownership, classification, and criticality.
- To define roles and responsibilities for managing and protecting assets.
- To assign an owner to each asset, responsible for ensuring its protection, proper operation, availability, integrity, and confidentiality.
- To ensure appropriate classification and handling of assets based on their information sensitivity and value.
- To minimise the risk of misuse, theft, or unauthorised access to assets through suitable controls and monitoring.
- To support incident response and recovery processes by providing clear tracking of assets.
- To align with applicable standards such as ISO 27001 and regulatory frameworks.

1.2 Scope

The Asset Management Policy aims to ensure the effective identification, classification, and protection of the assets of [Organization Name]. It applies to all assets owned, leased, or managed by the Organization, including personnel, hardware, software, cloud resources, data, processes, and any other intellectual property.

This Policy applies to all employees, contractors, and third parties who access these assets.

It covers all stages of the asset lifecycle—from acquisition and development to end-of-life and disposal—and applies to all locations of the Organization, including remote environments (e.g., cloud, DR) and third-party environments.

2. Asset Management Policy

2.1 Asset Lifecycle Management

- Asset lifecycle management includes the systematic management of the Organization's assets throughout their entire lifecycle. Therefore, [Organization Name] implements and maintains a process for managing and securing assets during their lifecycle (procurement, installation, maintenance, and disposal), defining responsible roles for its implementation.
- The level of security controls applied to each asset must be equal to or higher than the security controls applied to the data processed by the asset.
- Each asset must be labelled according to its classification level.
- [Organization Name] must specify asset security requirements before procurement.
- Minimum maintenance procedures must be defined based on asset criticality.

© CYberSynchorny, 2024

- At least annually, a review must be performed to determine whether the asset lifecycle management plan is implemented effectively and whether adequate resources (staff, tools, funding, etc.) are available.
- Before reuse or end-of-life, all data must be securely erased.
- The Organization maintains an asset inventory (register) to ensure a clear, accurate, and up-to-date record of all assets (hardware, software, information) kept internally or externally (e.g., at third parties).
- The inventory records dependencies and interdependencies between assets, systems, and processes to create an accurate depiction of the Organizational environment for risk assessment, in compliance with requirement [RM2] of Decision K.D.P. 389/2020.
- Each asset must have an assigned owner who may determine its criticality.
- The existence of an identified asset owner ensures proper, systematic, and secure management of the Organization's inventories. The owner must:
    - Have clearly defined responsibilities for maintaining, updating, and securing the inventory.
    - Be informed of changes in relevant policies or procedures.
    - Collaborate with other departments (e.g., IT) to apply required security measures.
    - Maintain administrative accountability even if tasks are delegated.
- The asset inventory must include, at a minimum, acceptable use, function, location, and asset dependencies, in line with [AM3] of Decision K.D.P. 389/2020.
- All assets must be identified, tracked, and inventoried, ideally through automated systems.
- The inventory must allow monitoring of assets requiring security controls, at least manually, according to [AM2] of Decision K.D.P. 389/2020.
- Where applicable, the Organization must maintain a blacklist of unauthorised applications and executable types.
- Automated identification outputs should be supplemented with process information to depict dependencies.
- The inventory must be updated regularly (at least annually) and include:
    - Information asset / IT system
    - Electronic / physical location
    - Asset owner
    - Applicable security level

Asset records are maintained within the "Asset-Based Risk Assessment Workbook."

2.2 Asset Recording and Monitoring Policy

[Organization Name] establishes, implements, and maintains monitoring capabilities for its assets, as required by [AM3] of Decision K.D.P. 389/2020, to detect anomalies in location, usage, or performance through monitoring algorithms and mechanisms.

2.3 Logging and Monitoring Parameters

[Organization Name] records and monitors security-related activity across all systems, and at a minimum, all critical assets. Requirements include:

• All assets must be synchronised to the same network time source using the Network Time Protocol (NTP).

• Log files must be adequately protected from unauthorised access, modification, or deletion.

•The management of logging and monitoring activities must be assigned to a subset of users with privileged accounts.

• Incident management and incident response procedures must be activated immediately when anomalies are detected during the monitoring of asset activities.

© CYberSynchorny, 2024

• Monitoring results (logs) must contain at least the following information:

– Date

– Time

– Involved assets (source and destination IP addresses)

– Log type

– Additional explanatory information

For each asset, the Organization must define:

- **Type of Monitoring:**

Definition of the monitoring type per asset (e.g., System, Security, Application).

Identification of specific monitoring parameters for each type (e.g., system events, security, applications).

- **Monitoring Scope:**

Definition of the scope of monitoring at the event level.

Logging of various event types (e.g., audit success, audit failure, login success, object access success, warning).

- **Retention Period:**

Definition of the retention period for the relevant logs.

Preferably, a specific time period (e.g., 3 months) should be set for log storage.

- **Storage Location:**

Definition of the log storage location.

Options include integrated device storage, storage on a syslog server, or another storage medium.

- **Parameter Management:**

Implementation ensuring that monitoring parameters remain up-to-date and aligned with Organizational needs.

[Organization Name] ensures that the following events are logged:

- Access to files and processes of assets (without displaying passwords or other authentication secrets)
- Failed attempts to execute files
- Use or attempted use of elevated privileges
- Network traffic and HTTP/DNS requests
- Data transfers to and from removable media
- Configuration changes
- Changes to accounts and security policies of assets
- Password changes for privileged user accounts
- Creation of privileged user accounts
- Login to assets from locations that have not been predetermined
- Repeated failed access attempts within a short period
- Network scanning
- Modifications to log files, including their deletion or the disabling of logging capabilities

© CYberSynchorny, 2024

Additional requirements:

- At least two (2) network time sources must be configured to ensure accurate timestamping.
- Where possible, monitoring data must be reviewed daily, either manually or semi-automatically, to identify anomalies, trends, upcoming attacks, or active attacks.
- Any interruption in logging and monitoring processes must be treated as a security incident.
- If monitoring capabilities fail, appropriate measures must be taken to disable the affected asset until the cause of the failure is fully investigated (excluding assets that are directly related to security management).
- Relevant logs must be retained for at least 3 months per system. If this is not technically possible, a mechanism must exist for requesting an exception to the policy.
- Exception requests must justify how the related risk is reduced through compensating controls, and approval must follow the change-management process.

3. Secure Disposal or Reuse of Assets

Any asset belonging to [Organization Name] that contains sensitive information, personal data and/or software licenses must be checked prior to its disposal to ensure that such information has been securely removed.

The decision to repair or dispose of a damaged asset that contains classified information and sensitive data must be assessed in terms of the associated information security risk.

As mentioned earlier in the asset management procedure, there is a documented process that describes how assets are managed throughout their lifecycle. This process includes actions performed by authorised roles during:

- Procurement (the asset categories and information security requirements are defined),
- Installation (necessary preparations for installation are determined and verified),
- Maintenance (a maintenance schedule is defined for the asset; periodic checks and security updates are included; regular software updates and hardware upgrades are applied; compliance with security policies is ensured; signs of issues are continuously monitored and resolved promptly),
- Disposal (data and results are recorded prior to disposal).

Within this process, information security elements are also included to ensure that information security is an integral part of the asset lifecycle — procurement, installation, maintenance and disposal. For more information, refer to the Data Protection Policy.

Changes to assets are managed according to a Change Management Procedure [CMP], which governs the control and management of changes to systems, applications and other supporting assets involved in information processing. In defining the change management procedure, [Organization Name] provides for change requests to ensure that requested changes from relevant participants are taken into account.

The change management process must enable [Organization Name] to assess risks associated with change requests and to design changes while considering appropriate security measures. The change management procedure must include the preparation and verification of changes (see Change and Configuration Management Policy).

As part of this framework, the criteria used by [Organization Name] to allocate resources to criticality categories are also described. Security specifications appropriate to the intended use of each asset are defined before procurement during the preparation of requirements (Request for Proposal – RFP).

© CYberSynchorny, 2024

4. Review

Documents related to Asset Management must be reviewed and updated at least annually, or whenever significant changes occur in the environment of [Organization Name], to ensure that the policy remains effective, secure, and aligned with Organizational objectives. More specifically, the policy may need to be revised in cases of major additions, upgrades, or removal of existing assets, as well as the integration of third-party suppliers or service providers who manage or have access to Organizational assets.

It is reminded that in cases of changes to assets, the process that must be followed is the Change Management procedure.

4. References

Category	ID	Control	Control Objective
Category	ID	Control	Control Objective
Asset Management	AM1	Asset lifecycle management	To ensure that assets are protected throughout their entire lifecycle, including procurement, deployment, maintenance, and disposal.
Asset Management	AM2	Asset recording and ownership	To ensure that all assets are recorded in an inventory and that ownership is assigned in order to achieve traceability and accountability.
Asset Management	AM3	Asset monitoring	To ensure that assets are monitored for attacks, anomalies, and security threats, enabling activation of incident and event response procedures.
Asset Management	AM5	Cryptography	To ensure confidentiality, integrity, and authenticity of information through the adoption of appropriate cryptographic solutions.
Risk Management	RM2	Framework	To establish an inventory of assets, systems, and processes within the Organization.

© CYberSynchorny, 2024

4.5 Tool 5 - Supplier and Third-Party Management Policy (TPS)

[Organization Name]

THIRD PARTIES MANAGEMENT POLICY

© CYberSynchorny, 2024

Table of Contents

1. Purpose
2. Scope of Application
3. Document Recipients
4. Roles and Responsibilities
4.1. Responsibilities of [Organization Name] security Executive Management (Cyberspace Directorate)
4.2. Responsibilities of the Information and Data Security Officer
4.3. Responsibilities of the Steering Committee
4.4. Responsibilities of [Organization Name] security Computer Users
5. Policy on Communication with External Parties
5.1. Identification of Third-Party Cooperation with the Cyberspace Directorate
5.2. Contract Signing
5.3. Compliance with Security Policies
5.4. Selection of Third Parties
5.5. Security Requirements in Collaborations with Third Parties
5.6. Termination of Contracts with Third Parties
5.7. Right to Conduct Security Audits of the Third Party
5.8. Reporting Security Issues and Incidents
5.9. Third Parties and the Supply Chain
5.10. Reporting Changes in Third-Party Personnel
5.11. Feedback
5.12. Policy Verification and Review
6. Obligation of Implementation
7. Disciplinary Sanctions for Non-Compliance

© CYberSynchorny, 2024

1. Purpose

This Third Parties Management Policy describes how the Cyberspace Directorate communicates and cooperates with external partners, entities, contractors and other third parties, while complying with all requirements for safeguarding the protection of the information of the SOC.

More specifically, this policy applies to the monitoring and oversight of external partners and third parties, the management of contracts with external partners and third parties, as well as any changes that may arise regarding the form of cooperation and/or the access of third parties to the Service's data and information (e.g. access to [Organization Name] security infrastructures).

2. Scope of Application

This Policy applies to all employees, contractors and third parties who have access to the premises of the SOC. This Policy recognises the need to establish a framework for control and enforcement of rules for third parties that cooperate with the Cyberspace Directorate, in compliance with the principles and rules for the Information and Data Security of the SOC.

3. Document Recipients

- [Organization Name] security Analyst L1 (Security Analyst Level 1)
- [Organization Name] security Analyst L2 and L3 (Security Analyst Level 2 & Level 3)
- [Organization Name] security Manager
- Systems Architect
- Operations Manager
- [Organization Name] security Executive Management (Cyberspace Directorate)
- Engineer
- Incident Response & Threat Intelligence Team
- Steering Committee
- Information Systems Technician
- Helpdesk Technicians (Helpdesk Team)
- Infrastructure Systems Administrator
- Information and Data Security Officer
- [Organization Name] security Computer Users
- Data Protection Officer (DPO)

4. Roles and Responsibilities

Clearly defined roles and responsibilities are of critical importance for the development and achievement of a successful framework for the conclusion and constructive cooperation between Third Parties and the SOC.

4.1. Responsibilities of [Organization Name] security Executive Management (Cyberspace Directorate)

The main responsibilities of [Organization Name] security Executive Management include the approval and review of the Third-Party Cooperation Management Policy, as well as the creation of the necessary working conditions for the employees of the SOC. Finally, they are responsible for decision-making regarding the imposition of sanctions in cases of disciplinary offences related to improper application of the Policy.

© CYberSynchorny, 2024

4.2. Responsibilities of the Information and Data Security Officer

The main responsibilities of the Information and Data Security Officer include the maintenance and updating of information security policies and procedures in relation to the current situation of the SOC, as well as the training of staff regarding the implementation of these policies.

4.3. Responsibilities of the Steering Committee

The main responsibilities of the Steering Committee include supervising the accuracy and adequacy of the content of the contracts signed between the Service and third parties.

4.4. Responsibilities of [Organization Name] security Computer Users

The main responsibilities of users who interact with the Cyberspace Directorate include the proper implementation of this Policy, as well as reporting any potential data leakage incident.

5. Policy on Communication with External Parties

5.1. Identification of Third-Party Cooperation with the Cyberspace Directorate

The policy on cooperation of third parties with the Cyberspace Directorate includes the definition of roles and responsibilities, the conditions of cooperation and the communication procedures. This also includes agreements on the exchange of security information and the handling of potential incidents, the delineation of access rights, the communication of predefined intervention scenarios, the evaluation of security specifications and the assurance of compliance with legal requirements for data protection.

Employees must identify the external entities with which they interact and be aware of the nature and purpose of the communication.

5.2. Contract Signing

Any new cooperation with a Third Party/External Partner must be accompanied by the signing of the necessary contracts and agreements. An agreement between the Service and a third party must be clearly worded so that the content of the service provided is easily understood.

In addition, where necessary, it shall be accompanied by a service level agreement. The Steering Committee is responsible for supervising the correctness of the content.

Written agreements define the service levels offered by the external partner to the SOC, including availability, functionality, performance, operation, security and other aspects.

Furthermore, all parties involved shall have clearly defined duties regarding the implementation and management of the security controls deemed necessary for the secure provision of services.

Each agreement specifies the levels of availability, functionality, performance, operation, security and other characteristics of the service provided by the External Partner to the Cyberspace Directorate. In addition, all parties involved shall have clearly defined duties regarding the implementation and management of security controls deemed necessary for the secure provision of services.

© CYberSynchorny, 2024

In cooperation with the Data Protection Officer (DPO), templates of non-disclosure agreements and contracts with confidentiality clauses are developed and maintained, which, among other things, define the confidential information and the manner of its handling, retention and disposal.

5.3. Compliance with Security Policies

When communicating with external entities, employees must comply with the security and confidentiality policies of the SOC.

The procedures governing the management of External Partners and Third Parties, as well as the security measures applied to protect the information communicated, must comply with applicable regulations, with particular emphasis both on requirements related to the protection of confidential, critical and personal data and on requirements concerning the outsourcing of critical services.

5.4. Selection of Third Parties

For the conclusion of an agreement with an External Partner/Third Party, the Cyberspace Directorate sets predefined and documented evaluation criteria regarding their selection.

Any potential cooperation of a third party with the Cyberspace Directorate presupposes the existence and execution of certain actions to ensure the integrity of SOC. In other words, the third party must meet security specifications, ensuring the protection of critical data and information at a level at least equal to that of the Service.

Some of the required prerequisites for concluding a cooperation with a Third Party are compliance with international quality and security standards, as well as compliance with relevant regulations. Other prerequisites include the logical and physical security of the facilities used for service provision, the use of strong encryption mechanisms for remote access to information systems, and the ability to recover after a disaster.

5.5. Security Requirements in Collaborations with Third Parties

To ensure the protection of information, the Cyberspace Directorate clearly defines, together with the external partner, the responsibilities for the management and protection of Information and Data both during the term and after the termination of the contract.

Through the signed contract, the time and levels of access of External Partners to the Information Systems and infrastructures of the [Organization Name] are defined. Access is granted only to authorised representatives of the External Partner, for the execution of specific activities in accordance with the contract concluded, prohibiting any other personal use, through the imposition of legal sanctions for malicious or unlawful use.

For this purpose, appropriate access controls, both procedural and technical (e.g. remote connection using VPN, logging of the connection, etc.), shall be applied so as to ensure predefined protection levels regarding External Partners' access to the Information Systems and infrastructures of the SOC.

Any modifications and changes to [Organization Name] systems and data, as well as to the connections with third parties, shall be carried out in accordance with the contractually agreed procedures.

The physical access of third parties to [Organization Name] premises follows the "Physical Security" policy, complying with all required security rules and specifications.

When communicating with third parties, [Organization Name] security employees must avoid disclosing confidential [Organization Name] security information without the required authorisation.

© CYberSynchorny, 2024

5.6. Termination of Contracts with Third Parties

Upon termination of a contract or its transfer to another External Partner, the Cyberspace Directorate ensures that the contract clearly states the obligation of the Third Party to return any equipment received from the SOC. The equipment returned, including stored Information, shall be recorded.

In case of disagreements or problems arising during communication with external entities, employees must inform the competent responsible staff within the [Organization Name].

The contract clearly defines the liability of the Third Party in the event of direct or indirect damage caused to [Organization Name] security equipment or systems. In case of non-compliance with the agreed terms, the signed contract provides for specific penalties for non-compliance with the relevant Information Security principles.

5.7. Right to Conduct Security Audits of the Third Party

The Organization ensures that the agreement concluded with the external partner includes a clause explicitly granting it the authority to conduct inspections or regular and ad hoc audits at the facilities of the external partner, using personnel from the Cyberspace Directorate. This includes all the controls and security measures implemented by the External Partner to ensure the security of the services provided.

5.8. Reporting Security Issues and Incidents

When issues arise related to the Information Systems and infrastructures of the SOC– such as inappropriate use, security incidents or attempted breaches – External Partners are required to report them immediately.

Information shall be provided based on a predefined classification (e.g. issues and type of incidents, severity and priority), response time and escalation levels.

The External Partner is responsible for testing and evaluating security before re-establishing the connection, recovering or restoring systems in accordance with the signed contract, as well as for covering the costs in case of loss or destruction of data in the [Organization Name] security Information Systems (e.g. data reconstruction costs), as specified in the contract, in the event of a security incident for which the External Partner is responsible or involved.

External partners are not allowed to exploit any security weaknesses, whether procedural or technical. In case security gaps are identified, they shall be reported immediately to the [Organization Name] security Manager.

When facing difficulties or adverse situations in communication with external entities, employees must apply appropriate management and conflict resolution techniques.

5.9. Third Parties and the Supply Chain

Supply Chain Management is inextricably linked to the management of collaborations with third parties.

Indicatively, the Service's partners are required to:

- convey information security requirements and good security practices to their subcontractors and partners,

© CYberSynchorny, 2024

- provide assurances (e.g. recognised certifications) regarding the security of critical components (systems, software, etc.) that are included in or support the products and services they offer to the Cyberspace Directorate,
- provide information on the information security characteristics of the products and services they offer,
- provide the capability of traceability of the origin of critical components (systems, software, etc.) that are included in or support the products and services they offer to the Cyberspace Directorate.

More detail on Supply Chain Management is provided in the Policy on Preparation for Supply Chain Management Regulations.

5.10. Reporting Changes in Third-Party Personnel

In order to regularly update the access rights of the external partner, the Cyberspace Directorate ensures that the contract signed with the external partner clearly describes who is responsible for informing it of any changes concerning the personnel involved.

Furthermore, the External Partner is obliged to inform the Cyberspace Directorate of any additional relevant Organizational changes.

5.11. Feedback

[Organization Name] security employees must take into account the opinions and views of external partners for the improvement of [Organization Name] security systems and services.

5.12. Policy Verification and Review

The third-party cooperation management policy is periodically reviewed and verified to ensure that it remains applicable and effective.

During this review, any new changes and the potential impacts arising since the previous version of the policy are analysed.

6. Obligation of Implementation

The third-party cooperation management policy constitutes an integral part of the operation of the [Organization Name]and aims at ensuring the integrity of data and information exchanged between Third Parties and the Service.

All parties involved are obliged to comply with this policy to ensure effective cooperation between Third Parties and the Service.

7. Disciplinary Sanctions for Non-Compliance

Any breach of this policy, as well as any violation thereof, will be treated with strictness and may result in disciplinary measures, including the initiation of legal proceedings, depending on the severity of the violation.

Data subjects concerned have the right to submit questions regarding this policy and to request clarifications from the Information and Data Security Officer.

This policy enters into force as of [Approval Date] and is reviewed periodically to ensure its alignment with the needs and requirements of the Service.

© CYberSynchorny, 2024

4.6 Tool 6 - Access Control Policy

[Organization Name]

THIRD PARTIES MANAGEMENT POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
1.1 Purpose
1.2 Scope
2. Access Control Policy
2.1 Introduction
2.2 Access Control to [Organization Name] security Resources
3. Role-Based Identity and Access Management
4. User Authorization
5. Identity Verification Measures – User Credentials
6. Password Management
7. Passwords
8. User Privileged Rights
9. Accounts with Elevated Access Rights
10. External Access to [Organization Name] security Resources
11. Third-Party Connections
12. Off-Organization Accounts
13. Monitoring and Logging of Activities (logs)
14. Best Technical Measures and Practices for Password Protection
15. Review
16. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

The purpose of this Access Control Policy is to define guidelines and other Policy terms for the management and control of access to [Organization Name] resources and data, in order to ensure the security of [Organization Name] security information systems and information, and to prevent unauthorized access.

1.2 Scope

This Access Control Policy applies to all departments and all employees of [Organization Name], including third parties who may require – on a temporary or permanent, standard or privileged, external or internal – access to [Organization Name] security resources.

This policy also applies to all [Organization Name] security assets, covering access to applications, networks, resources and buildings.

1. Access Control Policy

2.1 Introduction

All information systems of [Organization Name] are protected by "access control" mechanisms. These mechanisms comply with the basic principles of secure access (Authentication, Authorization, Logging). Additionally, where feasible, SSO (Single Sign-On) technology must be used.

[Organization Name] establishes, implements and maintains an asset inventory in order to ensure that the Organization has a clear, accurate and up-to-date view of the assets (e.g. hardware, software, information, resources, networks and buildings) it maintains. The inventory identifies the owner of these assets.

The inventory enables the Organization to monitor all assets for which information security measures must be implemented and maintained. Monitoring and logging of activities (logs) must be performed. The extent of monitoring and logging of activities arises from the results of a risk assessment carried out under the responsibility of the asset owners. The main characteristics defined are: type of logging, retention period, storage medium. Logging of security-related activities is enabled at least on critical systems. Logging of security-related activities must be enabled on all systems.

[Organization Name] must provide access to its information systems for its staff and may provide access to its suppliers and third parties acting on its behalf. It is understood that access must be granted only where necessary so that the aforementioned users can perform their tasks.

[Organization Name] establishes, implements and maintains identity and access management measures that consider role-based access measures, with the aim of providing technical and Organizational means to enforce the principle of least privilege and to manage privileged users accordingly. Role-based access control must ensure that sufficient permissions are granted to users based on their responsibilities associated with relevant roles. Role-based access control must be exercised in accordance with human resources security procedures, as defined in [HRS1], in order to ensure that access roles are aligned with the roles and responsibilities of personnel within the Organization.

Basic principles of secure access:

- Authentication: Authentication is the process by which an information system recognises/identifies the requester who requests access to a system. The user must prove who they are. The user then provides their credentials.

© CYberSynchorny, 2024

- Authorization: Once the credentials are valid, the information system authorizes the user with the appropriate access rights.
- Accounting/Accountability: All accesses/authorizations are logged in order to maintain a history for future use.

2.2 Access Control to [Organization Name] security Resources

Access to all resources must be granted according to [Organization Name] business needs and governed by the principles of “access to information strictly as required”, “least privilege” and “segregation of duties”.

Categories of Resources:

1. Electronic Resources:

- Information Systems
- Software Applications
- Databases
- Network Infrastructure

2. Physical Resources:

- Buildings and Offices
- Equipment and Materials

The access control policy is an extensive framework and must be continuously adapted to address new challenges and threats. Below are some responsibilities and procedures that [Organization Name] security must apply in order to achieve the objectives defined in the above policy.

3. Access Management:

- Definition and management of access rights
- Allocation of roles to prevent violations

4. Authentication:

- Use of secure authentication methods, such as passwords, One-Time Passwords (OTP) and biometric data

5. Granting of Rights:

- Definition of access rights based on role and need
- Periodic review of access rights
- Updating based on changes in duties

6. Policies for Access to Sensitive Data:

- Implementation of special policies for access to sensitive data, protecting the confidentiality and integrity of information

7. Access Logging:

- Comprehensive logging of access for verification and anomaly detection

8. Handling Violations:

- Definition of procedures for handling violations and disciplinary measures

9. Monitoring and Detection:

- Automatic monitoring of activities and detection of unusual patterns

10. Training and Awareness:

© CYberSynchorny, 2024

- Staff training on safe use of resources
- Awareness-raising on security threats

11. Policy Review:

- Periodic review of the policy to align it with technological developments and the needs of the Organization

1. 3. Role-Based Identity and Access Management

Role-based access control must be performed in accordance with human resources security procedures as defined in [HRS1] in Decision K.D.P. 389/2020, in order to ensure that access roles are aligned with the roles and responsibilities of personnel within the Organization. Users must be granted access rights to [Organization Name] security resources based on their role (Role Based Access Control), receiving a predefined set of rights. Each role must have only the necessary rights to perform the corresponding tasks.

[Organization Name] must establish adequate measures to ensure that personnel working on behalf of the Organization, who have access to Organizational resources, support the information security policy, and the objectives of [Organization Name].

It also creates a plan to ensure that information security is embedded throughout the employment life cycle. The plan includes appropriate information security measures at each stage of employment, e.g. background checks prior to hiring, training and awareness of employees, inclusion of adequate provisions in employment contracts, development of an acceptable use policy, return of devices containing critical information, and removal of access to systems and applications.

Below are some identity and access management procedures, in order to provide the technical and Organizational means to enforce the principle of least privilege and the management of privileged users.

2. Role Definition:

- Each user is associated with a specific role based on their job duties. [Organization Name] security maintains a register of accounts and their related access to its information resources.

3. Assignment of Rights Based on Role:

- Definition of adequate access rights for each user based on their role, ensuring the principle of least privilege. Asset owners must authorize access and define the rights and access rules for the resources they manage, taking into account their criticality as determined by risk analysis.

4. Identity Verification:

- Access to [Organization Name] security resources must be based on validating the legitimacy of the user through the verification of their credentials, in order to ensure that access rights correspond to the responsibilities and duties of employees at [Organization Name]. Such access must be granted using effective identity verification methods to ensure that each user is correctly associated with their respective role.

5. Review of Access Rules:

- Periodic review of access rules and update according to changes in users' duties and responsibilities.

6. Staff Training:

- Training staff on the importance of the principle of least privilege and the proper use of access rights. Requirements for protecting credentials must be clearly communicated to all relevant personnel at regular intervals.

© CYberSynchorny, 2024

7. Activity Monitoring:

- A monitoring system to verify compliance with access rules. [Organization Name] must use an Identity and Access Management (IAM) system to continuously monitor user credentials, enforce security policies, notify users of non-compliant practices and allow immediate correction of any deviations.

8. Integration with Human Resources Security Procedures:

- Cooperation with human resources security procedures to ensure alignment of access roles with professional responsibilities. In the event of departure, the asset owner must take appropriate measures to delete or deactivate accounts.
- Procedures for disabling or deleting accounts must be designed to be as automated as possible through the use of an Identity and Access Management (IAM) system.

4. User Authorization

For authorizing access to [Organization Name] security resources, the criticality of the resource, the business need for access, the principle of least access, and the results of the risk analysis must be taken into account. Specifically, all access rights must be defined according to the following principles:

- Principle of Least Privilege
- Principle of Need to Know

User access rights must be predefined, in accordance with the job positions and duties at [Organization Name], as defined by [Organization Name] security Management.

Additionally, these rights must be approved by the head of each Organizational unit, based on the following:

- Reasons for accessing the specific system
- Segregation of duties
- The required level of access
- To grant authorization for additional access rights to a user beyond the predefined ones, a relevant request form must be completed
- In cases of access to [Organization Name] security systems by external partners/third parties, approval for granting access must be recorded and provided by the person responsible for the respective system
- Application developers and technical staff must not have access to production systems and related production data, unless there is a specific reason
- Records must be kept of all access rights, whether active or not
- Inactive accounts (define time in days) must be automatically disabled and their access rights revoked
- Disabled accounts must not be deleted
    - If disabled accounts contain Personal Data, they must be handled as required by the applicable legislation
- Access rights must be revoked in cases where users are on leave and/or sick leave
- Access rights must be revoked in cases where users no longer work for [Organization Name]
- Access rights must be revoked during non-working hours and holidays
- The suitability of user and administrator access rights must be checked at regular intervals (define time in months) in order to ensure the correctness of assigned accesses and rights

© CYberSynchorny, 2024

- In cases of misuse of these access rights, the Business Owner of the system and the Internal Audit Unit have the right to revoke such access rights

For more information, see the Human Resources Policy.

5. Identity Verification Measures – User Credentials

Access to all [Organization Name] security resources must be controlled through authentication mechanisms for secure user access, in order to ensure that only authorized users can access them. There are three types of credentials: “something the user has”, “something the user is”, “something the user knows”. For example, these may be usernames/passwords, access cards, smart cards, security tokens, biometric data, PINs, etc., or a combination thereof.

- Each user, whether a natural person or an entity, must have unique identification credentials for access to [Organization Name] security services and resources in order to ensure non-repudiation.
- Non-personal (generic) credentials are prohibited. For example, each credential must be linked to a single specific natural person/user. When this is not feasible, information systems must be supported by software that has the capability to verify the identity of the user who uses the non-personal account.
- A record of all user credentials must be maintained. This record must be encrypted and include at least the following:
    - The mapping of user/credential
    - The person who approved it
    - The date of creation of the credential
    - The access rights of each credential
    - Whether the credential is active
- Systems in which authentication is achieved by username/password must comply with this Policy. Validation of authentication data is performed only after full entry of the credentials.
- In systems where authentication is achieved through username/password, in cases where any of the fields (username/password) is incorrect, the system must not inform the user which field is wrong.

[Organization Name] security systems are protected against multiple failed access attempts (brute force), and all login attempts, successful or failed, are logged in accordance with the Logging and Monitoring Policy.

- In cases where repeated failed access attempts occur, the user’s account must be locked, suspended, or disabled.
- On critical systems, or systems that contain critical data, or systems accessible from the internet, a combination of credentials, two-factor authentication and strong authentication must be used. The same applies to remote access.
- Before a system is introduced into the production environment, all default system accounts, such as vendor accounts and anonymous accounts, must be deleted. If deletion of these accounts is not possible, they must be disabled. In cases where neither disabling nor deletion is possible, default passwords must be changed. Each of these actions must be recorded in detail and maintained in an appropriate register, ensuring full transparency and traceability.
- Authentication to [Organization Name] security systems must not be possible outside working hours and holidays unless there is a documented business need. Furthermore, authentication to [Organization Name] security systems must not be possible for users who are on leave. This reduces malicious activities on [Organization Name] security systems/buildings in case an employee’s credentials are stolen. In this

© CYberSynchorny, 2024

way, access to [Organization Name] security systems/buildings is granted only with the presence and authentication of the employee. It is noted that certain exceptions may exist, which must be approved by the respective system owner. All exceptions must be recorded in a relevant register.

The authentication process must be resistant to replay attacks and ensure that no sensitive data are revealed that could be exploited by malicious users (e.g. cleartext).

6. Password Management

A proper strategy for the creation and management of passwords significantly reduces the risk of password cracking, interception, or guessing, thus preventing unauthorized access. All information systems must be protected with a password.

- Furthermore, all critical information systems or systems accessible from the internet (Internet Facing Applications) or systems that support remote access must support Multi-Factor Authentication and strong authentication.
- Default passwords of systems must be changed (including passwords preset by the manufacturer and/or supplier).
    - On all operating systems, local default accounts such as “administrator”, “root”, “guest”, “default” must be renamed. If a default account cannot be disabled, it must be renamed.
    - On operating systems such as Microsoft Windows, the local administrator account must be renamed. In addition, the passwords of such accounts must be managed (changed according to this Policy), and these accounts must have different passwords generated randomly. These passwords must be stored in encrypted form.
- The feature that allows password “Hints” must be disabled.
- All workstation-type systems that are not used for more than 15 (fifteen) minutes must be automatically locked (password protected screen saver).
- All servers that are not used for more than 5 (five) minutes must be automatically locked (password protected screen saver).
- All inactive sessions that remain idle for more than 15 minutes must be automatically terminated (auto logout).
- The use of shared accounts must be kept to an absolute minimum.
    - The use of shared accounts for the daily execution of tasks is prohibited.
    - The use of shared accounts is allowed only where there is no alternative way to perform tasks and after appropriate approval.
    - Where a shared account is used, access to information systems must be protected by software capable of verifying the identity of the user who uses the shared account.
    - Where a shared account is used, upon departure/transfer of any of the users of the shared account, the password must be changed immediately.
- Where the SNMP network protocol is used, the default community strings “public”, “private” and “system” must not be set and at the same time must differ from the passwords used for interactive access to the device. Where possible, SNMPv3 must be used, which supports encryption and authentication.

© CYberSynchorny, 2024

- Storing passwords in clear text in system interconnection files is prohibited. Passwords must be protected by applying best technical measures and practices for password protection, both for storage and transmission.
- The use of passwords through unencrypted communication channels (e.g. http, ftp, telnet, etc.) is prohibited.
- In case of a breach or suspected breach of a user or system password, procedures under the Security Incident Management Policy must be applied. [Organization Name] reserves the right to perform checks on passwords.

7. Passwords

[Organization Name] maintains a password security standard that describes the minimum acceptable requirements for security passwords with regard to their complexity, lifetime, reuse, etc.

Passwords issued, both for new user accounts and for reissuing passwords for existing user accounts, must be randomly generated, one-time and have a validity period not exceeding 7 days.

- **Password history:** Passwords must be different from at least the last X passwords of the user.
- **Maximum password age:** The maximum lifetime of a password must not exceed (define time in days) days. At the end of this period, changing the password must be mandatory.
- **Password age (for System, Service Accounts and Admin Accounts):** For system/service accounts and accounts with elevated access rights (privileged accounts), the maximum lifetime of a password must not exceed (define time in days) days.
- **Minimum password age:** The minimum lifetime of a password must be 1 (one) day.
- **Minimum password length:** Passwords must be at least 10 (ten) characters long.
- **Minimum password length (for System, Service and Admin Accounts):** For system/service accounts and accounts with elevated access rights (privileged accounts), passwords must be at least 15 (fifteen) characters long.
- **Password complexity:** Passwords must contain at least 3 (three) of the 4 (four) different character types:
    - Uppercase letters [A B C D E F … Z]
    - Lowercase letters [a b c d e f … z]
    - Numbers [0 1 2 3 4 5 6 7 8 9]
    - Special characters [( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > . ? /)]
- **Password illegal patterns:** Passwords must not be identical to the user's account name (username) and must not be common words (dictionary words) or based on personal information of the user (e.g. family names, car make, team, etc.). Furthermore, passwords must not consist of sequential characters (e.g. 12345, 54321, qwerty, abcdef, etc.).
- **Password encryption:** Passwords must not be stored in plain text or use weak encryption mechanisms. Furthermore, where passwords are stored in encrypted form, these passwords must not be retrievable (disable storing passwords using reversible encryption).
- **Lockout threshold:** The account must be automatically locked after 5 (five) unsuccessful login attempts.
    - **Lockout counter:** The number of minutes that must elapse from the time a user fails to log in before the failed login attempt counter is reset to 0 must be 30 minutes.

© CYberSynchorny, 2024

- **Lockout duration:** The locked account should be unlocked by an authorized system administrator.

- **Dormant accounts:** Dormant accounts must be disabled and their access rights revoked. A dormant account is one that has not been used to log into the system for more than the number of days defined as “Maximum password age”, i.e. X days.

Additionally, for user authentication to critical systems or systems accessible from the internet, Multi-Factor Authentication and strong authentication must be used. Multi-Factor Authentication and strong authentication must be applied for remote access to systems. It is understood that One-Time Password (OTP) tokens must be randomly generated.

- **One-Time Password – Validity Period:** The maximum lifetime of an OTP must not exceed (define time in minutes) minutes.
- **One-Time Password – Lockout Threshold:** The account must be automatically locked after (define number) unsuccessful OTP entry attempts.
- **One-Time Password – Lockout Counter:** The number of minutes that must elapse from the time a user fails to log in before the failed login attempt counter is reset to 0 must be (define time in minutes) minutes.
- **One-Time Password – Lockout Duration:** The locked account should be unlocked by an authorized system administrator.
- **One-Time Password – Password Complexity:** OTPs must contain at least 2 (two) of the 4 (four) different character types:
    - Uppercase letters [A B C D E F … Z]
    - Lowercase letters [a b c d e f … z]
    - Numbers [0 1 2 3 4 5 6 7 8 9]
    - Special characters [( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > . ? /)]

8. User Privileged Rights

According to Decision K.D.P. 389/2020, [Organization Name] establishes measures to ensure the proper management of privileged users and the activation of their privileges only when needed. [Organization Name] ensures that users are not granted privileged rights by default and that systems and applications do not run with default user privileged rights, in order to mitigate the risk of privilege escalation and ensure the protection of user privileged rights from malicious acts or other negative behaviours or intentions.

1. **Criteria for Granting Privileged Rights:**
    - Privileged user access to [Organization Name] security resources, which allows them to perform administration or maintenance tasks, must be granted only when there is a clear and confirmed business need (need-to-use basis) and on an event-by-event basis.
2. **Approval by Responsible Person:**
    - The person granting privileged rights must be a responsible, authorized person who understands the implications of privileged access and use.
3. **Register Maintenance:**

© CYberSynchorny, 2024

- A register of privileged user accounts must be maintained. This register must record the account and the resource to which privileged access has been granted, the user assigned to the account, the type of privileged access granted, as well as the dates of granting and reviewing the rights.
- The privileged account register must include at least the following: resource, account, type of privileged access, date of granting, resource owner, review date, purpose.

4. **Need Assessment Procedure:**
    - Definition of specific criteria for analysing the need for privileged access, to ensure that such access is granted only in cases of genuine need.
5. **Link to Specific Events:**
    - Privileged access must be linked to specific events and granted only for the duration of such events.
6. **Recording and Supervision:**
    - Logging of all instances of privileged access, including the specific events that justify such access.
7. **Review and Reallocation:**
    - Periodic review of privileged rights, with any reallocation or revocation performed according to developments and needs.

9. Accounts with Elevated Access Rights

If a person holds more than one user role when using [Organization Name] resources (e.g. privileged and standard user), they must have separate login accounts for each role. Each administrator must have their own personal (named) account as a standard user to perform daily tasks. For server and application administration, each administrator must have a separate named account, which they will use only when it is necessary for accessing and managing servers and applications.

The passwords of privileged accounts must be known exclusively to the authorized owner of the account. The use of accounts with elevated access rights for the performance of daily tasks by system administrators is prohibited.

Access to privileged accounts is protected using Multi-Factor Authentication (MFA).

Privileged user account activity is logged and monitored and may be archived (electronically), while these logs are adequately protected from deletion or alteration.

The review of privileged user access rights must be performed at least quarterly in order to confirm the authorization of all active accounts.

In addition, all actions of administrators as well as any other user connections to the following systems may be recorded (screen/video recording) with the assistance of a specialized control/mechanism/software:

- Systems classified as Critical
- Systems that manage and/or contain and/or process confidential information (such as personal data, banking data)
- Systems that contain shared accounts
- Systems hosted in De-Militarized Zones (DMZs)
- Systems accessible by external partners

© CYberSynchorny, 2024

The creation and use of generic privileged accounts must be avoided. If the use of such accounts is unavoidable, the relevant business need must be documented in detail and adequately justified.

10. External Access to [Organization Name] security Resources

According to Decision K.D.P. 389/2020, [Organization Name] must ensure adequate access control measures for external access to Organizational resources.

[Organization Name] must ensure the possibility of remote access to the network using Virtual Private Networks (VPN), and access to remote [Organization Name] security resources must be permitted only through approved and securely configured gateways. External access to [Organization Name] security resources must be protected using Multi-Factor Authentication (MFA).

Before granting external access, compliance checks of devices with the minimum required security profile must be performed (e.g. assessment of the status of anti-malware software, security updates, disk encryption), and access to [Organization Name] security resources must be allowed only if these criteria are met.

Below are procedures for granting external access and maintaining a list of external accesses.

1. Approval of External Access:

- External access to Organizational resources is granted only after approval by an authorized responsible person.

2. Access Granting Procedure:

- External access is granted following a relevant request, which must include the reasons for access and the necessary security measures being applied.

3. Recording External Accesses:

- [Organization Name] maintains a detailed list of all external access granted per system. This list must include details about users (e.g. identifiers, internal/external user, etc.) and access levels.

4. Duration of Access:

- Definition of the period during which external access is valid, with the possibility of renewal after new approval.

5. Security Measures:

- Definition of security measures to be followed during external access, including connection encryption and rights management.

6. Updating Security Systems:

- Any change to external access must be immediately reflected in the Organization's security systems.
- External connections must be logged and systematically monitored for suspicious or malicious activities, in accordance with the Logging and Monitoring Policy, ensuring timely detection and effective management of potential security incidents.

11. Third-Party Connections

- Remote connections from third parties to [Organization Name] security network must be avoided where possible.
- Any connection to the Organization's IT infrastructure must be controlled and authorized by the Information Security Officer.

© CYberSynchorny, 2024

- Third parties (e.g. companies) must have agreed and signed an appropriate Third-Party Agreement and Non-Disclosure Agreement (NDA) in order for the connection to be approved. In case of processing personal data, a Data Processing Agreement must also be signed.
- Access rights must be defined before signing the agreement.
- In cases of third-party connections to the Organization's network, secure data transmission mechanisms between [Organization Name] security and third parties must be in place (see Network Security Policy), as well as mechanisms for monitoring all actions performed by third parties.
- Third parties must handle the Organization's information in accordance with the Asset Management Policy.
- Third parties must designate a person as the contact person responsible for their connection to [Organization Name]. If the contact person changes, [Organization Name] security must be notified immediately.
- When the connection is no longer required or is terminated, third-party access rights must be removed immediately.
- All connections must be monitored as provided in the Network Security Policy.
- In cases where unattended access by external partners is required:
    - Access must be restricted only to external partners who have signed a service provision agreement and a confidentiality agreement (see Management Policy).
    - Access must be restricted ONLY to the Organization's external network (DMZ), in an isolated local network (isolated VLAN). Under no circumstances must unattended access be granted to external partners in the production environment.
    - Access must be strictly limited only to systems whose data are masked and/or scrambled, pseudonymized, or to systems that do not contain confidential information or personal data.
    - The IT equipment used as a means of connection for remote access to the Organization's network, information systems and information must undergo a posture assessment before access is granted. Specifically, the IT equipment must:
        - be updated with the latest security patches
        - be scanned with anti-malware software
        - be protected (on-access scanning) by anti-malware software (see Systems Security Policy)
        - not be connected to malicious network addresses (bad reputation IPs)
    - All remote connections must be recorded (session recording) using specialized software (e.g. ObserveIT, CyberArk, Centrify, Balabit).
- If the above conditions for unattended access are not met and the connection from external partners and/or third parties is required to production systems and/or the internal network of the Organization, such connection must be accompanied throughout its duration (e.g. via Webex or locally) by an authorized officer/administrator of [Organization Name].
- In cases of misuse of these rights, [Organization Name] reserves the right to revoke authorization for remote access.

© CYberSynchorny, 2024

12. Off-Organization Accounts

In cases where accounts are required on platforms and applications outside [Organization Name] (e.g. cloud services, support accounts, etc.), a procedure must be defined and followed for their creation. The procedure must include, among other things:

- Recording in a register containing the accounts, the authorized users and the reasons for which they are required/used
- Designation of two officers as administrators (one responsible and one deputy)
- Review of administrators and password changes in cases of staff departures/transfers
- Deactivation of the account when it is no longer required
- Reporting of any incident (activity or concern or suspicion) that may directly or indirectly harm the security of [Organization Name] information systems and/or information

It is noted that Multi-Factor Authentication must be used and the password must be changed annually where possible.

13. Monitoring and Logging of Activities (logs)

Below are the criteria and procedures for monitoring and logging activities (logs) related to the security of information systems. The purpose is to ensure the active protection of [Organization Name] critical information assets.

1. Type of Logging:

- Definition of the types of activities to be logged, including but not limited to access attempts, changes to data structures, and risk analysis attempts.

2. Retention Period:

- Definition of the period for retaining logs, taking into account legal requirements and data recovery needs.

3. Storage Medium:

- Definition of the storage medium for logs, emphasizing security and effective information retrieval.

4. Activation on Critical Systems:

- Ensuring that logging is enabled on all critical information systems to ensure active monitoring.

5. Activation on All Systems:

- Security-related activity logging must be enabled on all systems to maintain a complete overview of activities.

6. Risk Analysis:

- Conducting risk analysis to determine which activities require special monitoring.

14. Best Technical Measures and Practices for Password Protection

- The use of a strong password and its frequent change are among the most important actions recommended to protect your accounts from malicious users.
- Keep all your passwords secret.

© CYberSynchorny, 2024

- Do not use the same password everywhere.
- An employee of [Organization Name] will NEVER ask you for any password.
    - Passwords must not be disclosed to ANYONE (supervisor, colleague, system administrator, friends, etc.). If anyone asks you for your password, report it immediately to the Security Officer.
- Passwords must be between 10 (ten) and 127 (one hundred and twenty-seven) characters long and contain at least 3 (three) of the 4 (four) different character types. Character types are:
    - Uppercase letters [A B C D E F … Z]
    - Lowercase letters [a b c d e f … z]
    - Numbers [0 1 2 3 4 5 6 7 8 9]
    - Special characters [( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > . ? /)]
- Passwords provided by administrators, suppliers and system manufacturers must be changed immediately.
- Passwords must not be written down or stored unless strong protection mechanisms are used.
- Passwords must not be identical to the user's account name (username).
- Passwords must not be common words (from a dictionary) or based on personal information of the user (e.g. family names, car make, team, etc.).
- Passwords must not be sequential characters (e.g. 12345, 54321, qwerty, abcde, etc.).
- The "Remember Password" feature of applications (Internet Explorer, Firefox, Google Chrome, etc.) must be disabled.
- Where feasible or deemed necessary, two-factor authentication technology must be used, combining passwords with smart cards and/or biometrics.

15. Review

Documents related to Access Control must be reviewed and updated at least annually or in the event of significant changes to the [Organization Name] environment (e.g. Organizational structure, business activities and market trends, legal and regulatory requirements and compliance requirements, implementation of new systems, new risks, emerging threats, etc.).

16. References

Category	ID	Control	Control Objective
Identity and Access Management	IAM1	Role-based access control	To verify user authenticity and authorization, based on least privilege and Organizational roles and responsibilities.

© CYberSynchorny, 2024

Identity and Access Management	IAM2	Control of external access	To ensure adequate measures are in place for external access to Organizational resources.
Identity and Access Management	IAM3	Management of privileged users	To ensure adequate measures for users who have privileged access to Organizational resources, systems and networks.
Identity and Access Management	IAM4	Strong identity verification measures	To ensure that the identity of authorized individuals is verified securely using strong authentication measures.
Identity and Access Management	IAM5	Credential management	To ensure secure credential management for access to corporate resources and secure user identity verification for the use of Organization services.
Identity and Access Management	IAM7	Identity life cycle management	To ensure that roles and identity approval reflect the life cycle of the user's identity.

© CYberSynchorny, 2024

4.7 Tool 7 - Vulnerability and Patch Management Policy

[Organization Name]

THREAT - VULNERABILITY MANAGEMENT AND HARDENING POLICY

© CYberSynchorny, 2024

Table of Contents

1. Purpose
2. Scope of Application
3. Document Recipients
4. Roles and Responsibilities
4.1. Responsibilities of [Organization Name] security Executive Management (Cyberspace Directorate)
4.2. Responsibilities of the Information and Data Security Officer
4.3. Responsibilities of the [Organization Name] security Manager
4.4. Responsibilities of the Incident Response & Threat Intelligence Team
4.5. Responsibilities of the Steering Committee
4.6. Responsibilities of the Systems Architect
4.7. Responsibilities of the Operations Manager
4.8. Responsibilities of Engineers
4.9. Responsibilities of [Organization Name] Computer Users
5. Hardening Policy
5.1. General Principles
5.2. Security Risk Assessment
5.3. Stages of Information Security Audits
5.4. Vulnerability Identification
5.5. Conduct of Information Security Audits
5.6. Vulnerability Assessment and Penetration Testing
5.7. Distinction between Vulnerability Assessment and Penetration Testing
5.8. Management and Reporting of Information Security Audit Findings
5.9. Vulnerability Management 1
5.9.1. Management of Remedial Actions 1
5.9.2. Documentation of Vulnerability Management
5.10. Implementation of the Hardening Policy in the [Organization Name]
5.10.1. Hardening Practices
5.11. Training and Awareness
6. Policy Verification and Review
7. Obligation of Implementation
8. Disciplinary Sanctions for Non-Compliance

© CYberSynchorny, 2024

1. Purpose

The purpose of this Threat - Vulnerability Management and Hardening Policy is to establish a valid and robust framework for the identification, control and assessment of vulnerabilities and threats affecting the systems of the [Organization Name], with the objective of taking timely corrective measures to eliminate potential risks, as well as to define the steps followed for the implementation of the general hardening policy on the information systems of the [Organization Name].

2. Scope of Application

This Policy applies to all employees, contractors and third parties who have access to the infrastructures of the [Organization Name].

This Policy recognises the necessity of establishing a framework that includes basic principles and rules for the management of threats and vulnerabilities that affect the operation of the [Organization Name], as well as a comprehensive set of measures and procedures aimed at enhancing the security of information systems.

3. Document Recipients

- [Organization Name] security Analyst L1 (Security Analyst Level 1)
- [Organization Name] security Analyst L2 and L3 (Security Analyst Level 2 & Level 3)
- [Organization Name] security Manager
- Systems Architect
- Operations Manager
- [Organization Name] security Executive Management (Cyberspace Directorate)
- Engineer
- Incident Response & Threat Intelligence Team
- Steering Committee
- Information Systems Technician
- Helpdesk Technicians (Helpdesk Team)
- Infrastructure Systems Administrator
- Information and Data Security Officer
- [Organization Name] security Computer Users
- Data Protection Officer (DPO)

4. Roles and Responsibilities

Clearly defined roles and responsibilities are of critical importance for the development and achievement of a successful framework in relation to Information Security.

The Information and Data Security Officer, together with the [Organization Name] security Manager and the Incident Response & Threat Intelligence Team, are responsible for implementing and enforcing the Threat and Vulnerability Management and Hardening Policy.

© CYberSynchorny, 2024

4.1. Responsibilities of [Organization Name] security Executive Management (Cyberspace Directorate)

The main responsibilities of the [Organization Name] security Executive Management (Cyberspace Directorate) include the approval and review of the Threat and Vulnerability Management and Hardening Policy, as well as the creation of the necessary conditions to prevent the occurrence of any vulnerability in the [Organization Name].

Finally, they are responsible for decision-making concerning the imposition of sanctions in cases of disciplinary offences related to the improper implementation of this Policy.

4.2. Responsibilities of the Information and Data Security Officer

The main responsibilities of the Information and Data Security Officer include the maintenance and updating of this Policy, based on the recommendations of the [Organization Name] security Manager and the Incident Response & Threat Intelligence Team.

The Officer also actively participates in staff training regarding the implementation of the Policy.

4.3. Responsibilities of the [Organization Name] security Manager

The main responsibilities of the [Organization Name] Manager include participating in the identification, management and assessment of potential vulnerabilities that may arise during the operation of the [Organization Name].

In cooperation with the Incident Response & Threat Intelligence Team, the [Organization Name] Manager is responsible for managing and assessing each incident and its subsequent consequences.

The [Organization Name] security Manager is responsible for taking measures to prevent the recurrence of similar incidents.

Furthermore, the [Organization Name] security Manager designs and implements risk management analysis relating to the protection of the [Organization Name]'s information and data, in order to investigate the root causes of incidents and determine the corrective actions required.

4.4. Responsibilities of the Incident Response & Threat Intelligence Team

The main responsibilities of the Incident Response & Threat Intelligence Team include ensuring control, coordination and decision-making capability in order to address vulnerabilities and threats.

4.5. Responsibilities of the Steering Committee

The Steering Committee plays a critical role in supervising and guiding [Organization Name] activities so as to ensure alignment with the strategic objectives of the Service and compliance requirements.

The Steering Committee provides the strategic direction, coordination and oversight required to ensure the resilience and effectiveness of the [Organization Name] in protecting systems against threats and vulnerabilities, as well as the continuous improvement of security.

4.6. Responsibilities of the Systems Architect

The Systems Architect is responsible for the proper operation of the [Organization Name] security infrastructure.

© CYberSynchorny, 2024

They are experts with extensive experience in designing large-scale protection solutions. The role of the Systems Architect is to adapt all systems so that they fit the specific characteristics of the government network and enable maximum performance.

The Systems Architect designs the security architecture of the systems and ensures that the infrastructures comply with hardening best practices, i.e. reducing attack surfaces through access control, proper system configuration, and limiting services and resources to those strictly necessary.

The Systems Architect selects, designs and integrates vulnerability detection and risk management systems and contributes to the selection and integration of tools that analyse and monitor the latest threats (threat intelligence feeds), thus enabling the [Organization Name] security to prevent attacks based on timely information.

4.7. Responsibilities of the Operations Manager

The main responsibilities of the Operations Manager include monitoring and updating the physical and logical access of [Organization Name] security users.

Always with the consent of the [Organization Name] security Manager, the Operations Manager informs the relevant parties of any modification to user access rights or the termination of a user's access.

The Operations Manager is responsible for the continuous monitoring of systems and networks for threats, coordinating the [Organization Name] security team to ensure timely response to suspicious activities or attacks.

The Operations Manager cooperates with the Systems Architect and other technical teams to prioritise the vulnerabilities that must be remediated based on their impact and risk, while also overseeing the implementation of the hardening strategies designed by the Systems Architect, ensuring that they are applied across all systems and that security levels remain high.

The Operations Manager is the link between the Organizational functioning of the [Organization Name] security and the technical management of threats, vulnerabilities and hardening.

They ensure that the strategies designed by security architects are implemented on a daily basis, organise the [Organization Name] security team, monitor threats in real time and guide the team in the event of security incidents.

4.8. Responsibilities of Engineers

Each engineer in the [Organization Name] security is responsible for the proper operation of systems, the protection of infrastructures and the reduction of risks through the identification of vulnerabilities and the application of best practices to harden systems.

4.9. Responsibilities of [Organization Name] security Computer Users

The main responsibilities of end users include the proper implementation of this Policy, as well as reporting any vulnerability that comes to their attention.

© CYberSynchorny, 2024

5. Hardening Policy

5.1. General Principles

Taking into account the frequency of changes in Information Systems, the continuous development and integration of new systems, and the evolving threat landscape, the timely identification and management of vulnerabilities is highly important and can contribute significantly to effective risk management.

Technical vulnerabilities or weaknesses may arise from:

- Errors or omissions in system configuration
- Software or firmware vulnerabilities which may be due to outdated versions or even current versions in which weaknesses have been discovered
- Errors or failures in the architecture, structure and configuration of systems that increase their exposure to risks and threats
- Legacy systems with outdated architectures

All of the above can create security gaps in the [Organization Name] security infrastructures, which may be exploited to obtain unauthorised access or to perform malicious activities.

Therefore, the Cyberspace Directorate must take the necessary protective measures to ensure the timely identification, assessment and effective management of technical vulnerabilities affecting the information systems.

The [Organization Name] security Manager and System Administrators monitor developments in system vulnerabilities, new threats and the evolving threat landscape in general.

5.2. Security Risk Assessment

This Policy focuses on the identification and limitation of threats. Common policies include the implementation of updated threat detection algorithms and continuous staff training.

In addition, protection against vulnerabilities requires frequent updating and upgrading of systems and software in order to address security weaknesses.

The [Organization Name] security Manager is responsible for the design and implementation of Security Risk Assessments, in line with the [Organization Name]'s Information Security Principles and Strategy, in order to identify, assess and manage risks that threaten the security of systems and to ensure compliance with internal and external regulatory requirements.

Information risk assessments must be based on a valid and properly structured methodology, which indicatively consists of the following stages:

- Initiation and Planning
- Identification and Evaluation of Information Systems
- Assessment of Threats and Vulnerabilities
- Impact Analysis
- Identification and Assessment of Security Risks
- Reporting and appropriate Communication of Security Risks
- Continuous Risk Monitoring and Submission of Supplementary Reports

© CYberSynchorny, 2024

5.3. Stages of Information Security Audits

Information Security Audits shall follow a well-structured life cycle, which includes the following stages:

- Initiation and definition of the scope of the audit
- Planning
- Conduct of the audit and documentation
- Reporting
- Follow-up

5.4. Vulnerability Identification

Within the framework of vulnerability identification, regular security and vulnerability assessments are carried out to ensure that information systems are not exposed to threats arising from unauthorised changes, lack of security updates or the emergence of new types of attacks.

Ad hoc security audits shall be carried out in cases where:

- New Information Systems are to be introduced/connected into the environment of the [Organization Name].
- There is suspicion of security gaps in the [Organization Name] security Information Systems (new threats, security incident or internal audit findings, etc.)
- Remediation actions have been carried out to address identified vulnerabilities or security incidents, in order to verify that they have been successfully resolved

5.5. Conduct of Information Security Audits

The frequency of the various types of audits must be determined taking into account applicable regulatory requirements and in accordance with the risk level and classification of the Information System and infrastructure under review.

Systems and infrastructures deemed critical and/or at higher risk must be audited more frequently and more thoroughly compared to those at lower risk.

In addition to scheduled security audits, ad hoc audits may also be conducted in the following cases:

- Before migrating a critical system or application to the production environment, with particular emphasis on those accessible from the internet (internet-exposed systems)
- After the implementation of significant changes/modifications to Information Systems and/or infrastructures
- Following a Security Incident

Furthermore, the [Organization Name] security Manager, within the scope of their role and responsibilities, may conduct or schedule, with the involvement of third parties, ad hoc security audits.

If, during the audits, significant issues arise in critical applications in the production environment, the audits must be temporarily halted in order to identify the cause of the problem and/or adjust the way in which the audits are conducted.

© CYberSynchorny, 2024

If weaknesses are identified that may cause operational issues or unauthorised access to classified information, the team conducting the audits must obtain renewed explicit authorization from the [Organization Name] security Manager before proceeding.

Any vulnerabilities or security gaps assessed as critical must be reported immediately to the [Organization Name] security Manager in order for immediate mitigation actions to be taken.

5.6. Vulnerability Assessment and Penetration Testing

To be effective, the conduct of penetration tests must include various stages such as network reconnaissance, identification of systems and services, vulnerability scanning, exploitation in the case of intrusion tests, report drafting, recommended remediation actions based on findings, as well as follow-up and re-testing to ensure that the risk has been mitigated or eliminated.

New systems or applications integrated into the environment must be subjected to penetration tests and internal and/or external vulnerability assessments, particularly if they are connected to the Internet.

5.7. Distinction between Vulnerability Assessment and Penetration Testing

Vulnerability assessment and penetration testing are two critical information security processes used in the [Organization Name]. Despite their similarities, they differ significantly in purpose, methodology and outcomes. More specifically:

- **Vulnerability Assessment:** The primary objective of vulnerability assessment is the identification, recording and prioritisation of vulnerabilities or weaknesses in systems, applications and networks. This process focuses on identifying potential attack points without attempting to exploit them, using automated vulnerability scanning tools that systematically check systems for known weaknesses, such as outdated software or configuration errors. The result is a list of identified vulnerabilities, along with information about their severity and recommendations for addressing them. It does not, however, provide information on whether these vulnerabilities can actually be exploited in practice.
- **Penetration Testing:** The aim of penetration testing is to exploit identified vulnerabilities in order to understand the actual risk they present. It simulates a real attack by an adversary to assess how vulnerable systems are. Penetration Testing involves not only the use of automated tools, but also human involvement, where security specialists use attack techniques to attempt to gain access to systems, steal data or compromise internal networks. The results of a penetration test describe how the vulnerabilities were exploited, which data or systems could be compromised, and propose specific measures to prevent similar attacks in the future.

5.8. Management and Reporting of Information Security Audit Findings

Upon completion of security audits, the team that conducted the audit shall prepare and submit to the [Organization Name] security Manager a report detailing the audit findings.

The findings must be presented in an understandable manner and, to a minimum, include the following information:

- Vulnerability title
- System/application in which the vulnerability was identified
- Purpose, scope and methodology of the specific audit
- Critical level of the vulnerability

© CYberSynchorny, 2024

- Detailed description of all findings, including explanation and criticality of all control weaknesses, exceptions, observations and violations recorded during the audit
- Type of vulnerability (misconfiguration, default settings, unused protocols, outdated versions, etc.)
- Summary of proposed remedial actions to address each audit finding

Additionally, for penetration tests or internal audits, the following must be documented:

- Methodology used and any tools applied
- Period during which the audits were conducted
- Estimated impact of the finding
- Recommendations for addressing vulnerabilities and security gaps
- Evidence of findings (screenshots, proof-of-concept)
- Any issues that arose or were caused during the conduct of the audits

5.9. Vulnerability Management

Vulnerability management within the [Organization Name] security framework is a critical process that ensures the resilience of information systems against known and emerging threats.

To be effective, this process must include clear procedures for planning, execution of remedial actions and documentation.

The [Organization Name] security Manager analyses vulnerabilities in order to assess their criticality for the Cyberspace Directorate.

To address vulnerabilities, the [Organization Name] security Manager cooperates with System Administrators and the Incident Response & Threat Intelligence Team.

Vulnerability management in the [Organization Name] security includes the following steps:

- **Planning Remedial Actions:** Planning of remedial actions is critical for the prompt and organised handling of identified vulnerabilities.
- **Prioritisation:** Vulnerabilities are prioritised based on severity (e.g. high, medium, low), taking into account additional factors such as the likelihood of exploitation and the impact on critical systems.
- **Resource Allocation:** Assignment of responsible persons for each vulnerability according to their expertise (e.g. system administrators, analysts, etc.).
- **Definition of Communication Points:** Definition of communication points for feedback and issue resolution.

5.9.1. Management of Remedial Actions

The execution of remedial actions is the process of implementing fixes to address vulnerabilities.

The implementation of remedial actions includes applying available patches, ensuring that they have been properly installed on all critical systems.

In addition, security configurations identified as vulnerable are verified and, where an immediate fix cannot be applied, compensating controls are implemented (e.g. access restrictions, enhanced monitoring).

Finally, testing of fixes is carried out to ensure that vulnerability has been addressed without adversely affecting other functionalities, and systems are reassessed to confirm the elimination of the vulnerability.

© CYberSynchorny, 2024

5.9.2. Documentation of Vulnerability Management

Documentation is essential for maintaining records of actions taken and for assessing the effectiveness of the vulnerability management process.

This includes recording all identified vulnerabilities in the management system with details such as date of identification, severity and responsible department.

For this purpose, regular reports are prepared for [Organization Name] security Executive Management (Cyberspace Directorate), containing statistics on the number of vulnerabilities, the progress of remediation and any outstanding issues.

5.10. Implementation of the Hardening Policy in the [Organization Name]

The Hardening Policy describes the steps followed for the information systems of the [Organization Name] security in order to enhance system security by reducing vulnerabilities and potential attacks.

This Policy applies to all information systems and networks of the [Organization Name]. Within the [Organization Name] security context, the hardening policy aims to strengthen system security.

Before applying the hardening policy, a detailed analysis of information system vulnerabilities must be carried out. This includes identifying potential vulnerabilities, misconfigurations and other potential points of entry for attacks.

Hardening measures must be applied to all [Organization Name] security information systems in accordance with defined configurations. This includes:

- Changing default credentials
- Applying necessary software updates
- Modifying operating system and application settings
- Ensuring that required services are enabled
- Disabling non-essential services to reduce the attack surface

Security settings must be reviewed and applied in line with the best security practices and updated whenever necessary.

When applying measures, the impact on system functionality must be taken into account and the possibility of rollback in case of issues must be evaluated.

5.10.1. Hardening Practices

Hardening practices include:

- Restricting system access rights to minimise the risk from unauthorised users
- Continuous review and updating of firewall rules to protect against unwanted traffic
- Frequent checks to identify and remediate system vulnerabilities
- Use of automated tools to implement continuous monitoring and reinforcement of security policies
- Strengthening monitoring processes for prompt detection of unusual activities and rapid response to potential threats

© CYberSynchorny, 2024

These practices contribute to enhancing [Organization Name] security, protecting systems from potential risks and enabling more effective response to threats.

After the implementation of hardening measures, systems must be continuously monitored to determine the effectiveness of the measures. Access accounts, configurations and updates must be regularly checked to ensure system security.

5.11. Training and Awareness

Training staff in threat and vulnerability recognition and management is vital for the proper functioning of the [Organization Name].

Users and staff must be trained in the proper use of new security measures.

For this reason, continuous training sessions on vulnerability identification are conducted.

Any questions or requests for clarification regarding the content of this Policy must be addressed to the Information and Data Security Officer and the [Organization Name] security Manager.

6. Policy Verification and Review

The Threat and Vulnerability Management and Hardening Policy is periodically reviewed and verified to ensure that it remains applicable and effective.

During this review, new potential changes arising since the previous version are analysed. New vulnerabilities must be identified and incorporated into hardening measures.

7. Obligation of Implementation

The Threat and Vulnerability Management and Hardening Policy constitutes an integral part of the security policy of the [Organization Name].

All parties involved are obliged to comply with this Policy in order to ensure the security of the Service's information systems and data.

8. Disciplinary Sanctions for Non-Compliance

Any breach of this Policy, as well as any violation thereof, will be treated with strictness and may result in disciplinary measures, including the initiation of legal action, depending on the severity of the violation.

Data subjects concerned have the right to submit questions regarding this Policy and to request clarifications from the Information and Data Security Officer.

This Policy enters into force as of [Approval Date] and is periodically reviewed to ensure its alignment with the needs and requirements of the Service.

© CYberSynchorny, 2024

4.8 Tool 8 - Network Security Policy

[Organization Name]

NETWORK AND COMMUNICATIONS SECURITY POLICY

© CYberSynchorny, 2024

Table of Contents

1. Purpose
2. Scope of Application
3. Document Recipients
4. Roles and Responsibilities
4.1 Responsibilities of [Organization Name] security Executive Management (Cyberspace Directorate)
4.2 Responsibilities of the Information and Data Security Officer
4.3 Responsibilities of the [Organization Name] security Manager
4.4 Responsibilities of the Incident Response & Threat Intelligence Team
4.5 Responsibilities of the Steering Committee
4.6 Responsibilities of the Systems Architect
4.7 Responsibilities of the Operations Manager
4.8 Responsibilities of Engineers
4.9 Responsibilities of [Organization Name] security Computer Users
5. Policy
5.1 Network Security Principles
5.2 Network Architecture and Network Segmentation
5.3 Network Information – Data Ingress and Egress Policy
5.4 Selection of Network Security Controls
5.5 Prerequisites for Connecting Devices to the Network
5.6 Security Audit of Network Equipment
5.7 User Training
6. Policy Verification and Review
7. Obligation of Implementation
8. Disciplinary Sanctions for Non-Compliance

© CYberSynchorny, 2024

1. Purpose

This Network and Communications Security Policy recognizes the need to establish a framework that includes the fundamental principles and rules for safeguarding network security at the level of [Organization Name] security infrastructures. Within this context, the Policy provides guidelines relating to network security architecture, the selection and implementation of adequate security mechanisms and controls, as well as the management of networks, in order to prevent any type of unauthorised access and to ensure the availability and integrity of [Organization Name] security information.

In addition, it describes the way in which information ingress and egress policies to and from the network are managed, in order to ensure a secure and regulatory-compliant flow of information across the network.

2. Scope of Application

This Policy applies to all employees, contractors and third parties who have access to the network infrastructures of the [Organization Name].

This Policy recognises the need to establish a framework which includes fundamental principles and rules for the management of networks, in order to prevent any kind of unauthorised access to them, which could affect the operation of the [Organization Name].

3. Document Recipients

- [Organization Name] security Analyst L1 (Security Analyst Level 1)
- [Organization Name] security Analyst L2 and L3 (Security Analyst Level 2 & Level 3)
- [Organization Name] security Manager
- Systems Architect
- Operations Manager
- [Organization Name] security Executive Management (Cyberspace Directorate)
- Engineer
- Incident Response & Threat Intelligence Team
- Steering Committee
- Information Systems Technician
- Helpdesk Technicians (Helpdesk Team)
- Infrastructure Systems Administrator
- Information and Data Security Officer
- [Organization Name] Computer Users
- Data Protection Officer (DPO)

4. Roles and Responsibilities

Clearly defined roles and responsibilities are of critical importance for the development and achievement of a successful framework in relation to Information Security and the maintenance of network and communications security.

© CYberSynchorny, 2024

The Information and Data Security Officer together with the [Organization Name] security Manager is responsible for the implementation and enforcement of this Policy.

4.1 Responsibilities of [Organization Name] security Executive Management (Cyberspace Directorate)

The main responsibilities of the [Organization Name] security Executive Management (Cyberspace Directorate) include the approval and review of this Network and Communications Security Policy and the establishment of the necessary conditions for preventing the occurrence of any network-related issues.

Finally, [Organization Name] security Executive Management is responsible for decision-making concerning the imposition of sanctions in cases of disciplinary offences related to the improper implementation of this Policy.

4.2 Responsibilities of the Information and Data Security Officer

The main responsibilities of the Information and Data Security Officer include the maintenance and updating of the Network and Communications Security Policy, based on the recommendations of the [Organization Name] security Manager and the Incident Response & Threat Intelligence Team.

The Officer also actively participates in staff training regarding the implementation of this Policy.

4.3 Responsibilities of the [Organization Name] security Manager

The main responsibilities of the [Organization Name] security Manager include active participation in the identification and overall restoration of the network in the event of a problem.

If an issue arises in the [Organization Name] security network, the [Organization Name] security Manager together with the Incident Response & Threat Intelligence Team is responsible for managing and assessing the incident as well as its subsequent impact.

The [Organization Name] security Manager is responsible for adopting appropriate measures to restore the network.

4.4 Responsibilities of the Incident Response & Threat Intelligence Team

The main responsibilities of the Incident Response & Threat Intelligence Team include ensuring control, coordination and decision-making capability in order to address network security incidents in an effective and coordinated manner.

4.5 Responsibilities of the Steering Committee

The Steering Committee is responsible for the design of network architecture, ensuring the security of communications and making critical decisions relating both to day-to-day operations and to the long-term security strategy of the [Organization Name].

Its responsibilities include the strategic planning of networks and communications, the selection of appropriate technologies and decision-making in critical situations.

© CYberSynchorny, 2024

4.6 Responsibilities of the Systems Architect

The responsibilities of the Systems Architect in the [Organization Name] security are multi-faceted and include both technical expertise and strategic planning for the management of security infrastructures and services.

The main responsibilities of the Systems Architect include:

- Developing secure network architectures
- Designing network topologies
- Supervising and managing firewall, IDS/IPS, SIEM and related systems
- Managing external connections
- Integrating and managing security technologies
- Planning and supervising upgrades and updates of network infrastructures

4.7 Responsibilities of the Operations Manager

The main responsibilities of the Operations Manager include monitoring and updating physical and logical access for [Organization Name] security users.

Their responsibilities also include organising, supervising and optimising the processes that ensure secure communications and the proper functioning of network infrastructures.

The Operations Manager oversees network operations, monitors network traffic management and communication protocols.

4.8 Responsibilities of Engineers

Engineers are responsible for the proper operation of [Organization Name] security systems and play a critical role in the management, protection and optimisation of network infrastructures and communications, aiming to enhance both network security and performance.

This position includes both technical and operational responsibilities, with emphasis on ensuring that the network remains protected against attacks and operates with high performance.

4.9 Responsibilities of [Organization Name] security Computer Users

The main responsibilities of users include the proper implementation of this Policy as well as the reporting of any non-compliance with the Policy that comes to their attention.

5. Policy

This Policy applies to all [Organization Name] networks, and specifically to:

- Internal virtual networks or infrastructures (VLANs)
- Contact points with external public networks or infrastructures (WANs) that are under the direct management of the [Organization Name]
- Contact points with external private networks (VPNs) that are under the direct management of the [Organization Name].

© CYberSynchorny, 2024

5.1 Network Security Principles

Each network infrastructure used or deployed must adhere to a set of fundamental principles, and in particular:

- It is designed, developed and configured in accordance with predefined security requirements and best practices for network security architecture design and technical security standards
- It provides the required level of confidentiality, integrity, availability and resilience
- It provides the necessary level of user access control, restricting users to the minimum level of access required to perform their duties
- It provides the required level of access control at the contact points between the internal network and external or third-party networks
- It provides the required level of performance, resilience, availability and reliability to meet the needs of the [Organization Name].
- It implements appropriate security safeguards (network devices, cabling, etc.)

The [Organization Name] network security policy defines the rules and procedures for protecting the network. This includes monitoring traffic, access management, threat control and other security initiatives.

More specifically, to maintain network security in the [Organization Name], the following actions are defined:

- **Threat Detection:** Rules are defined for detecting anomalies and threats in network traffic. Threat detection in the [Organization Name] security includes the use of intrusion detection tools, network traffic monitoring and log analysis. The use of techniques such as behavioural data collection and anomaly detection may also assist in addressing threats.
- **Perimeter Security Protection:** Policies are defined for blocking, access control and monitoring of peripheral devices. To protect network perimeter security in the [Organization Name], advanced firewalls, intrusion detection/prevention systems (IDS/IPS) and other detection tools are used. In addition, continuous updating of security policies, access control and network traffic monitoring contribute to preventing attacks.
- **Access Management:** Rules are defined for network access, including user rights and authorisations. For network access management in the [Organization Name], role-based access control (RBAC) is used, allowing access based on each user's role.
- **Traffic Monitoring:** Rules are defined for monitoring network traffic in order to detect unusual activities. For effective traffic monitoring in the [Organization Name], Network Security Monitoring (NSM) is used. This includes analysing traffic for anomalies, using IDS/IPS and reviewing user accounts. Detailed logging and analysis of network activity are essential for threat detection.
- **Cryptography and Data Protection:** Rules are defined for encryption regarding the security of the [Organization Name] network, using protocols such as HTTPS for encrypting communications. Additionally, data encryption is applied to storage and transmission of network packets.

5.2 Network Architecture and Network Segmentation

Ensuring the confidentiality, integrity and availability of information during transmission requires that the [Organization Name] security network architecture adheres to the following fundamental security principles:

- Security requirements are taken into account during the network design phase ("security by design")
- Use of multiple layers and different types of protection
- User access is granted with the minimum privileges assigned to each user

© CYberSynchorny, 2024

- Application of best practices and adherence to relevant technical standards for network and network device security, in order to ensure secure operation of the network infrastructure
- Application of specific technical security standards on network devices to safeguard them and the services they provide
- Limitation or, where possible, complete avoidance of single points of failure, as well as provision of sufficient network resources to ensure network availability
- Provision of Fail-Safe Systems which, in the event of specific types of failure, inherently respond in a way that causes no or minimal damage to the remaining network infrastructure
- The Cyberspace Directorate shall maintain documentation of the network architecture and network device configurations

For the protection of information, network segmentation must also be implemented. More specifically, segmentation is applied according to:

- Data transmission flows (e.g. from/to internal network, from/to external public network, from/to external private network)
- The physical location of users
- The logical environment in which the infrastructure resides

Network architecture design must be implemented in such a way as to ensure the high availability of critical network devices (e.g. border routers, core switches, firewalls), critical communication links (e.g. leased lines from different providers) and internet-related services.

5.3 Network Information – Data Ingress and Egress Policy

To safeguard information entering and leaving the [Organization Name] security networks, the Incident Response & Threat Intelligence Team, in cooperation with the [Organization Name] security Manager, has defined specific rules for the ingress and egress of information to and from the [Organization Name] security networks, in accordance with Service requirements and procedures.

The aim is to ensure the secure and regulatory-compliant flow of information through the network.

More specifically:

- Information is classified according to its level of sensitivity. This helps determine the restrictions and security measures required for its ingress and egress.
- Necessary restrictions are implemented, including encryption, digital signatures, authenticity checks, etc.
- Before information is imported or exported, checks are performed to verify the origin and destination of the data, in order to prevent unwanted information flows and protect against attacks such as data blocking or misuse.
- The authorisations required for information ingress and egress under the Policy are strictly enforced. Users or user groups must have the necessary authorisations to perform these actions.
- In the event of a serious breach or incident, an incident analysis is carried out to identify root causes and to take preventive measures, and relevant stakeholders are informed of the incident and the measures taken.

© CYberSynchorny, 2024

5.4 Selection of Network Security Controls

For the optimal selection of appropriate security controls and mechanisms for the network infrastructure, periodic assessments of network security risks are conducted.

The results of the risk assessments guide the selection of suitable security mechanisms that provide an appropriate level of protection.

Security mechanisms and controls are implemented based on the network's access level.

According to the classification level of each network and the results of the risk assessment, a combination of the following security mechanisms/controls shall be implemented:

- Web Application Firewalls and Database Firewalls
- Network Detection and Response (NDR) systems
- Intrusion Detection/Prevention Systems (IDS/IPS)
- IDS systems for detecting malicious and unauthorised access points to the network/internet
- Protection against DoS/DDoS attacks
- Web content filtering
- Protection against malicious software (EDR)
- Data Loss Prevention (DLP) mechanisms
- Secure connectivity (e.g. VPN, SSH, HTTPS)
- User access controls (e.g. strong authentication)
- Use of port security controls for critical systems
- Implementation of Network Access Control (NAC) within the internal network
- Periodic review of firewall rules

5.5 Prerequisites for Connecting Devices to the Network

Connecting devices and computers to the [Organization Name] security network is particularly critical for [Organization Name] security; therefore, certain prerequisites have been established. Specifically:

- **Asset Management Registration:** Every device or computer connected to the [Organization Name] security network must be registered in the Asset Management system. This includes details such as model, operating system, responsible user and the device's unique identifier (e.g. MAC address).
- **Updated Software:** Devices must have all current patches and software updates installed (operating system and applications). Failure to update may leave security gaps that can be exploited by malicious actors.
- **Installed Malware Detection Tool:** Devices must have up-to-date Endpoint Detection and Response (EDR) software installed for malware detection and mitigation.
- **Prohibition of Default Passwords:** All devices and applications must not use default passwords.
- **Continuous Monitoring:** Devices must be configured to support monitoring and logging of all activities to enable timely threat detection and response.
- **Access Control Mechanisms:** Mechanisms such as Network Access Control must be in place to ensure that only authorised devices connect to the network.

© CYberSynchorny, 2024

The implementation of these prerequisites will contribute to improving the overall security of the network and to protecting the [Organization Name] security from potential threats.

5.6 Security Audit of Network Equipment

Periodic security audits are conducted for all network infrastructures in order to confirm compliance with standards and best practices.

Furthermore, changes to network architecture, equipment and security configurations must be authorised, implemented and documented in accordance with the Change Management Policy.

5.7 User Training

Training users in the Network and Communications Security Policy is critical for the prevention and handling of cyber threats.

The purpose of this Policy is to ensure understanding of the importance of complying with the rules and restrictions in order to safeguard data security.

A fundamental element is understanding attack techniques as well as the ability to detect and respond to them.

6. Policy Verification and Review

The Network and Communications Security Policy is periodically reviewed and verified to ensure that it remains applicable and effective.

During this review, potential new changes arising since the previous version are analysed. This is done to ensure that the Policy remains aligned with the latest security requirements.

7. Obligation of Implementation

The Network and Communications Security Policy forms an integral part of the overall security policy of the [Organization Name].

All users and relevant stakeholders are obliged to comply with this Policy for the protection of information and the security of the [Organization Name] security network.

The Incident Response & Threat Intelligence Team monitors compliance with the Policy by conducting regular checks and assessments to ensure that the Policy rules are observed.

8. Disciplinary Sanctions for Non-Compliance

Any breach of this Policy, as well as any violation thereof, will be treated with strictness and may result in disciplinary measures, including the initiation of legal proceedings, depending on the severity of the violation.

Data subjects concerned have the right to submit questions regarding this Policy and to request clarifications from the Information and Data Security Officer.

This Policy enters into force as of [Approval Date] and is periodically reviewed to ensure its alignment with the needs and requirements of the Service.

© CYberSynchorny, 2024

4.9 Tool 9 - Systems & Applications Security Policy

[Organization Name]

SYSTEM & APPLICATIONS SECURITY POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
   1.1 Purpose
   1.2 Scope of Application
2. Systems & Applications Security Policy
   2.1 Malware Protection
   2.2 System Hardening and Basic Security Requirements
   2.3 Mobile Device Security
   2.4 Other Recommended Measures for Protecting Mobile Devices / Portable Equipment
   2.5 Operating System Protection
3. Application Security
4. Application Lifecycle
   4.1 Purpose
   4.2 Requirements Definition
   4.3 Design
   4.4 Development and Implementation
   4.4.1 Environment Segregation
   4.5 Testing and Installation
   4.6 Application Installation Measures
   4.7 Application Manuals
   4.8 User Training
   4.9 Change Management Process
5. Outsourcing Development to Third Parties
6. Review
7. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

This document contains indicative Policy Terms for the protection of the Organization's information assets and technological infrastructure against a range of threats. It also sets out terms to ensure that all applications and systems used within [Organization Name] are properly designed, implemented, maintained and protected, as they constitute an integral part of the smooth operation of [Organization Name].

This Policy aims, among other things:

- To protect the confidentiality, integrity and availability of the data processed and stored in applications and systems.
- To define security requirements for the design, development, testing and maintenance of applications and systems.
- To mitigate risks associated with various vulnerabilities by enforcing the implementation of secure programming practices, patch management and regular vulnerability assessments.
- To ensure compliance with standards related to application and system security (e.g. coding standards).
- To promote accountability and security awareness among developers, administrators and end users, fostering a culture of secure systems management.

1.2 Scope of Application

The Systems and Applications Security Policy of [Organization Name] cover all information systems, applications, operating systems and related components that are used, developed, managed or hosted by [Organization Name], including those provided by third parties to [Organization Name] or managed entirely by external partners.

It applies to all stages of the lifecycle of applications and systems – design, development, testing, maintenance and final decommissioning.

2. Systems & Applications Security Policy

2.1 Malware Protection

[Organization Name] protects its systems and applications from malware threats through preventive measures. This includes the implementation of antivirus and anti-malware solutions, regular scanning, timely application of patches and monitoring of suspicious activities. Specifically:

- [Organization Name] has established, implements and maintains processes / policy and measures for protecting systems from malware and malicious code, in order to ensure the confidentiality, integrity, availability and authenticity of information.
- All [Organization Name] endpoint devices have antivirus software installed and kept up to date, managed via a centralised platform. The centralised platform enables continuous monitoring and automatic updating of the responsible personnel with regard to virus and malicious code protection across all systems (workstations, servers, mobile devices, firewalls, etc.).
- On all endpoint devices, where feasible, antivirus protection mechanisms, intrusion detection and other advanced security mechanisms such as web filtering must be enabled via the antivirus software.
- The antivirus software must be configured appropriately to perform the following:

© CYberSynchorny, 2024

- automatic scanning of incoming items,
- scanning and blocking electronic communications containing malicious code or file types with increased risk,
- regular scans of information storage locations,
- disabling auto-run / auto-start of software from various media,
- alerting in cases where a threat is detected,
- automatic deletion or quarantine of detected threats,
- automatic updating of the software and signatures.

- [Organization Name] has additionally implemented antimalware solutions that include capabilities for vulnerability detection and anti-exploitation filters to enhance system security.
- Where feasible, [Organization Name] implements anti-tampering protection mechanisms to prevent the disabling of protection by unauthorised individuals.

2.2 System Hardening and Basic Security Requirements

[Organization Name] ensures that all applications and systems are securely configured through a systematic process of system service hardening (system hardening). This includes the removal of unnecessary software, disabling of unused services and configuration of security settings in order to minimise vulnerabilities. More specifically, the following measures are taken:

- Where feasible, services / supporting programmes that are not necessary are removed from [Organization Name] systems.
- Host-based firewalls are installed on [Organization Name] endpoint devices, where feasible, to protect against malicious code, control the use of removable media, etc.
- Software installation or configuration is carried out exclusively by specially authorised [Organization Name] personnel.
- [Organization Name] ensures that non-privileged users do not have the ability to disable or modify security settings on systems.
- [Organization Name] ensures that non-privileged users do not have the ability to install software on critical systems.
- For each system of [Organization Name], an owner has been identified who, in cooperation with other technical personnel, is responsible for the roles requiring access and the corresponding level of access.
- For each system of [Organization Name], a record (golden copy) must be available, which includes the most up-to-date, stable and secure configuration.
- [Organization Name] must follow secure configuration guidelines provided by the manufacturer or other trusted sources (e.g. CIS Benchmarks) for the protection of its systems.

2.3 Mobile Device Security

Mobile devices and other portable equipment are subject to significant risk because they can easily be moved outside the premises of [Organization Name]. Consequently, the likelihood of loss, damage or theft increases. Given the high risk, all mobile devices / portable equipment that have access to [Organization Name] data or

© CYberSynchorny, 2024

systems must comply with established security protocols, including device encryption, secure authentication and remote wipe capabilities. Specifically, the following measures are taken:

- [Organization Name] implements and maintains mobile device security measures to ensure the confidentiality, integrity and availability of the information handled.
- All mobile devices must have adequate measures to protect against theft and data loss (e.g. device-level encryption, strong authentication, secure communication and networking (VPN).
- All mobile devices (including their applications) that use [Organization Name] Organizational data must be managed by a central mobile device management system (MDM and MAM-type solutions).

2.4 Other Recommended Measures for Protecting Mobile Devices / Portable Equipment

- Only authorised personnel may use portable equipment on behalf of [Organization Name]. It is understood that such personnel must also comply with the Acceptable Use Policy.
- Portable equipment delivered to an authorised user is recorded in a relevant register. The equipment is returned in the event of termination of employment or when it is no longer required for the performance of duties.
- Only authorised portable equipment may be used on [Organization Name] premises.
- Use of authorised portable equipment for the user's personal benefit is prohibited.
- [Organization Name] reserves the right to monitor portable equipment, as well as the right to retrieve, modify, delete and back up any information stored on such equipment, without prior notice, where this concerns information security matters of the Organization.
- [Organization Name] reserves the right to revoke any related authorisation if the use of such device constitutes a source of risk for the security of [Organization Name] systems and information.
- Portable equipment must automatically lock when not in use for more than [XX] minutes.
- Where feasible, portable equipment must be protected by anti-malware software.
- Portable equipment must be protected by a local firewall, especially when it is connected to unknown and/or untrusted and/or public networks (see Network Security Policy).
- Portable equipment must be protected by Data Loss Prevention (DLP) software that detects and prevents unauthorised data transfers.

2.5 Operating System Protection

For the preparation and configuration of operating systems, a process for configuring baseline operating systems must be defined and followed. This process includes, among others, the following:

- Review of best practices for secure operating system configurations.
- Configuration of operating systems taking into account best practice secure configurations for each operating system (system hardening).
- Execution of functional and security testing.
- Annual review of operating systems. Any additional security configurations and security updates must be carried out / installed annually.

Furthermore, Operating Systems:

© CYberSynchorny, 2024

- Located on [Organization Name] internal networks, where feasible, must be members of a Domain.
- That must be exposed to an external network are recommended to be placed in a separate perimeter network segment, isolated and segregated from the rest of the internal network, providing an additional layer of security. If necessary, a separate Active Directory (AD) domain should be created specifically for DMZ systems, with no trust relationship with the internal domain.
- Must be synchronised with a central NTP (Network Time Protocol) time system for consistent time/date settings.
- Must have the latest security updates and upgrades installed, according to their criticality.
- Must have only [Organization Name]-authorised applications installed. Such applications must be kept up to date with the latest security patches.
- Default accounts such as “administrator”, “root”, “guest”, “default” must be disabled.
- Must be protected with security passwords. Passwords must comply with the Access Control Policy and use of MFA must be enforced where feasible.
- Hard disks must be encrypted where feasible.
- Only essential services must be enabled. Services that are not required for business purposes must be disabled, such as Bluetooth and WiFi services.
- Where feasible, boot from alternative sources other than the primary hard drive must be disabled.
- Must automatically lock after 15 minutes of inactivity, or 5 minutes for high-risk systemsMust be protected by anti-malware software.
- Must have remote access disabled when it is not necessary. Only authorised personnel should be able to access them remotely.
- Must have the local firewall enabled while only necessary ports should be open.
- Use of shared folders on such systems must be avoided. If shared folders are necessary, appropriate access rights must be defined and reviewed regularly.
- The autorun parameter must be disabled.
- For each software component, an owner must be identified who, in cooperation with other technical personnel, will determine the roles for which access to the software is required and the corresponding level of access.

3. Application Security

The security of customised applications is a key parameter of the overall cyber security framework of [Organization Name], ensuring that applications are designed, developed and maintained with strong protection against vulnerabilities and threats.

By integrating secure coding practices, test scenarios and continuous monitoring, [Organization Name] aims to protect applications against risks associated with information and cyber security. Specifically:

- [Organization Name] has established a Secure Development Lifecycle process. See Section 4 below.
- [Organization Name] has set security requirements for applications and software developed, which are taken into account in each new application or software development.

© CYberSynchorny, 2024

- In the final stages of development and before migration to the production environment, system tests must be conducted in accordance with defined criteria and requirements for quality, functionality and security.
- Separate development and production environments must be maintained.
- When conducting application development tests, anonymous data must be used.
- Where application development is outsourced to third parties, at a minimum security specifications that the application must meet must be provided. Sufficient guarantees, assurances and evidence confirming that these requirements are met must be requested prior to acceptance or operation of the application.
- [Organization Name] must have secure software development guidelines, specialised per programming language or development environment (coding standards), in line with international best practices.
- Risk assessments and/or threat profiling must be carried out during the design of software to determine appropriate security measures.
- Applications and software must be developed based on the "security and privacy by design" principles.
- At a minimum, the following must be carried out:
    - risk assessment at the initial stage of the project,
    - security testing and code review during the project development stages,
    - security and secure configuration assessment upon project delivery.
- There must be a complete separation of duties between personnel responsible for development, testing and production operation of systems.
- Software changes must be made via the change management process.

4. Application Lifecycle

In accordance with Decision K.D.P. 389/2020, [Organization Name] must ensure adequate security measures in the context of software development activities carried out by the Organization.

The management of the Software Development Life Cycle (SDLC) is a critical part of the development process. The SDLC refers to the sequence of processes and phases through which software passes from design to implementation, quality control, assurance, maintenance and, ultimately, decommissioning. Each phase has its own practices and procedures and is designed to ensure the quality, security and maintainability of the software throughout its lifecycle.

All applications must be accompanied by their lifecycle documentation. Particular emphasis must be given to the general security of the application and the protection of its data. At each stage of the lifecycle, security safeguards such as encryption must be used.

For each new application development, a separate project must be created and in each project security measures must be incorporated into the lifecycle. During an application lifecycle, at least the following phases/actions must be observed:

4.1 Purpose

- The application must be assessed and categorised according to an appropriate risk level.
- Bearing in mind information classification, new or revised applications must be assessed accordingly.

© CYberSynchorny, 2024

- The level of access required by user groups must be determined in line with the application's functionality.
- Any other security measures must be identified.

4.2 Requirements Definition

With regard to information security, for each application the following must be identified and recorded:

- User rights and roles according to their job position. Unnecessary rights must be revoked.
- Requirements for protection of the application against malicious software.
- Backup and recovery plan for the application and its information.
- Change Management process.
- Software development lifecycle management process.

4.3 Design

The design of each application must include fulfilment of the application requirements and how these are expected to be implemented. During the design phase, a risk assessment or threat profiling must be carried out and based on the results, suitable security measures must be designed.

Risk assessment and threat profiling are key elements of the application development process. Through risk assessment, the following must be performed:

- Identification and recording of potential risks for the software.
- Determination of the likelihood of each risk occurring and its impact on the proposed application.
- Ranking of risks based on their severity.

Through threat profiling, the following must be performed:

- Identification of potential threats in the software environment.
- Analysis of potential threats to the code, data and system vulnerabilities.

4.4 Development and Implementation

During application development, test plans and security penetration scenarios for the application must be carried out. Additionally, measures must be implemented for segregating software development and testing environments from the operational production environment.

4.4.1 Environment Segregation

Segregating application development environments from the production environment is important for the security, reliability and stability of systems. This is achieved by implementing appropriate measures, specifically:

1. **Infrastructure Segregation:** Application development is always carried out in a development environment, while the production environment resides in a separate environment. This segregation ensures that any errors or issues arising during development do not affect production code.
2. **Use of Database Copies:** During development, it is recommended to use copies of databases. It is important to carefully control use of these data so as not to affect the production database.

© CYberSynchorny, 2024

3. **Data Cleansing:** During transition from the development environment to the production environment, it must be ensured that the data are clean, free of information that should not exist there and which may have been incorrectly transferred from development.
4. **Deployment Rules:** A documented process must exist for transferring code and data from development/testing environments to the production environment.

These measures help maintain the security and stability of production systems while enabling effective software development and testing.

4.5 Testing and Installation

Functionality and security tests for the application must be conducted before the application is installed. If the application fails these tests, it must return to the initial stage of its lifecycle.

Any data used for testing must be anonymous and not linked to confidential or sensitive information.

To ensure anonymity and protection of sensitive information during testing, the Organization may take the following measures:

1. **Data Anonymisation:** Personal data used in tests must be anonymised (Data Masking & Anonymisation). Through this practice, elements that could lead to identification of individuals are removed or replaced.
2. **Use of Test Databases:** Special test databases containing dummy or anonymised data may be used instead of real customer or user data.
3. **Access Restriction:** Access restrictions must be enforced, and only the necessary personnel should have access even to sensitive data for testing purposes.
4. **Staff Training:** Staff involved in testing must be trained on the importance of protecting data anonymity and sensitivity.

Through these measures, [Organization Name] ensures that tests are performed securely and limits any violation of data anonymity.

4.6 Application Installation Measures

Prior to application installation, a detailed analysis of application requirements is carried out, taking into account its functionality, security needs and potential risks, in accordance with [AS1] of Decision K.D.P. 389/2020.

Specific access rights are defined and assigned to users based on the principle of least privilege. During installation, technical measures such as the use of signed applications, encrypted connections and controlled execution environments are applied.

During operation, applications are subject to continuous monitoring using behavioural analysis and activity visualisation tools and log monitoring systems. Furthermore, critical systems use advanced measures for modifying security settings, such as automatic updates and frequent vulnerability checks in accordance with [AS1] of Decision K.D.P. 389/2020.

4.7 Application Manuals

Application user manuals must be prepared, kept up to date and always maintained in their latest version.

© CYberSynchorny, 2024

4.8 User Training

The owner of each application must ensure that end users of the application are adequately trained prior to commencing use of the application.

Maintenance and Evaluation:
The application must be maintained and evaluated at regular intervals through Service Level Agreements (SLAs).

4.9 Change Management Process

For every application change, appropriate security measures are implemented, such as:

- Implementation of security measures to address identified risks and threats.
- Use of countermeasures such as encryption, intrusion detection, access restrictions and others.

Software control is performed via the change management process in accordance with Decision K.D.P. 389/2020:

- Changes to processes and information systems are implemented securely, without compromising the confidentiality, integrity, availability or authenticity of information.
- Confirmation that each new software version is compatible with the security measures in place.
- Risk assessment in the context of change requests and change design, taking into account appropriate security measures.

[Organization Name] must consider performing, at a minimum, a risk assessment at the initial stage of the project, conducting security tests and code review during project development stages, and carrying out a security and secure configuration assessment upon project delivery.

It ensures that the data used for testing is anonymous and not linked to confidential and sensitive information in the context of development activities.

5. Outsourcing Development to Third Parties

Where [Organization Name] outsources application development to third parties on its behalf, it must emphasise the importance of precise security specifications, guarantees and assurances regarding applications developed by third parties or used by the Organization. Specifically, it must:

1. Define precise security specifications that applications must meet in the requirements document (Request for Proposal – RFP). These may include aspects such as data protection, management of security threats and compliance with any regulatory standards.
2. Request in advance guarantees and assurances from the contractor or application provider that the security specifications are met. These guarantees may include application testing procedures, security reports and other assurances on correct and secure operation.

6. Review

The Systems and Applications Security Policy must be reviewed and updated at least annually or in case of significant changes in the environment of [Organization Name] or other needs, such as major changes in infrastructure or applications (e.g. deployment of new systems or decommissioning of old applications at the end of their lifecycle).

© CYberSynchorny, 2024

7. References

Category	ID	Measure	Objective of Measure
Category	ID	Control	Control Objective
Systems Security	SS1	Malware Protection	To ensure that Organizational assets are not affected by malware and malicious code.
Systems Security	SS2	System and Device Hardening and Basic Security Requirements	To minimise, as far as possible, the attack surface of information systems by reducing their functionality and features.
Systems Security	SS3	Mobile Device Security	To ensure appropriate security of mobile devices that have access to Organizational assets.
Systems Security	SS4	Application Configuration Management	To ensure appropriate management of applications used to access or process Organizational assets.

© CYberSynchorny, 2024

4.10 Tool 10 - Data Protection Policy

[Organization Name]

DATA PROTECTION POLICY

© CYberSynchorny, 2024

Table of Contents

Introduction
1.1 Purpose
1.2 Scope of Application

1. Data Protection Policy
   2.1 Data Lifecycle Management
   2.2 Classification and Labelling of Information
   2.3 Transfer and Exchange of Information
   2.4 Data Loss Prevention and Data Leakage Prevention
   2.5 Use of Cryptography
   2.6 Deletion or Destruction of Information
   2.7 Digital Signatures
2. Information Backups
3. Provisions in Contracts with Third Parties
4. Review
5. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

This document includes indicative Policy Terms for the data protection of [Organization Name] to ensure the confidentiality, integrity and availability of personal and sensitive data, in accordance with Decision K.D.P. 389/2020 and with the Cybersecurity Maturity Framework as published in the Decision on Network and Information Systems Security (Cybersecurity Maturity Controls) of 2024 (K.D.P. 245/2024).

This Policy describes how critical data of [Organization Name] are collected, stored, processed and protected.

The objectives of this Policy are as follows:

- Ensuring compliance for data security through alignment with regulatory requirements and applicable legislation (e.g. GDPR).
- Protection of Personal & Sensitive Data by preventing unauthorised access, processing, disclosure or loss.
- Establishment of various security controls through the implementation of technical, Organizational and physical security measures for data protection.
- Mitigation of risks related to data breaches and threats either from cyberspace or from internal threats (e.g. data leaks).

1.2 Scope of Application

The scope of the Data Protection Policy covers all critical information managed by [Organization Name]. This includes:

- All personal, sensitive and critical data of [Organization Name] that are stored, processed or transmitted within the Organization.
- All IT systems, databases, networks and cloud services that store or process sensitive information.
- Data in any form, e.g. electronic, paper-based or stored in the cloud.

The scope also includes [Organization Name] personnel, partners, suppliers and any other stakeholder who has access to or manages information belonging to [Organization Name].

2. Data Protection Policy

2.1 Data Lifecycle Management

[Organization Name] follows a structured Data Lifecycle Management (DLM) process to ensure the secure handling of data from their creation to their destruction. Access to data is strictly controlled based on classification levels and business requirements, ensuring compliance with Decision K.D.P. 389/2020. Data are retained only for as long as necessary and are securely deleted or anonymised when no longer needed. Regular audits and automated Data Loss Prevention (DLP) measures are implemented to safeguard data throughout their lifecycle.

More specifically, [Organization Name] takes the following actions:

- Defines appropriate measures for the protection of data throughout their lifecycle and according to their classification, in compliance with applicable legal and regulatory requirements.
- Records classified information in a register, which must have a designated person responsible for maintaining and updating the recorded information.

© CYberSynchorny, 2024

- Ensures that information is protected both during storage and during transmission.
- For critical or sensitive data of [Organization Name], encryption must be applied during storage (data at rest).
- [Organization Name] has defined specific retention periods for all categories of data and applies the necessary deletion actions.

2.2 Classification and Labelling of Information

[Organization Name] manages all data (electronic and/or paper-based) under its responsibility with security, reliability and accuracy. Such data must always be available only to authorised users. Based on their criticality, sensitivity and risk, these data must be subject to appropriate security measures.

For the effective management of information, [Organization Name] has defined a process that includes at a minimum the following stages:

1. Identification and recording of information
2. Information classification
3. Information labelling
4. Information handling

Furthermore, to ensure correct handling and protection, all Organizational data are classified (labelled) based on sensitivity and risk level. For labelling purposes, [Organization Name] has defined the following categories:

- **Public Use (Public)**
    - Public-use information refers to data that are not subject to access restrictions and can be freely shared with the public without jeopardising the Organization's security, confidentiality or legal obligations.
- **Internal Use**
    - These are information restricted to the internal circle of the Organization. They usually concern the Organization's operations, management, staff, financial activities and other internal details. Such information is often sensitive and requires protection against unauthorised access.
- **Limited Use**
    - Limited-use information refers to data intended for internal use only and must not be disclosed outside the Organization without appropriate authorisation. This may include business strategies and procedures, internal memos and other non-public information necessary for daily operations but not requiring the highest level of protection. Access to Limited-use information is restricted to employees, associates or third parties with a legitimate need-to-know and must be handled in accordance with established access control policies. Although such information does not require the same level of security as Confidential data, it still requires appropriate protection, such as encryption during transmission and restricted access during storage.
- **Confidential**
    - Confidential information refers to data that are sensitive and should be accessed only by authorised personnel with a legitimate business need. Unauthorised disclosure, access or use of such information could cause significant harm to the Organization and other interconnected entities. Therefore, strict access controls, encryption and data masking techniques must be applied to ensure their protection both at rest and in transit. It is recommended that Confidential

© CYberSynchorny, 2024

information be subject to formal data handling procedures, including Non-Disclosure Agreements (NDAs).

Note: Each Organization may define its own categories according to its needs.

Note: It is understood that for documents and information classified under the Law on Security Rules for Classified Information, Documents and Material and Related Matters of 2021 (84(I)/2021), the provisions of that Law and any Orders issued pursuant to it shall apply and are not necessarily related to the above labelling.

Each category, as described above, determines access rights, storage and security controls, as defined in [IAM1] of Decision K.D.P. 389/2020. Information must be appropriately labelled to reflect its classification, using metadata, other visual markers or automated labelling systems, e.g. TLP system. Employees must comply with labelling instructions to prevent unauthorised access and to support effective data protection and risk management.

More specifically, the following guidelines must be applied:

- Each classified piece of information of [Organization Name] must be clearly labelled for its users.
- A classification and labelling process must be established, adopted and maintained to ensure that information is classified and labelled according to its confidentiality and sensitivity.
- Information must be classified, at a minimum, into three categories: Public, Internal and Classified.
- The responsible information owners are accountable for classifying the information under their responsibility and for managing it in accordance with the process requirements of [Organization Name].
- [Organization Name] must ensure that controls are carried out to verify compliance with classification and labelling requirements.
- [Organization Name] must have a process for the secure deletion of data, which includes roles, responsibilities, methodologies, criteria and tools used for the deletion of data at each classification level, including measures applied when assets are transferred to external parties.
- Where a third party is used for deletion or destruction, [Organization Name] must include appropriate provisions and terms in the relevant contract to ensure proper and effective implementation of the relevant rules. Where data are stored with third parties (e.g. Cloud services), specific commitments and evidence must be provided by the third party regarding the implementation of the required measures. Otherwise, alternative compensation controls must be implemented.

2.3 Transfer and Exchange of Information

[Organization Name] ensures that all internal and external data transfers are carried out securely in order to prevent unauthorised access, interception or data leakage. More specifically:

- [Organization Name] defines appropriate protection measures for data transfer, both internally and with third parties, depending on the data classification level.
- Protection measures must be communicated to third parties with whom data are exchanged, and their compliance with these measures must be ensured.
- All employees of [Organization Name] must follow approved methods for data exchange, ensuring confidentiality and integrity throughout the process.
- During the transfer and exchange of information, regulatory and legal requirements must be taken into account, particularly in cases of international data transfers, as defined in [GOV2] of Decision K.D.P. 389/2020.

© CYberSynchorny, 2024

- [Organization Name] must implement appropriate encryption when exchanging or transferring critical or sensitive data. Examples include implementation of Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
- Encryption keys must be transferred separately, using a different medium (or method), without indication of their use.
- [Organization Name] must apply appropriate mechanisms to ensure the integrity and authenticity of the information exchanged.
- Within [Organization Name], a register must be kept of the information exchanged (critical or sensitive), recording the measures applied and the relevant assurances from the parties involved.
- Data masking mechanisms must be applied for enhanced protection, especially where sensitive data are involved, where this is feasible.

2.4 Data Loss Prevention and Data Leakage Prevention

[Organization Name] implements Data Loss Prevention (DLP) controls to protect sensitive information from unauthorised access, accidental exposure or malicious exfiltration. Security measures include, among others:

- [Organization Name] must define measures to minimise the risk of data loss and data leakage by taking appropriate technical and Organizational measures for prevention, in accordance with [DS5] of Decision K.D.P. 389/2020.
- The transfer of data using USB devices is not recommended.
- Access to media for data transfer and to non-corporate messaging or file-sharing systems is prohibited.

2.5 Use of Cryptography

[Organization Name] uses cryptographic techniques to protect sensitive data during transmission and storage. Specific encryption control points are applied to systems, services and applications of [Organization Name] that store or process internal, limited or confidential information. Such information must be encrypted using cryptographic algorithms (e.g. AES, RSA) to ensure the confidentiality and integrity of data.

More specifically:

- [Organization Name] must ensure that data classified as critical are encrypted during storage and transmission.
- Removable storage media as well as endpoint devices must be encrypted.
- [Organization Name] must establish a process for managing cryptographic measures used, including management of encryption keys (symmetric and asymmetric) throughout their lifecycle (generation, storage, control, distribution), using internationally accepted standards and procedures, including strict access rules to the management platform. This process must define roles and responsibilities related to implementation of the cryptographic policy, key management and the rules to be adopted for effective policy implementation.
- [Organization Name] ensures that only the latest versions of approved cryptographic protocols and software are used, as well as appropriate key lengths.
- When using cryptography, [Organization Name] must at a minimum use the following cryptographic algorithms:
    - For symmetric encryption, the AES algorithm with a key length of at least 128 bits.

© CYberSynchorny, 2024

- For digital signatures, the RSA algorithm with a key length of at least 2048 bits.
- For hashing, the algorithms SHA-256, SHA-512 or SHA-3-41.

- [Organization Name] must use cryptographic software and libraries only after they have been assessed by reputable third parties.
- Encryption keys are protected as data of the highest classification level of [Organization Name].
- Interception or leakage of encryption keys is treated as an information security incident.
- [Organization Name] follows cryptographic best practices for its cloud infrastructure.
- Where encryption cannot be implemented, this must be recorded as a risk and other measures must be designed and implemented to ensure the desired level of security, in line with the Risk Management Policy.

2.6 Deletion or Destruction of Information

The following proposed measures are generally effective for the secure destruction of information, whether in digital or physical form:

- Information is destroyed in a secure manner (e.g. multiple passes of software-based overwriting) to prevent any possibility of recovery.
- This process includes overwriting reusable storage media with repeated data patterns. The purpose is to ensure that previous data cannot be easily recovered with data recovery tools.
- Documents must be destroyed using approved methods (e.g. cross-cut shredding) that ensure they cannot be reconstructed.

2.7 Digital Signatures

It is recommended that [Organization Name] begins integrating digital signatures into various systems and processes with the aim of detecting any unauthorised data modifications and certifying the identity of the signer. Digital signatures serve as a powerful tool for ensuring data integrity, legal compliance and the reliability of information throughout their lifecycle, from creation to deletion.

They mainly help in:

- **Accountability and Traceability:** Digital signatures create an immutable record of who, when and how data were created, modified, accessed or distributed. This enhances accountability and ensures full traceability throughout the data lifecycle.
- **Trust:** The signer builds trust with stakeholders, customers and other regulatory bodies by providing assurances of data integrity and authenticity, which are essential for maintaining a secure data environment and ensuring compliance.

3. Information Backups

According to Decision K.D.P. 389/2020, [Organization Name] establishes, implements and maintains backup and data recovery procedures in order to ensure the timely and effective restoration of data following an incident or upon request. Backup and data recovery procedures must be thoroughly and frequently tested to ensure proper and reliable operation of all supporting processes and systems.

© CYberSynchorny, 2024

The systems and supporting infrastructures that enable backup and data restoration must be geographically dispersed (off-site storage) to protect against physical security threats.

4. Provisions in Contracts with Third Parties

It is important to include explicit provisions on the secure management and destruction of information in contracts with third parties. Such contractual clauses help safeguard sensitive information and ensure that [Organization Name]'s partners follow the necessary procedures and maintain the same standards of security, confidentiality and compliance as the Organization.

It is important to note that requirements for secure destruction of information may differ depending on the legislation and the type of information to be destroyed. Furthermore, continuous monitoring and updating with respect to best practices is vital to ensure the effective protection of information.

Key requirements of such a contract may include provisions for the following:

- Data protection and security requirements
- Data processing and handling
- Confidentiality and non-disclosure
- Incident response notification and possible data breach reporting
- Right to audit and monitoring
- Use of subcontractors and other third-party providers
- Data retention and disposal
- Liability and any professional indemnity
- Termination and return or destruction of data

5. Review

Documents related to Data Protection must be reviewed and updated at least annually or in case of significant changes in the environment of [Organization Name], in order to ensure that they remain up to date, effective and aligned with the Organization's needs, any legal/regulatory requirements and other technological developments, such as new emerging threats (e.g. after lessons learned from incidents that resulted in data loss).

Additionally, the Policy must be reviewed so as to reflect these changes in cases where the Organization expands its services, changes its data processing activities or starts handling new types of personal data (e.g. sensitive data, biometric data).

6. References

Category	ID	Control	Control Objective
Data Security	DS1	Information Lifecycle Management	To ensure the protection of data throughout the entire information lifecycle, including collection, recording, Organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or

© CYberSynchorny, 2024

			combination, restriction, erasure or destruction.
Data Security	DS2	Classification and Labelling of Information	To ensure that data are classified and labelled in a way that reflects their sensitivity so that their processing is appropriately safeguarded.
Data Security	DS4	Transfer and Exchange of Information	To implement adequate measures for the internal or third-party transfer and exchange of information in order to ensure the secure transfer of data.
Data Security	DS5	Data Loss Prevention and Data Leakage Prevention	To ensure the protection of data from intentional or unintentional loss and data leakage.
Network Security	NS4	Secure Communication Protocols	To ensure appropriate communication protocols are in place to achieve secure communication between network assets.
Human Resources Security	HRS4	External Partners	To ensure that external partners working on behalf of the Organization comply with the information security policy and the Organization's security objectives.

© CYberSynchorny, 2024

4.11 Tool 11 - Acceptable Use Policy

[Organization Name]

ACCEPTABLE USE POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
   1.1 Purpose
   1.2 Scope of Application
2. Acceptable Use Policy
   2.1 General Requirements – Obligations
   2.2 Email
   2.3 Use of the Internet
3. Passwords
4. Information Storage
5. Mobile Devices
6. Remote Work
7. Removable Storage Media
8. Review
9. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

This Policy defines the Acceptable Use Policy of [Organization Name] in relation to the access to and proper use of its information systems, technological resources and data. Its objectives are:

- The protection of confidentiality, integrity and availability of information assets.
- The prevention of misuse, unauthorised access or actions that may jeopardise information security.
- Ensuring compliance with other policies and applicable regulations/legislation.
- Promoting the safe and responsible use of technological and other resources in support of the Organization's mission and objectives.

1.2 Scope of Application

[Organization Name] aims to conduct its activities in a professional manner, applying high standards in the provision of its services. Therefore, all personnel must take the necessary measures to safeguard the integrity of information and information systems and their data, and follow the procedures and instructions described below to maintain security and legality.

The Acceptable Use Policy applies to all employees/users of [Organization Name], including third parties who may have access to [Organization Name] resources, in order to maintain a safe, efficient and ethical working environment. This Policy applies to all information and information systems of the Organization, including equipment used for remote work and material originating from various IT systems.

This Policy sets out clear expectations for all users in relation to:

- Computers, laptops and mobile devices owned by [Organization Name].
- Email accounts issued by [Organization Name] and access to corporate email.
- The internal network of [Organization Name].
- Access to the Internet.
- Software and applications provided by [Organization Name].

2. Acceptable Use Policy

2.1 General Requirements – Obligations

[Organization Name] has established and implements basic information security rules, which are to be included in employees' contracts. More specifically:

- The Acceptable Use Policy is communicated to all personnel and is accepted via their contracts, and subsequently personnel receive relevant training on the acceptable use of [Organization Name] resources and/or information, so that they apply measures proportionate to the criticality of the information they handle.
- Computers and/or other resources assigned to personnel must be used exclusively for approved business purposes, and any personal use is prohibited.
- [Organization Name] resources must only be used by authorised individuals and may not be made available to colleagues and/or any third parties.
- Only licensed software may be used on [Organization Name] resources.

© CYberSynchorny, 2024

- Any suspected security incident must be reported by any employee who becomes aware of it, in accordance with the Incident and Event Management Policy.
- It is recommended that compliance with the Acceptable Use Policy be monitored via questionnaires completed by personnel on an annual basis. Technical measures should be implemented so that personnel are informed of acceptable use instructions each time they are about to access [Organization Name] systems.

2.2 Email

Careless use of email or the Internet may expose [Organization Name]'s information networks to a wide range of risks related to various types of malware such as spyware, Trojans, worms, spam and other cyber threats, which can negatively impact the confidentiality, integrity and availability of [Organization Name] data.

When using email or the Internet, [Organization Name] personnel are responsible for consistently exercising due care with regard to network security.

The guidelines/instructions contained in this Policy apply both to any personal email messages and to the Organization's email messages. Email has been established as a communication method for [Organization Name] activities. Personal use of corporate email is prohibited in order to avoid and reduce the opening of unsolicited messages.

Emails can create binding obligations for [Organization Name] and expose it to the same extent as traditional correspondence. Inappropriate statements in email messages may lead to personal liability for the sender, as such statements may be used in court proceedings. Particular care must therefore be taken when drafting emails, and the same standards and protocols as in written correspondence must be applied.

In addition, messages that could jeopardise the integrity or reputation of [Organization Name] should be avoided.

You must not use [Organization Name] email to store, send/forward or otherwise transfer content of any of the following categories:

- Content that violates the employee's obligations to safeguard the Organization's classified information, or that violates [Organization Name]'s obligations to safeguard the classified information of its partners, or violates intellectual property rights (trademark, trade secret, copyright).
- Offensive or obscene content (including any type of pornography).
- Racist or sexist content.
- Content that is false or malicious, whether it concerns a member of staff or any person outside [Organization Name].
- Any content related to bullying or harassment (e.g. on the basis of gender, including sexual orientation, race or disability).
- Any other content that could otherwise be considered illegal.

Such actions constitute inappropriate behaviour and may trigger the Organization's disciplinary procedures.

2.3 Use of the Internet

The procedures and requirements for the use of the Organization's email apply equally to the use of the Internet, with the following additional guidelines:

- Employees must use the Internet exclusively for business purposes and avoid accessing inappropriate or unauthorised content.

© CYberSynchorny, 2024

- Access to social networking sites and personal entertainment sites must be limited during working hours, unless there is a clear business reason.
- Employees must avoid downloading files from untrusted sources and must not install software without the approval of [Organization Name]'s IT department.
- It must be verified that the download of information or material from websites does not violate intellectual property rights and does not incur unauthorised expenses for [Organization Name].
- Employees must avoid visiting websites or sending information via such sites that fall into the following categories (the list is not exhaustive):
    - Defamatory
    - Offensive, obscene (including any type of pornography)
    - Racist or sexist
    - Could cause bullying or harassment (related to gender, including sexual orientation, race or disability)
    - Containing illegal software or other pirated audiovisual material
    - Anything that could be considered illegal
    -

3. Passwords

Passwords are a critical component of the Organization's security. Sharing passwords with other employees or third parties is not permitted. Passwords must be stored securely and must not be recorded in readable form.

Employees must change their passwords periodically, in line with best practices, and must avoid using common or easily guessable passwords.

Employees must not keep password records unless these can be stored securely using approved storage and encryption methods.

For more information, please refer to the Access Control Policy.

4. Information Storage

The storage of business information on non-approved external storage devices or personal cloud accounts is prohibited.

Employees must regularly back up important data and ensure that such backups are stored on secure media.

All sensitive and confidential information must be stored in secure locations and must be encrypted.

5. Mobile Devices

When using mobile devices (e.g. laptops, mobile phones, etc.), particular care must be taken to ensure that the Organization's information is not put at risk. Special attention must be given when such equipment is used in public spaces, meeting rooms and other non-secured areas outside [Organization Name] premises.

Where possible, such devices should be protected through encryption to prevent unauthorised access to or disclosure of the information stored on them (see Asset Management Policy).

© CYberSynchorny, 2024

Remote access to the Organization's information via public networks and mobile information systems must only take place after appropriate authorisation has been granted and after successful user identification and authentication and using appropriate access control mechanisms exclusively via VPN.

If the transport of laptops is not necessary, [Organization Name] laptops must be locked in the office upon departure, unless sufficient physical security measures are in place in the building. If transport is mandatory and necessary for the performance of an employee's duties, then best practices for securing mobile devices must be followed, as outlined in the Information Systems Security section of this Policy.

6. Remote Work

In the case of remote work, appropriate measures must be taken to protect the environment before work begins, e.g. against theft of equipment and information, unauthorised disclosure of information, or unauthorised remote access to [Organization Name] internal systems.

Remote work must be authorised and approved by [Organization Name] Management. In addition, it must be ensured that the necessary infrastructure exists to support this mode of work.

Any passwords used for remote access to the Organization's systems must be memorised and not recorded. If a laptop is stolen, [Organization Name]'s IT Department must be notified as soon as possible.

7. Removable Storage Media

Limiting the use of removable storage media (USB disks) is an effective security measure in corporate environments and must be enforced. In very rare cases where such use is necessary, the following measures must be taken:

- Only authorised removable storage media may be used on [Organization Name] information systems and premises.
- Only authorised personnel may use authorised removable storage media.
- A process for authorising removable media must be recorded and followed. All authorisations must be time-limited, reviewed at regular intervals (at least annually) and recorded in a relevant register.
- All removable storage media issued to authorised users must be recorded in a relevant register.
- The use of personal removable storage media on [Organization Name] information systems is prohibited.
- The use of authorised removable storage media for personal purposes is prohibited.
- The storage of Confidential and/or Internal Use information on removable storage media is not permitted.
- USB-type removable storage media must use strong encryption mechanisms (at least hardware-based 256-bit AES encryption), including during storage, transit and movement.
- Unnecessary stored information on removable storage media must be deleted in accordance with the Asset Management Policy.
- Removable storage media must never be left unattended.
- The user of the removable storage media is responsible for the device as well as for the integrity and availability of the information stored on it.

© CYberSynchorny, 2024

- In case of theft or loss of removable storage media, the user's immediate supervisor and the Information Security Officer of [Organization Name] must be informed, and depending on the content, the Incident and Event Management Procedure may be activated (see Incident and Event Management Policy).

Non-compliance with the Acceptable Use Policy and the instructions described in this document, or misuse of the Organization's systems, constitutes a serious disciplinary offence which may result in dismissal with or without notice, depending on the gravity of the incident.

8. Review

Documents related to the acceptable use of resources must be reviewed and updated at least annually or in case of significant changes in the environment of [Organization Name], in order to ensure that they remain up-to-date, effective and aligned with the Organization's needs, any legal/regulatory requirements and other technological developments such as new emerging threats, etc.

9. References

Category	ID	Measure	Objective of Measure
Human Resources Security	HRS6	Employment Agreements and Acceptable Use	To ensure that responsibilities relating to information security and acceptable use of assets are incorporated into employment agreements and onboarding procedures, in order to achieve accountability and awareness.
Asset Management	AM3	Asset Monitoring	To ensure that assets are monitored for attacks, anomalies and security threats, so that procedures for incident and event handling can be activated.

© CYberSynchorny, 2024

4.12 Tool 12 - Human Resources Security, Training & Awareness Policy

[Organization Name]

HUMAN RESOURCES SECURITY, TRAINING & AWARENESS POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
   1.1 Purpose
   1.2 Scope of Application
2. Employment Life Cycle
   2.1 Before Employment
   2.2 Employment Parameters
3. During Employment
   3.1 Management Responsibilities
   3.2 Information Security Roles and Responsibilities
   3.3 Training, Education and Awareness
   3.3.1 Annual Training Programme
   3.3.2 Programme Effectiveness
   3.4 Disciplinary Procedure
4. Termination of Employment or Change of Role
   4.1 Responsibilities upon Termination
   4.2 Return of Assets
   4.3 Removal of Access Rights
5. Review
6. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

The purpose of the Human Resources and Training Policy is to ensure the protection of the data and information systems of [Organization Name], through the training and awareness of employees, the recording of policies and procedures for the entire employment life cycle, and the proper preparation for recognising and addressing relevant cyber security threats.

1.2 Scope of Application

This Human Resources and Training Policy applies to all staff and associates of [Organization Name], as well as to third parties acting on its behalf, including staff employed on fixed-term contracts, external partners and trainees.

This Policy has been designed to ensure the security, management and well-being of all the above categories of personnel, while at the same time ensuring compliance with applicable legal and regulatory provisions. In addition, its purpose is to reduce the risk of fraud and to protect the physical and logical assets of [Organization Name].

This Policy describes the actions that must be taken before, during, and upon termination or change of employment, contract or agreement of personnel, suppliers or third parties acting on behalf of [Organization Name].

2. Employment Life Cycle

2.1 Before Employment

In order to prevent misuse of [Organization Name] information and information systems, the Organization ensures that the necessary control procedures are in place so that personnel are suitable for the work assigned to them before they are hired by [Organization Name].

To the extent permitted by law, a procedure must be established in cooperation with the Human Resources (HR) Department of [Organization Name] for all future recruitments.

This procedure must take into account education, experience, qualifications, references, etc. Among other things, the following must be recorded:

- Job descriptions must be defined so as to cover the appropriate and expected outcome of each job role. Job descriptions must include, among other things, information security responsibilities for all required job roles.
- Before recruitment, appropriate background verification must be carried out, including checking the application against academic and professional qualifications, for both internal and external staff, and checking a clean criminal record. Records must be stored in the employee's personnel file.

2.2 Employment Parameters

All new hires must agree to and sign the relevant employment parameters/contracts with [Organization Name]. Employment contracts must clearly define employees' obligations and responsibilities for information security. The rules and policies apply both to [Organization Name] staff and to services provided via third parties, where they affect the security of [Organization Name].

Contracts must include, inter alia, the following:

© CYberSynchorny, 2024

- Responsibility for managing information security throughout the employment life cycle, as well as employees' understanding of their responsibilities in relation to this information.
- The confidentiality agreement (before the start of work and prior to access to the Organization's information and information systems).
- The responsibility of the Organization's employees to comply with the laws and regulations related to the work of [Organization Name] as well as its circulars/internal instructions.

3. During Employment

All employees and external partners of [Organization Name] are expected to know and ensure their responsibilities in relation to information security.

1. All users are trained to perform tasks related to the information security requirements of their specific job roles.
2. The frequency of such training is determined in cooperation with the Information Security Officer and the Human Resources Department of [Organization Name].
3. The induction process includes information security awareness topics and, where required, role-specific training.
4. All employees must be informed about [Organization Name] information security policies and about the disciplinary procedure in case of non-compliance with these policies.
5. Any employee who interferes with or refuses to cooperate in the investigation of non-compliance with these policies will be subject to disciplinary measures, up to and including termination of employment.
6. Records of training and/or awareness activities and details of the training and/or awareness must be documented and retained.
7. The Human Resources Department must immediately inform the IT Department of internal transfers of employees.
8. The IT Department must ensure the immediate modification of employees' logical access rights following notification by the Human Resources Department.
9. The Information Security Officer must periodically review the appropriateness of logical and physical access rights in line with job responsibilities.
10. A documented disciplinary procedure must exist, setting out the actions to be taken in the event of an information security breach.
11. Department heads ensure adequate participation of their team members in information security awareness training.

3.1 Management Responsibilities

Management, in cooperation with the Head of Human Resources and the Information Security Officer, is responsible for:

- Defining and documenting employees' roles and responsibilities and informing them of their corresponding obligations and responsibilities.
- Preparing training plans to ensure that employees have an information security knowledge level appropriate to their role and comply with employment parameters, which include information security, in accordance with the provisions of paragraph 3.3 below.

© CYberSynchorny, 2024

- Conducting regular and ad-hoc checks to ensure that employees understand their role and responsibilities and comply with their obligations and responsibilities. These checks include tests to assess the effectiveness of training and compliance with [Organization Name] security policies, procedures and measures.
- Analysing the results of the checks in order to assess staff compliance. Where issues are identified, the relevant procedures must be activated to deal either with security incidents or with the application of disciplinary or other measures.

3.2 Information Security Roles and Responsibilities

Specific employees of [Organization Name] must document their role and responsibilities in relation to information security in their job description.

An employee must include a reference to information security in their job description if one or more of the following applies:

- Owner of information security policies and procedures
- Coordination and oversight of information security matters
- Information owner

3.3 Training, Education and Awareness

All employees of [Organization Name] and, where appropriate, external partners must receive appropriate training and regular updates in relation to information security policies and procedures, commensurate with their job position. The objective of the programme is to ensure understanding of the basic principles of information security and cyber security, to raise awareness of current cyber threats and to train staff in how to respond to cyber-attacks and security incidents.

More specifically:

- [Organization Name] must implement a holistic training and awareness programme for employees on information protection and information security issues and carry out actions aimed at familiarising employees and reducing the likelihood of incidents, in accordance with [TA1] of Decision K.D.P. 389/2020.
- The objectives for training employees on information security must be defined and maintained.
- [Organization Name]'s training programme on Information Security and cyber security must be designed taking into account employees' roles and duties and must include at least one annual training and briefing of employees on [Organization Name] Security Policies.
- [Organization Name]'s training programme on Information Security/cyber security must be designed to ensure it provides sufficient information on staff roles and responsibilities in relation to Information Security.
- [Organization Name]'s training programme on Information Security and cyber security must be created in line with the Organization's policies and related procedures, taking into account the information that must be protected and the measures implemented to protect such information from potential data loss and/or unauthorised access, in accordance with [TA2] of Decision K.D.P. 389/2020.
- Senior Management of [Organization Name] is responsible for approving the annual training and awareness programme on information security in order to promote commitment and a security culture regarding [Organization Name] information.

© CYberSynchorny, 2024

- The effectiveness of the training programme, as well as the level of staff knowledge and awareness on Information Security issues, is assessed periodically (at least annually).
- The training and awareness process for employees/partners must include periodic activities throughout the duration of the employment/engagement relationship, from recruitment/assignment to termination.
- Awareness activities, such as campaigns (e.g. an "Information Security Day") and the publication of leaflets or newsletters (e.g. emails), must be included in the training programme.
- The Human Resources Department of [Organization Name] must retain evidence regarding completion of training and its results.
- It is recommended to establish communication channels with internal or external groups related to information security so that staff remain informed of the latest recommended practices, techniques and security technologies.
- To implement the training programme, [Organization Name] may follow the following awareness practices:
    - Provision of training material via customised platforms.
    - Delivery of training through presentations, seminars and simulated exercises.
    - Periodic checks of understanding of the programme content.
    - Continuous information on new threats through updates of the annual cyber-threat landscape and technical threat mitigation actions.

3.3.1 Annual Training Programme

The training and awareness needs of the relevant individuals regarding information security are identified:

- During preparation of the annual training and awareness programme on information security
- During preparation of [Organization Name]'s annual budget
- During completion of annual training evaluations and annual performance appraisals
- As a result of actions arising from various [Organization Name] activities, e.g. Exercises, Security Incident Management, Risk Assessment
- As a result of changes in [Organization Name]'s business needs.

3.3.2 Programme Effectiveness

The effectiveness of the programme can be assessed through:

- Staff participation and understanding via functions provided by dedicated training and assessment platforms.
- Analysis of cyber-attack incident statistics and the ways/times such incidents are handled.
- Collection of feedback from participants.

The continuous improvement of the programme ensures better protection of [Organization Name] against newer and more advanced cyber threats and the participation of all employees in the common goal of resilience against cyber-attacks.

© CYberSynchorny, 2024

3.4 Disciplinary Procedure

There is a documented formal disciplinary procedure, in accordance with applicable laws and regulations, for taking action in the event of breaches related to information security. This procedure must be communicated to employees, in order to improve compliance with their obligations and responsibilities.

This procedure is followed in cases of serious, documented information security breaches that have a high impact on [Organization Name] based on the risk assessment. The procedure sets out levels so that factors such as the nature and severity of the breach and its impact on [Organization Name], whether it is a first or repeated offence, whether the offender received appropriate training, as well as applicable legislation, contractual obligations and other relevant factors, are taken into account.

This procedure acts as a deterrent against potential information security breaches.

4. Termination of Employment or Change of Role

The Human Resources Department of [Organization Name] is responsible for ensuring that a documented procedure exists for termination of employment or change of role, safeguarding the interests of [Organization Name]:

1. The Human Resources Department immediately notifies the relevant departments (e.g. IT Department, etc.) of cases of termination of employment so that actions for the revocation of the employee's access rights and privileges can be planned promptly.
2. The Human Resources Department must include in the notification the employee's last working day at [Organization Name].
3. All logical and physical access will be revoked on the date of settlement of outstanding obligations or the date of departure from [Organization Name] (whichever comes first).
4. The Human Resources Department, in collaboration with other departments, will enforce a user termination procedure, including revocation of user access rights and the return of assets.
5. All physical and logical access rights to [Organization Name] information processing facilities/information will be revoked at the end of service for each user.
6. The Human Resources Department ensures that all employees who resign complete a termination of employment form before leaving [Organization Name] and that such records are retained.
7. The Human Resources Department defines the channels through which the various departments (e.g. IT Department, etc.) will be notified to revoke logical and physical access rights in cases of termination of employment.
8. Any equipment assigned to the user must be returned securely for any further review or action.
9. The communication and coordinated actions involved in the termination process are controlled and limited to specific individuals from the appropriate departments.
10. In the case of dismissal, the employee must not be allowed access to any information or information processing facilities. The dismissed employee is escorted out of the Organization's premises, and any outstanding tasks of the termination process are completed.

The above procedure includes the following:

© CYberSynchorny, 2024

4.1 Responsibilities upon Termination

Responsibilities upon termination or change of employment must be defined and the responsible persons must be designated.

The Human Resources Department, in cooperation with the relevant Supervisor and the IT Department of [Organization Name], is responsible for implementing the termination of employment or change of role procedure. In the case of termination of employment, the Supervisor reminds the employee of the need to comply with specific obligations even after departure, such as confidentiality agreement, intellectual property, protection of personal data, etc.

4.2 Return of Assets

All employees and external partners of [Organization Name] must return all Organization assets in their possession prior to termination of their employment/engagement.

The Human Resources Department, in cooperation with the relevant Supervisor and the IT Department, ensures that any asset that was in the possession of the departing employee is returned securely to the Organization.

4.3 Removal of Access Rights

Access rights to [Organization Name] premises as well as to information and information processing systems, for employees and external partners, must be removed immediately after the end of employment, contract or agreement, or adjusted in case of change of role.

Upon receipt of an employee's resignation letter, the relevant Supervisor assesses whether the employee's existing access rights need to be reviewed and reduced while the employee is still working, and informs the IT Department accordingly.

Upon termination of employment by [Organization Name], the employee's access rights are immediately disabled and accounts are deleted when access is no longer required.

The access rights of [Organization Name] employees must be reviewed by the relevant Supervisor when their roles change, and any access that is no longer required must be revoked.

In all cases, the Human Resources Department must promptly inform the relevant persons so that they can carry out their respective actions, for example:

- The IT Department, for access to electronic systems
- The Human Resources Department, for access to buildings
- Reception, so that from the termination date the individual is treated as a visitor, etc.

If the Supervisor considers that the departing employee has knowledge that is necessary for the Organization's business continuity, they are responsible for ensuring that such knowledge is transferred to another employee of the Department/Service.

5. Review

The owner of this Policy is the Head of the Human Resources Department, who is responsible for its implementation, maintenance and review. All policies and procedures related to Human Resources Management must be reviewed and updated at least annually or in the event of significant changes in the environment of [Organization Name] (e.g. Organizational structure, business activities and market trends, legal and regulatory requirements and compliance requirements, implementation of new systems, new risks, emerging threats, etc.).

© CYberSynchorny, 2024

6. References

Category	ID	Control	Control Objective
Human Resources Security	HRS1	Employment life cycle	To implement adequate measures to ensure that personnel working on behalf of the Organization, who have access to Organizational resources, support the information security policy and the Organization's objectives.
Human Resources Security	HRS2	Employee monitoring	To ensure that personnel working on behalf of the Organization comply with the information security policy and fulfil their security responsibilities throughout the employment life cycle.
Human Resources Security	HRS3	Disciplinary measures and enforcement	To ensure that personnel working on behalf of the Organization are responsible for intentional or unintentional activities that affect the Organization's information security objectives.
Human Resources Security	HRS4	External partners	To ensure that external partners working on behalf of the Organization follow the information security policy and the Organization's security objectives.
Human Resources Security	HRS5	Protection from insider threats	To ensure protection against network and information security threats originating from within the Organization.

© CYberSynchorny, 2024

Human Resources Security	HRS6	Employment agreements and acceptable use	To ensure that responsibilities regarding information security and acceptable use of assets are incorporated into employment agreements and onboarding procedures, in order to achieve accountability and awareness.
Awareness and Training	TA1	Information security awareness	To establish an information security awareness programme for all personnel within the Organization, taking into account the elements described in information security policies, standards, guidelines and procedures.
Awareness and Training	TA2	Information security awareness and training	To provide training to all Organization personnel, as defined in the information security programme.
Data Security	DS5	Prevention of data loss and data leakage	To ensure the protection of data against intentional or unintentional loss and data leakage.

© CYberSynchorny, 2024

4.13 Tool 13 - Physical Security Policy

[Organization Name]

PHYSICAL SECURITY POLICY

© CYberSynchorny, 2024

Table of Contents

1. Purpose
2. Scope of Application
3. Document Recipients
4. Roles and Responsibilities
   4.1 Responsibilities of [Organization Name] security Management (Cyberspace Directorate)
   4.2 Responsibilities of the Information and Data Security Officer
   4.3 Responsibilities of the Operations Administrator
   4.4 Responsibilities of the Incident Response & Threat Intelligence Team
   4.5 Responsibilities of the Guidance Team
   4.6 Responsibilities of the [Organization Name] security Manager
   4.7 Responsibilities of [Organization Name] security Computer Users
5. Physical Security Policy
   5.1 Identification of Physical Security Needs
   5.2 Design and Implementation of Physical Security Measures
   5.2.1 Risk Management Plans and Incident Management Plans
   5.3 Physical Security Measures – Access to [Organization Name] Facilities
   5.4 Physical Protection of Critical Information Assets
   5.5 Physical Security of the [Organization Name]
   5.6 Physical Security of the Data Center
   5.7 Security Measures for Internal and Classified Areas
   5.8 Measures for the Prevention and Response to Fire, Flood and Other Natural Disasters
   5.9 Uninterruptible Power Supply
   5.10 Training and Awareness
   5.11 Verification and Review of the Policy
6. Obligation of Implementation
7. Disciplinary Sanctions for Non-Implementation

© CYberSynchorny, 2024

1. Purpose

This Physical Security Policy describes the establishment and implementation of principles and appropriate physical security measures for the protection of the physical assets, equipment and building infrastructures of the [Organization Name]. The physical security policy at the [Organization Name] is important for ensuring the security of physical assets and systems, as it defines both the requirements and the appropriate measures for the physical security of facilities and access control to buildings and other areas.

The purpose of this policy is to ensure the effective protection of the Service's physical environment from physical risks and threats.

2. Scope of Application

This Policy applies to all employees, contracted personnel and third parties who have access to the [Organization Name] security facilities.

This Policy recognises the need to establish a framework which includes basic principles and rules for the protection of [Organization Name] infrastructures and equipment from physical and external threats, as well as the safeguards for the Physical Access of employees and third parties who have access to the Cyberspace Directorate's facilities.

3. Document Recipients

- [Organization Name] security Analyst L1 (Security Analyst Level 1)
- [Organization Name] security Analyst L2 and L3 (Security Analyst Level 2 & Level 3)
- [Organization Name] security Manager
- Systems Architect
- Operations Administrator
- [Organization Name] security Management (Cyberspace Directorate)
- Engineer
- Incident Response & Threat Intelligence Team
- Guidance Team
- IT Systems Technician
- Helpdesk Technicians (Helpdesk Team)
- Responsible Administrator of Infrastructure Systems
- Information and Data Security Officer
- [Organization Name] security Computer Users
- DPO (Data Protection Officer)

4. Roles and Responsibilities

Clearly defined roles and responsibilities are critical for the development and achievement of a successful framework relating to Physical Security. The Information and Data Security Officer, together with the [Organization Name] security Management and the [Organization Name] security Manager, are responsible for the implementation of the Physical Security Policy, ensuring its correct application and execution.

© CYberSynchorny, 2024

4.1 Responsibilities of [Organization Name] security Management (Cyberspace Directorate)

The core responsibilities of [Organization Name] security Management include the approval and review of the Physical Security Policy, as well as the related Risk Management Plans and Security Incident Management Plans.

In addition, Management is responsible for creating the necessary conditions to protect the Service's physical facilities. Finally, it is responsible for making decisions on the imposition of sanctions in cases of disciplinary offences relating to Physical Security.

4.2 Responsibilities of the Information and Data Security Officer

The core responsibilities of the Information and Data Security Officer include maintaining and updating information security policies and procedures in relation to the current status of the [Organization Name], as well as training staff on the application of these policies.

In addition, the Officer informs [Organization Name] security Management of any occurrence of potential security incidents. In the event of an incident, the Officer, together with the Incident Response & Threat Intelligence Team, activates the corresponding plan with the aim of addressing the incident and preventing its recurrence.

4.3 Responsibilities of the Operations Administrator

The core responsibilities of the Operations Administrator include controlling and updating the physical and logical accesses of [Organization Name] security users.

Additionally, the Administrator informs [Organization Name] security Management and the Information and Data Security Officer of any modification of user access rights or of the revocation of any user's access. The Administrator is responsible for maintaining this Policy in cooperation with the Information and Data Security Officer.

4.4 Responsibilities of the Incident Response & Threat Intelligence Team

The core responsibilities of the Incident Response & Threat Intelligence Team include identifying emergency situations and coordinating actions for the implementation of incident response plans, as well as documenting control measures for addressing risks.

4.5 Responsibilities of the Guidance Team

The Guidance Team is responsible for managing and monitoring the security of [Organization Name] information systems, and protection of information assets also depends directly on physical access to infrastructures.

The Guidance Team monitors compliance of the [Organization Name] security measures adopted with the physical security requirements set by the Cyberspace Directorate.

4.6 Responsibilities of the [Organization Name] security Manager

The core responsibilities of the [Organization Name] security Manager include participation in the identification, assessment and planning of risk management regarding the protection of [Organization Name] information and

© CYberSynchorny, 2024

data, as well as active participation in the investigation of security incidents, so that their causes are examined and the necessary corrective actions are designed.

4.7 Responsibilities of [Organization Name] security Computer Users

The core responsibilities of users include the proper application of the Physical Security Policy, as well as reporting any security incident that comes to their attention.

5. Physical Security Policy

5.1 Identification of Physical Security Needs

The Cyberspace Directorate maintains all necessary physical access controls to protect information and data. Users must:

- Keep their physical environments, such as workplaces and devices, secure.
- Immediately report any tampering with or theft of devices.

Network equipment components of the Service, including individual computers, must be secured with locking mechanisms wherever feasible.

Areas that contain data and information in any form or provide access to any element of the Service's Network, are protected by appropriate physical entry controls to ensure that access is granted only to authorised personnel.

Visitors have access to secure areas only under the constant supervision of authorised personnel.

The [Organization Name] physical facilities meet the necessary physical security requirements so that both employees and visitors are adequately protected from Physical and Environmental Threats.

The Cyberspace Directorate:

- Assesses the physical threats and risks that may be encountered, and based on this assessment, defines the needs for physical security measures.
- Provides necessary instructions for dealing with emergency situations that may occur in the [Organization Name] building.
- Conducts regular disaster response exercises in order to identify gaps and improve the physical security of its facilities.

5.2 Design and Implementation of Physical Security Measures

Based on the identified needs, appropriate physical security measures are developed and implemented. These may include the installation of security systems, protection from natural disasters and the implementation of emergency plans.

As part of the design, it is determined who has access to the [Organization Name], with a specific definition of roles and access permissions.

5.2.1 Risk Management Plans and Incident Management Plans

The Cyberspace Directorate has drawn up Risk Management Plans and Incident Management Plans to ensure the integrity of data and its operational continuity.

More specifically, for the drafting of Risk Management Plans:

© CYberSynchorny, 2024

- A risk analysis is performed to identify the risks that may affect the [Organization Name], using techniques such as SWOT analysis and other risk assessment methods.
- Strategies are developed to address the identified risks, such as preventive measures, risk transfer (e.g. insurance) and emergency plans.

Similarly, for the Incident Management Plans:

- Potential incidents that may affect the smooth operation of the S[Organization Name] due to natural disasters and cyber-attacks are identified.
- Plans are drawn up for the immediate response to incidents, including evacuation, communication and recovery procedures.

For their proper implementation, adequate staff training and regular monitoring of risk parameters and the results of applied measures are prerequisites. Staff must be trained in the procedures and protocols of the incident response plans and participate in regular simulation exercises to assess their readiness.

After the completion of exercises, the results of exercises and real incidents are recorded and analysed to identify weaknesses.

The Risk Management and Incident Management Plans are reviewed annually or after significant incidents in order to incorporate new knowledge and improvements. They are additionally adjusted based on new needs and technological developments.

5.3 Physical Security Measures – Access to [Organization Name] Facilities

To maintain the security of its facilities, the Cyberspace Directorate has adopted a number of controls and protective measures. Specifically:

- Access to the [Organization Name] facilities is via the main entrance. At the main entrance, access is controlled by authorised Service personnel and staff are prohibited from entering the building outside business hours.
- Employees are allowed access to the facilities only during their shift hours.
- The building is equipped with an alarm system and a smoke detection system, which are monitored remotely.
- The building is surrounded by security cameras (CCTV).
- All Service personnel have access to the building after identity verification and recording of their details at the entrance.
- Personal electronic equipment is handed over upon entry, while access by third parties is by appointment, after stating their full name at the facilities' entrance and undergoing the physical checks mentioned above.

5.4 Physical Protection of Critical Information Assets

With regard to the physical security of the [Organization Name], the Cyberspace Directorate ensures and has taken the necessary measures to protect the facilities from natural disasters, as well as to protect equipment and prevent potential system downtime or information loss. Specifically:

- Assets and electronic equipment of the [Organization Name] (computers, laptops, servers, components) are placed above floor level in order to protect them in case of flooding.

© CYberSynchorny, 2024

- A programme has been defined for recording, monitoring and assessing activities to detect potential malfunctions, by performing test security operations to identify vulnerabilities.

The combination of these practices helps ensure physical security at the [Organization Name], protecting equipment, data and staff from threats.

The facilities where critical information is stored or processed are constructed in such a way that information is adequately protected from physical and environmental threats. The construction and design of the facilities protect the critical information assets from unauthorised access, alteration and destruction.

5.5 Physical Security of the [Organization Name]

Physical security in [Organization Name] refers to the measures taken to protect the [Organization Name]'s physical environment and equipment. These measures help ensure the security of the systems and data managed by the [Organization Name].

More specifically:

- Access to the [Organization Name] security is controlled via restricted entry points and the use of access control systems.
- The [Organization Name] security building has a comprehensive video surveillance system using security cameras to detect breaches and malfunctions.
- All [Organization Name] security areas have appropriate systems in place to maintain suitable temperature and humidity in order to protect sensitive equipment.
- Backup power systems are in place to ensure the continuous operation of the [Organization Name] security in the event of power outages.
- The [Organization Name] security is equipped with fire detection systems for protection against fire, including fire extinguishers, fire-fighting equipment, fire detectors and fire-suppression systems.

Physical security is an important part of the overall security of the [Organization Name], as it ensures that critical infrastructures remain inaccessible to unauthorised actors.

5.6 Physical Security of the Data Center

The Data Center area is permanently locked. Servers are kept locked in racks throughout the day and are raised above floor level to protect them from potential flooding or moisture.

In addition, there is appropriate air-conditioning at a stable temperature using specialised units, while fire protection and fire safety are provided through special carbon dioxide (CO_2) fire extinguishers.

5.7 Security Measures for Internal and Classified Areas

To ensure the level of security in critical internal areas of the [Organization Name] security building facilities, a series of measures are applied, which serve the proper monitoring of these areas as well as the prevention of unauthorised access.

The selection and implementation of physical access control mechanisms are based on the criticality of the Information and Information Assets hosted within them.

The following protective measures for internal areas are applied for the security of critical and classified areas (e.g. Data Center):

© CYberSynchorny, 2024

- Locking of internal entrances.
- Reinforced/raised floors, bullet-resistant window glazing and ceilings protected from moisture, as well as appropriate ventilation/air-conditioning systems installed, monitored for proper operation and maintained.
- Packaging materials from new equipment are removed immediately from the Data Center.
- Equipment used temporarily within the Data Center (laptops, monitors, keyboards, mice, power cables, network cables, etc.) is removed after the completion of the relevant work.

5.8 Measures for the Prevention and Response to Fire, Flood and Other Natural Disasters

To prevent the occurrence and spread of potential fire, a number of measures are taken, including:

- Use of non-flammable construction materials.
- Thorough cleaning of premises.
- Installation of electrical grounding.
- Installation of fire-resistant doors.
- Critical information in printed or electronic form is stored in fire-resistant cabinets/safes.
- Instructions for the prevention and response to fires and other emergencies are posted throughout the premises.

In addition to preventive security measures, in the event of a fire at the [Organization Name] security facilities, all necessary steps are taken to limit and quickly extinguish the fire.

The facilities also have a mechanism for unlocking exits in case of malfunction.

Information assets and information systems are installed in appropriate locations to ensure there is no risk of leakage from the water supply and sewage network or risk of water ingress from external windows.

All building facilities meet generally accepted specifications and seismic standards.

5.9 Uninterruptible Power Supply

Information systems are protected from power outages or other problems in electricity supply through backup generators owned by the Cyberspace Directorate.

Critical Information Assets and Information Systems are protected from voltage interruptions or any other problem in power supply. Additionally, uninterruptible power supplies (UPS) are used to ensure their continuous operation.

5.10 Training and Awareness

Employees are trained on the risks and safe practices for maintaining physical security. Awareness-raising activities are also carried out on the importance of physical security, such as training programmes and information events.

Any questions or requests for clarification regarding the content of this Policy must be addressed to the Information and Data Security Officer.

© CYberSynchorny, 2024

5.11 Verification and Review of the Policy

The Physical Security Policy is periodically reviewed and verified to ensure it remains applicable and effective. During this review, new physical security threats and any changes that have occurred since the previous version are analysed.

6. Obligation of Implementation

This Policy is an integral part of the [Organization Name] security policy. All involved parties are obliged to comply with this procedure to ensure effective physical security of the [Organization Name].

7. Disciplinary Sanctions for Non-Implementation

Any violation of this Policy, as well as any breach of physical security of infrastructures and equipment, will be treated strictly and may result in disciplinary measures, including legal action, depending on the severity of the violation.

Data subjects concerned have the right to submit questions about this Policy and to request clarifications from the Information and Data Security Officer.

This Policy enters into force as of [Approval Date] and is reviewed periodically to ensure its compliance with the needs and requirements of the Service.

© CYberSynchorny, 2024

4.14 Tool 14 - Incident and Event Management Policy

[Organization Name]

INCIDENT AND EVENT MANAGEMENT POLICY

© CYberSynchorny, 2024

Table of Contents

1. Purpose
2. Scope
3. Document Recipients
4. Roles and Responsibilities
   4.1. Responsibilities of [Organization Name] Management Executives (Cyber Directorate)
   4.2. Responsibilities of the Information and Data Security Officer
   4.3. Responsibilities of the Incident Response & Threat Intelligence Team
   4.4. Responsibilities of the [Organization Name] Manager
   4.5. Responsibilities of [Organization Name] L2 and L3 Analysts (Security Analyst Level 2 & Level 3)
   4.6. Responsibilities of the Guidance Team
   4.7. Responsibilities of [Organization Name] Computer Users
5. Policy
   5.1. Incident Detection and Incident Management
   5.2. Actions in the Event of an Incident
   5.3. Incident Root Cause Analysis
   5.4. [Organization Name] Management
   5.5. Convening the Incident Response & Threat Intelligence Team
   5.6. Incident Reporting, Investigation, Evaluation and Handling
   5.7. Data Integrity and Recovery Checks
   5.8. Problem Management
   5.9. Restoration of Normal Operation
   5.10. Conducting a Cybersecurity Incident Exercise
   5.11. Indicators for Measuring Incident Performance
   5.12. Training and Evaluation – Procedures of the Incident Response & Threat Intelligence Team
   5.13. Policy Verification and Review
6. Obligation of Implementation
7. Disciplinary Sanctions for Non-Implementation

© CYberSynchorny, 2024

1. Purpose

This Incident and Event Management policy describes the establishment and implementation of principles and appropriate physical security measures for the protection of the physical assets, equipment and building infrastructures of the [Organization Name]. The physical security policy at the [Organization Name] is important for ensuring the security of physical assets and systems, as it defines both the requirements and the appropriate measures for the physical security of facilities and access control to buildings and other areas.

The purpose of this policy is to ensure the effective protection of the Service's physical environment from physical risks and threats.

2. Scope of Application

This Policy applies to all employees, contracted personnel and third parties who have access to the [Organization Name] facilities.

This Policy recognises the need to establish a framework which includes basic principles and rules for the protection of [Organization Name] security infrastructures and equipment from physical and external threats, as well as the safeguards for the Physical Access of employees and third parties who have access to the Cyberspace Directorate's facilities.

3. Document Recipients

- [Organization Name] security Analyst L1 (Security Analyst Level 1)
- [Organization Name] security Analyst L2 and L3 (Security Analyst Level 2 & Level 3)
- [Organization Name] security Manager
- Systems Architect
- Operations Administrator
- [Organization Name] security Management (Cyberspace Directorate)
- Engineer
- Incident Response & Threat Intelligence Team
- Guidance Team
- IT Systems Technician
- Helpdesk Technicians (Helpdesk Team)
- Responsible Administrator of Infrastructure Systems
- Information and Data Security Officer
- [Organization Name] security Computer Users
- DPO (Data Protection Officer)

4. Roles and Responsibilities

Clearly defined roles and responsibilities are critical for the development and achievement of a successful framework relating to Physical Security. The Information and Data Security Officer, together with the

© CYberSynchorny, 2024

[Organization Name] security Management and the [Organization Name] security Manager, are responsible for the implementation of the Physical Security Policy, ensuring its correct application and execution.

4.1 Responsibilities of [Organization Name] security Management (Cyberspace Directorate)

The core responsibilities of [Organization Name] security Management include the approval and review of the Physical Security Policy, as well as the related Risk Management Plans and Security Incident Management Plans.

In addition, Management is responsible for creating the necessary conditions to protect the Service's physical facilities. Finally, it is responsible for making decisions on the imposition of sanctions in cases of disciplinary offences relating to Physical Security.

4.2 Responsibilities of the Information and Data Security Officer

The core responsibilities of the Information and Data Security Officer include maintaining and updating information security policies and procedures in relation to the current status of the [Organization Name], as well as training staff on the application of these policies.

In addition, the Officer informs [Organization Name] security Management of any occurrence of potential security incidents. In the event of an incident, the Officer, together with the Incident Response & Threat Intelligence Team, activates the corresponding plan with the aim of addressing the incident and preventing its recurrence.

4.3 Responsibilities of the Operations Administrator

The core responsibilities of the Operations Administrator include controlling and updating the physical and logical accesses of [Organization Name] security users.

Additionally, the Administrator informs [Organization Name] security Management and the Information and Data Security Officer of any modification of user access rights or of the revocation of any user's access. The Administrator is responsible for maintaining this Policy in cooperation with the Information and Data Security Officer.

4.4 Responsibilities of the Incident Response & Threat Intelligence Team

The core responsibilities of the Incident Response & Threat Intelligence Team include identifying emergency situations and coordinating actions for the implementation of incident response plans, as well as documenting control measures for addressing risks.

4.5 Responsibilities of the Guidance Team

The Guidance Team is responsible for managing and monitoring the security of [Organization Name] information systems, and protection of information assets also depends directly on physical access to infrastructures.

The Guidance Team monitors compliance of the [Organization Name] security measures adopted with the physical security requirements set by the Cyberspace Directorate.

4.6 Responsibilities of the [Organization Name] security Manager

The core responsibilities of the [Organization Name] security Manager include participation in the identification, assessment and planning of risk management regarding the protection of [Organization Name] security

© CYberSynchorny, 2024

information and data, as well as active participation in the investigation of security incidents, so that their causes are examined and the necessary corrective actions are designed.

4.7 Responsibilities of [Organization Name] security Computer Users

The core responsibilities of users include the proper application of the Physical Security Policy, as well as reporting any security incident that comes to their attention.

5. Physical Security Policy

5.1 Identification of Physical Security Needs

The Cyberspace Directorate maintains all necessary physical access controls to protect information and data. Users must:

- Keep their physical environments, such as workplaces and devices, secure.
- Immediately report any tampering with or theft of devices.

Network equipment components of the Service, including individual computers, must be secured with locking mechanisms wherever feasible.

Areas that contain data and information in any form or provide access to any element of the Service's Network, are protected by appropriate physical entry controls to ensure that access is granted only to authorised personnel.

Visitors have access to secure areas only under the constant supervision of authorised personnel.

The [Organization Name] security physical facilities meet the necessary physical security requirements so that both employees and visitors are adequately protected from Physical and Environmental Threats.

The Cyberspace Directorate:

- Assesses the physical threats and risks that may be encountered, and based on this assessment, defines the needs for physical security measures.
- Provides necessary instructions for dealing with emergency situations that may occur in the [Organization Name] security building.
- Conducts regular disaster response exercises in order to identify gaps and improve the physical security of its facilities.

5.2 Design and Implementation of Physical Security Measures

Based on the identified needs, appropriate physical security measures are developed and implemented. These may include the installation of security systems, protection from natural disasters and the implementation of emergency plans.

As part of the design, it is determined who has access to the [Organization Name], with a specific definition of roles and access permissions.

5.2.1 Risk Management Plans and Incident Management Plans

The Cyberspace Directorate has drawn up Risk Management Plans and Incident Management Plans to ensure the integrity of data and its operational continuity.

More specifically, for the drafting of Risk Management Plans:

© CYberSynchorny, 2024

- A risk analysis is performed to identify the risks that may affect the [Organization Name], using techniques such as SWOT analysis and other risk assessment methods.
- Strategies are developed to address the identified risks, such as preventive measures, risk transfer (e.g. insurance) and emergency plans.

Similarly, for the Incident Management Plans:

- Potential incidents that may affect the smooth operation of the [Organization Name] security due to natural disasters and cyber-attacks are identified.
- Plans are drawn up for the immediate response to incidents, including evacuation, communication and recovery procedures.

For their proper implementation, adequate staff training and regular monitoring of risk parameters and the results of applied measures are prerequisites. Staff must be trained in the procedures and protocols of the incident response plans and participate in regular simulation exercises to assess their readiness.

After the completion of exercises, the results of exercises and real incidents are recorded and analysed to identify weaknesses.

The Risk Management and Incident Management Plans are reviewed annually or after significant incidents in order to incorporate new knowledge and improvements. They are additionally adjusted based on new needs and technological developments.

5.3 Physical Security Measures – Access to [Organization Name] security Facilities

To maintain the security of its facilities, the Cyberspace Directorate has adopted a number of controls and protective measures. Specifically:

- Access to the [Organization Name] security facilities is via the main entrance. At the main entrance, access is controlled by authorised Service personnel and staff are prohibited from entering the building outside business hours.
- Employees are allowed access to the facilities only during their shift hours.
- The building is equipped with an alarm system and a smoke detection system, which are monitored remotely.
- The building is surrounded by security cameras (CCTV).
- All Service personnel have access to the building after identity verification and recording of their details at the entrance.
- Personal electronic equipment is handed over upon entry, while access by third parties is by appointment, after stating their full name at the facilities' entrance and undergoing the physical checks mentioned above.

5.4 Physical Protection of Critical Information Assets

With regard to the physical security of the [Organization Name], the Cyberspace Directorate ensures and has taken the necessary measures to protect the facilities from natural disasters, as well as to protect equipment and prevent potential system downtime or information loss. Specifically:

- Assets and electronic equipment of the [Organization Name] (computers, laptops, servers, components) are placed above floor level in order to protect them in case of flooding.

© CYberSynchorny, 2024

- A programme has been defined for recording, monitoring and assessing activities to detect potential malfunctions, by performing test security operations to identify vulnerabilities.

The combination of these practices helps ensure physical security at the [Organization Name], protecting equipment, data and staff from threats.

The facilities where critical information is stored or processed are constructed in such a way that information is adequately protected from physical and environmental threats. The construction and design of the facilities protect the critical information assets from unauthorised access, alteration and destruction.

5.5 Physical Security of the [Organization Name]

Physical security in [Organization Name] refers to the measures taken to protect the [Organization Name]'s physical environment and equipment. These measures help ensure the security of the systems and data managed by the [Organization Name].

More specifically:

- Access to the [Organization Name] security is controlled via restricted entry points and the use of access control systems.
- The [Organization Name] security building has a comprehensive video surveillance system using security cameras to detect breaches and malfunctions.
- All [Organization Name] security areas have appropriate systems in place to maintain suitable temperature and humidity in order to protect sensitive equipment.
- Backup power systems are in place to ensure the continuous operation of the [Organization Name] security in the event of power outages.
- The [Organization Name] security is equipped with fire detection systems for protection against fire, including fire extinguishers, fire-fighting equipment, fire detectors and fire-suppression systems.

Physical security is an important part of the overall security of the [Organization Name], as it ensures that critical infrastructures remain inaccessible to unauthorised actors.

5.6 Physical Security of the Data Center

The Data Center area is permanently locked. Servers are kept locked in racks throughout the day and are raised above floor level to protect them from potential flooding or moisture.

In addition, there is appropriate air-conditioning at a stable temperature using specialised units, while fire protection and fire safety are provided through special carbon dioxide (CO_2) fire extinguishers.

5.7 Security Measures for Internal and Classified Areas

To ensure the level of security in critical internal areas of the [Organization Name] security building facilities, a series of measures are applied, which serve the proper monitoring of these areas as well as the prevention of unauthorised access.

The selection and implementation of physical access control mechanisms are based on the criticality of the Information and Information Assets hosted within them.

The following protective measures for internal areas are applied for the security of critical and classified areas (e.g. Data Center):

© CYberSynchorny, 2024

- Locking of internal entrances.
- Reinforced/raised floors, bullet-resistant window glazing and ceilings protected from moisture, as well as appropriate ventilation/air-conditioning systems installed, monitored for proper operation and maintained.
- Packaging materials from new equipment are removed immediately from the Data Center.
- Equipment used temporarily within the Data Center (laptops, monitors, keyboards, mice, power cables, network cables, etc.) is removed after the completion of the relevant work.

5.8 Measures for the Prevention and Response to Fire, Flood and Other Natural Disasters

To prevent the occurrence and spread of potential fire, a number of measures are taken, including:

- Use of non-flammable construction materials.
- Thorough cleaning of premises.
- Installation of electrical grounding.
- Installation of fire-resistant doors.
- Critical information in printed or electronic form is stored in fire-resistant cabinets/safes.
- Instructions for the prevention and response to fires and other emergencies are posted throughout the premises.

In addition to preventive security measures, in the event of a fire at the [Organization Name] security facilities, all necessary steps are taken to limit and quickly extinguish the fire.

The facilities also have a mechanism for unlocking exits in case of malfunction.

Information assets and information systems are installed in appropriate locations to ensure there is no risk of leakage from the water supply and sewage network or risk of water ingress from external windows.

All building facilities meet generally accepted specifications and seismic standards.

5.9 Uninterruptible Power Supply

Information systems are protected from power outages or other problems in electricity supply through backup generators owned by the Cyberspace Directorate.

Critical Information Assets and Information Systems are protected from voltage interruptions or any other problem in power supply. Additionally, uninterruptible power supplies (UPS) are used to ensure their continuous operation.

5.10 Training and Awareness

Employees are trained on the risks and safe practices for maintaining physical security. Awareness-raising activities are also carried out on the importance of physical security, such as training programmes and information events.

Any questions or requests for clarification regarding the content of this Policy must be addressed to the Information and Data Security Officer.

© CYberSynchorny, 2024

5.11 Verification and Review of the Policy

The Physical Security Policy is periodically reviewed and verified to ensure it remains applicable and effective. During this review, new physical security threats and any changes that have occurred since the previous version are analysed.

6. Obligation of Implementation

This Policy is an integral part of the [Organization Name] security policy. All involved parties are obliged to comply with this procedure to ensure effective physical security of the [Organization Name].

7. Disciplinary Sanctions for Non-Implementation

Any violation of this Policy, as well as any breach of physical security of infrastructures and equipment, will be treated strictly and may result in disciplinary measures, including legal action, depending on the severity of the violation.

Data subjects concerned have the right to submit questions about this Policy and to request clarifications from the Information and Data Security Officer.

This Policy enters into force as of [Approval Date] and is reviewed periodically to ensure its compliance with the needs and requirements of the Service.

© CYberSynchorny, 2024

4.15 Tool 15 - Business Continuity and Disaster Recovery Policy

[Organization Name]

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

© CYberSynchorny, 2024

Table of Contents

1. Introduction
   1.1 Purpose
   1.2 Scope of Application
2. Business Continuity Policy
   2.1 Business Impact Analysis
   2.2 Business Continuity Plan (BCP)
   2.3 Business Continuity Exercises and Simulations
   2.4 Disaster Recovery Plan (DRP)
   2.5 Backups and Data Recovery
   2.6 Lessons Learned and Continuous Improvement
   2.7 Availability Management
   2.8 Capacity Management
3. Review
4. References

© CYberSynchorny, 2024

1. Introduction

1.1 Purpose

The Business Continuity Policy establishes the framework to ensure that [Organization Name] can maintain or rapidly restore critical operations during and after an event that leads to service disruption, such as a cyberattack, a natural disaster or a system failure. It aims to minimise the impact of disruptions on operations, safeguard key resources and ensure the continuity of services to stakeholders and customers. The policy demonstrates [Organization Name]'s commitment to resilience and operational reliability.

More specifically, the objectives of the Business Continuity Policy are:

- The identification and prioritisation of critical business processes, resources and systems required for the continued operation of [Organization Name].
- The development and maintenance of a Business Continuity Plan (BCP) that describes in detail the procedures for addressing disruptions.
- The development and maintenance of a Disaster Recovery Plan (DRP) that describes in detail the procedures for addressing disruptions to IT systems.
- The definition of roles and responsibilities for managing business continuity across the Organization.
- The assurance of the resilience of critical infrastructures and resources through risk assessment methodologies, mitigation strategies and the provision of redundancy.
- The conduct of regular testing, training and updating of the Business Continuity Plan (BCP) to ensure its effectiveness and alignment with the current needs of [Organization Name].
- Compliance with relevant laws, regulations and standards in order to demonstrate the necessary reliability and professionalism on behalf of [Organization Name].

1.2 Scope of Application

The Business Continuity Policy applies to all departments, employees and third-party service providers involved in supporting or delivering critical business functions of [Organization Name], regardless of geographical location, that are necessary for the uninterrupted operation of [Organization Name]. It covers the physical, technical and administrative resources required for continuity, including IT systems, facilities, personnel and supply chains.

2. Business Continuity Policy

2.1 Business Impact Analysis

[Organization Name] maintains a Business Impact Analysis (BIA) process to identify all critical resources within [Organization Name] and to produce results in a relevant report, which is presented to management and approved by it. This process must be carried out annually and include the following:

- Definition of assessment criteria related to the context of [Organization Name], including types of impacts and time frames.
- Identification of activities that support the delivery of [Organization Name]'s products and services.
- Application of the assessment criteria to estimate the expected impacts over time arising from the interruption of these activities.
- Estimation of the time after which the impacts of not resuming the activities become unacceptable.

© CYberSynchorny, 2024

- Determination of time frames for resuming activities to minimum acceptable levels of operation within the aforementioned time.
- Identification of priority activities.
- Identification of dependencies of priority activities, including human resources, information and data, buildings, workplaces and related utilities, equipment and consumables, ICT systems, transport and logistics, financing and partners within [Organization Name]'s supply chain.

The results of the Business Impact Analysis must be recorded within the unified inventory of assets, systems and processes of [Organization Name].

[Organization Name] must define appropriate roles with responsibilities for conducting the Business Impact Analysis.

[Organization Name] must prioritise functions and systems based on the necessity to provide business services.

The Business Impact Analysis must be performed based on a classification system that considers defined criticality levels and examines whether critical functions or systems operate independently or are linked to other functions or systems of [Organization Name]. To this end, and where possible, meetings should be held with a representative group of staff from each department involved in order to collect information for the Business Impact Analysis.

Potential business continuity and disaster recovery strategies must be analysed and documented, by process and by type of impact, and the report to management must include at least the elements for the Recovery Time Objective (RTO), Maximum Allowable Outage (MAO) / Maximum Tolerable Period of Disruption (MTPD), Recovery Point Objective (RPO) and Minimum Business Continuity Objective (MBCO) that [Organization Name] has defined for each process or activity.

Where possible, business continuity strategies must be documented and presented to management, accompanied by a Cost-Benefit Analysis. Management evaluates these strategies and approves them as appropriate. Subsequently, the Business Continuity and Disaster Recovery Plans are drawn up in accordance with the strategies approved by management.

The scales used to assess expected impacts, as well as for risk analysis and evaluation, must be approved by [Organization Name]'s management and formulated in such a way that they are understandable to all involved personnel.

The Business Impact Analysis must be carried out at least at the level of:

- [Organization Name]'s compliance.
- Achievement of [Organization Name]'s objectives.
- Financial impacts, impact on [Organization Name]'s reputation.
- Impact on the health, safety and wellbeing of staff.
- Impact on the health, safety and wellbeing of users of the services.

2.2 Business Continuity Plan (BCP)

The Business Continuity Plan concerns the holistic management process that identifies potential threats that may interrupt [Organization Name]'s operations, whether due to internal or external factors. For example: pandemic, natural disasters (such as storms and floods), man-made disasters (such as terrorism or fire) or large-scale failures of IT systems. Business continuity management provides a framework for building Organizational resilience with the ability to respond effectively, safeguarding the interests of key external partners, reputation and value-creating activities.

© CYberSynchorny, 2024

[Organization Name] implements and maintains a Business Continuity Plan in order to ensure that [Organization Name] can respond to emergencies in an immediate and appropriate manner, and is able to maintain business operations and critical activities, minimising the consequences and damage resulting from an incident.

The Business Continuity Plan focuses on the impacts that [Organization Name] may face due to a disruption in its normal operation, regardless of the causes that triggered it.

Each Business Continuity Plan must be known to the involved personnel and be available when needed.

Additionally, the plan includes the following:

- The purpose, scope and objectives of each plan.
- The assumptions and exclusions of the plan.
- The roles and responsibilities of the team that will implement the plan.
- The steps and details to continue or recover business activities to a predefined level and within an acceptable timeframe. It also includes monitoring the impacts of the incident and responding to reduce its extent, taking into account the health and safety of individuals, limiting the spread of the disruption, and impacts on the environment and society.
- Definition of the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to avoid unacceptable consequences for [Organization Name]. The RTO and RPO must be defined for each process, service and, where feasible, for each important activity.
- Resource requirements as identified in the Business Impact Analysis, for the proper operation of critical processes within a predefined timeframe.
- Analysis of required human resources over time.
- The process and responsibilities for notification, assessment, decision to activate and implementation of the plan.
- Internal and external interdependencies and provisions for their continuity.
- Methods and contact details for communication between stakeholders.
- The relevant documentation that will be kept in case of activation.
- The stand-down procedure.
- Where possible, potential business continuity and disaster recovery strategies must be analysed and those recorded which, by process, by type of impact, by RTO and MAO (Maximum Acceptable Outage), can enable [Organization Name] to recover business activities within the predefined acceptable time.
- Business continuity strategies must be documented and presented to management, accompanied by a Cost-Benefit Analysis. Management must evaluate these strategies and approve them.
- Business Continuity and Disaster Recovery Plans must be drawn up in accordance with the strategies that have been accepted and approved by management.

2.3 Business Continuity Exercises and Simulations

[Organization Name] must implement and maintain measures to test, review and improve the Business Continuity Plan through simulated incident exercises.

Business continuity exercises and simulations must test [Organization Name]'s response to incidents and identify opportunities for improvement, achieving better results over time.

© CYberSynchorny, 2024

[Organization Name] must conduct business continuity exercises and simulations annually. When preparing the Business Continuity Plan, disaster recovery is also considered.

[Organization Name] maintains an exercise and testing plan/programme which ensures that exercises and tests are carried out that are compatible with [Organization Name]'s business continuity objectives, are based on appropriate scenarios, and target specific aspects of the plans.

For exercises and tests, written records are kept that state the history of the test, the times per step according to the applicable plan or part of the plan, and any observations.

The Business Continuity Plan must be linked to changing management procedures so that the consequences of any changes within [Organization Name] are taken into account.

2.4 Disaster Recovery Plan (DRP)

A Disaster Recovery Plan is implemented and maintained for the restoration and recovery of critical processes and activities, IT systems and supporting resources, such as power supply, after an incident, in order to ensure that [Organization Name] responds to emergencies in an immediate and appropriate manner and is able to maintain business operations and critical activities, minimising the consequences and damage resulting from an incident.

The plan must focus on the impacts that [Organization Name] may face due to disruption of the normal operation of IT systems, regardless of the causes that triggered it.

It includes, among others, the following:

- The purpose, scope and objectives of the plan.
- Clear instructions for IT staff for timely and effective response to incidents affecting [Organization Name]'s IT environment.
- The roles and responsibilities of the team that will implement the plan. Staff involved in operating the Disaster Recovery Plan must be fully informed about their responsibilities and accountabilities.
- Definition of Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to avoid unacceptable consequences for [Organization Name]. The plan clearly defines the target in relation to recovery time, the maximum acceptable downtime of systems and the resources required for recovery.
- The Disaster Recovery Plan must include all resources required, as identified in the Business Impact Analysis, for the proper operation of critical processes within a predefined timeframe.
- The Disaster Recovery Plan provides for the existence of appropriate licensed software for the recovery of data from the relevant backups.
- The assumptions and any exclusions of the plan.
- A table with contact details between stakeholders.
- The relevant documentation that will be kept in case of activation of the plan.

Where feasible, backup records must be encrypted using cryptographic algorithms.

Updates and changes to the Disaster Recovery Plan must be carried out in accordance with [Organization Name]'s change management process.

Disaster Recovery Plans must be stored in a secure location, protected by appropriate measures as information of the highest classification level, and it must be ensured that they are available in case of destruction of the primary site.

© CYberSynchorny, 2024

For exercises and tests, written records must be kept that state the history of the test, the times per step according to the applicable plan or part of the plan, and any observations.

2.5 Backups and Data Recovery

[Organization Name] implements and maintains a backup and data recovery procedure to ensure timely and effective restoration of data after an event or incident, or upon request. [Organization Name] has designated a responsible person for the operation and maintenance of backups.

Backup and data recovery procedures must be adequately and periodically tested in order to ensure the proper and reliable operation of all supporting processes and systems.

Production systems and support infrastructures that enable backup and data restoration must be geographically separated.

Backups must cover all information or their changes on at least a daily basis.

The backup frequency, at least for critical systems, must be defined to occur every [XX] hours. A backup retention scheme has been created at day/week/month/year level.

2.6 Lessons Learned and Continuous Improvement

[Organization Name] is committed to fostering a culture of continuous improvement in the planning and execution of business continuity. After each business disruption, incident or business continuity exercise, the leader together with the members of the Business Continuity Plan and/or Disaster Recovery Plan Execution Team undertakes the conduct of a structured debriefing meeting to review the process and record the lessons learned. Ideally, this meeting should be held within 24 hours of completing plan execution.

The Execution Team reviews various records to ensure they reflect the actual events and the full and accurate recording of the plan scenarios. In addition, successes and gaps that require improvement in the plans, procedures and responses of the Team are identified.

The results of these reviews are documented and incorporated into a new version of the Business Continuity Plan and the Disaster Recovery Plan. Incorporating lessons learned helps [Organization Name] continuously adapt to evolving risks.

2.7 Availability Management

The responsible Technology Department of [Organization Name] must develop an availability management strategy and maintain an availability management process for resources at all times, ensuring that the desired level of business services is provided. The process must cover both current availability and performance issues and future requirements. Availability must be reviewed on a regular basis.

Within this framework:

- [Organization Name] has assessed and determined the criticality of its resources in order to apply measures for their redundancy and availability according to the criticality of each resource. All IT systems related to critical resource(s) for [Organization Name] must have a defined capacity limit.
- [Organization Name]'s equipment provides redundancy in terms of power, capacity, network and connectivity, while critical equipment must have redundancy in the same site in active or passive mode.
- [Organization Name] maintains equipment at a secondary site which can be used to recover critical functions of [Organization Name] in case the equipment at the primary site is not available.

© CYberSynchorny, 2024

- If an asset has been identified as unavailable, the appropriate personnel is notified to investigate and perform the manual switchover to the backup system (if required).
- The availability level of assets is monitored continuously in order to identify in time cases of reduced availability.
- Provision has been made to allow access to and recovery of data as required from backups.
- Replication solutions must be implemented to an alternate site for critical systems, and a full functional test of the replication status and the ability of [Organization Name] to operate from there must be conducted annually.
- In the event of failure or unavailability of primary equipment, automatic actions are taken to activate the secondary equipment.
- Separate backups must be maintained at a third secure location so that [Organization Name] can also be protected from ransomware attacks.
- Immediate notifications must be sent to both business owners and system administrators in the event of unavailability of one or more systems or if a defined critical threshold has been exceeded.
- It is recommended that at least the following three categories be defined as thresholds for availability/capacity purposes (see paragraph 2.8 below):
    - **Warning Level:** An indicative threshold in an IT operating unit has been reached.
    - **Alert Level:** An indicative threshold in an IT operating unit has been reached that indicates a critical limit for which immediate action must be taken by the responsible engineer and the system owner.
    - **Critical Level:** Reaching the critical threshold requires activation of the information security incident response process.

2.8 Capacity Management

The use of computing resources (disk capacity, CPU utilisation, system throughput, etc.) must be monitored, coordinated and properly planned in order to ensure the required availability and performance of systems, in line with the evolving requirements of [Organization Name] both internally and externally (see Systems Security Policy).

[Organization Name] must have adopted a capacity management process in order to ensure the performance of information systems, including a mechanism for managing the capacity of these critical resources. Furthermore, handling of emergency situations with increased demand must be taken into account.

[Organization Name] must monitor capacity metrics of Information Systems, and for critical resources this monitoring must be implemented using automated mechanisms.

Asset owners are required to define the necessary availability management procedures to ensure that the desired level and performance of information systems for supporting relevant business processes and workloads is provided. The responsible Technology Department of [Organization Name] is required to ensure that these requirements are met by allocating and maintaining the necessary resources at minimum cost.

System tuning and monitoring must be carried out to ensure the best possible performance in terms of capacity.

Future capacity needs must be forecast. It is recommended that, for critical Organizational assets and core functions, studies have been carried out for planning appropriate resources over a five-year horizon.

Capacity planning must be carried out taking into account historical and recent data, as well as trends and [Organization Name]'s future plans and objectives.

© CYberSynchorny, 2024

[Organization Name] must conduct stress tests to confirm the effectiveness of related forecasts.

3. Review

The Business Continuity Policy must be reviewed and updated at least annually to ensure alignment with current business objectives, processes and threats, with the aim of improving its effectiveness. It may also be reviewed after business continuity exercises or simulations (e.g. tabletop exercises, live exercises), and the results are examined to identify weaknesses or gaps, and the plan is updated accordingly.

Additionally, the policy may be reviewed in the event of significant changes in [Organization Name]'s environment or after information security incidents or regulatory changes.

4. References

Category	ID	Measure	Objective of Measure
Business Continuity and Resilience	BCR1	Business Impact Analysis	To ensure that the Organization has analysed and assessed the critical business processes that must be taken into account in the business continuity plan, so that it can restore business processes to an acceptable level as soon as possible in the event of an event or incident.
Business Continuity and Resilience	BCR2	Business Continuity Plan	To ensure that the Organization has a plan to maintain the continuity of critical business processes and to restore them during and after an event or incident.
Business Continuity and Resilience	BCR3	Business Continuity Exercises and Simulations	To ensure that the Organization and its staff know their responsibilities during an event or incident that activates the business continuity plan.
Business Continuity and Resilience	BCR4	Disaster Recovery Plan	To ensure that the Organization has a plan to restore critical information systems to an acceptable level during or after an incident.
Data Security	DS3	Backups and Data Recovery	To enable restoration of information in the context of security events and incidents.

© CYberSynchorny, 2024

Asset Management	AM4	Availability Management	To ensure the availability of networks and information systems by achieving adequate resource availability, redundancy and high-availability systems/procedures.
Asset Management	AM6	Capacity Management	To ensure adequate capacity and performance of information systems and processes.
Network Security	NS6	Redundancy and High Availability	To ensure the availability of information and information networks by achieving sufficient availability of resources, backup equipment, high-availability systems and connections.

© CYberSynchorny, 2024

5 Supporting Tools and Templates

This section describes the structured set of supporting tools, guides, and templates that accompany the Organization's policies and procedures. These resources ensure consistency, traceability, and effective application of the cybersecurity and compliance framework.

5.1 Document Completion Guide

The Document Completion Guide provides clear and standardised instructions for drafting, tailoring, approving, and maintaining policies, procedures, and governance documents.

It explains how each document should be completed so that it can be adapted to the specific Organizational context while remaining aligned with the CYberSynchrony methodology and regulatory requirements.

5.2 Measure Effectiveness Evaluation Procedure

This procedure defines the KPIs and metrics that Organizations should use to measure the effectiveness of their cybersecurity controls, processes, and policies.

Examples include:

- Incident response time
- Patch implementation timelines
- Percentage of employees completing mandatory cybersecurity training
- Number and severity of audit findings

5.3 Statement of Applicability (SoA)

The Statement of Applicability (SoA) lists all controls considered by the Organization, indicating whether each control is implemented, not implemented, or not applicable.

For each control, the SoA explains the rationale behind its inclusion or exclusion and provides references to supporting documentation and evidence.

5.4 Asset-Based Risk Assessment Workbook

The risk assessment workbook (Excel format) includes structured fields for:

- Asset identification
- Threats
- Vulnerabilities
- Impacts
- Risk scoring and prioritisation

This enables the Organization to maintain a consistent, repeatable, and evidence-based risk assessment methodology.

5.5 Impact Assessment Templates (BIA, Impact Assessments)

This set of templates includes:

- Business Impact Analysis (BIA)
- Data Protection Impact Assessment (DPIA)
- Technical Impact Assessment templates

© CYberSynchorny, 2024

These templates support structured evaluation of operational, regulatory, privacy, and business impacts associated with potential incidents.

5.6 Checklists and Compliance Mappings

Supporting documents include compliance checklists and mapping tables for:

- C.D.P. 389/2020 (Cybersecurity Toolkit of the Digital Security Authority of Cyprus) [1]
- Hellenic National Intelligence Service Cybersecurity Policies [2]
- NIS2 (Network and Information Systems Directive 2) [3]
- ENISA Cybersecurity Standards [4]
- GDPR (General Data Protection Regulation) [5]
- CRA (Cyber Resilience Act) [6]
- ISO/IEC 27001:2022 (information security management systems) [7]

These resources help Organizations track compliance obligations and identify gaps.

© CYberSynchorny, 2024

6 Implementation and Monitoring

6.1 Compliance and Control Mechanisms

This section defines the mechanisms through which the Organization ensures ongoing compliance with policies and procedures.

These mechanisms include:

- Compliance checks
- Reporting workflows
- Corrective and preventive action mechanisms (CAPA)

Exception management processes

6.2 Performance Indicators and Effectiveness Measurement (KPIs, Metrics)

A set of technical and operational KPIs is used to evaluate the Organization's cybersecurity performance.

Examples include:

- MTTR (Mean Time to Respond)
- Vulnerability remediation rate
- Percentage of systems covered by security monitoring

Business continuity test success rate

6.3 Control and Audit Procedures

This section specifies the audit framework used to evaluate compliance and effectiveness across all cybersecurity processes. It includes:

- Internal audits
- External audits
- Evidence and documentation requirements
- Risk-based audit planning

© CYberSynchorny, 2024

7 Conclusions

The CYberSynchorny Policy Toolkit (D6.3) is the result of the best policies and practices applied in operational level by two National Cybersecurity Authorities (a) the Digital Security Authority of Cyprus (DSA) and (b) the Hellenic National Intelligence Service. The toolkit provides a comprehensive, practical, and adaptable framework for establishing a robust Organizational cybersecurity posture.

In a ready and easy-to-use process, cybersecurity stakeholders are able to uptake the fifteen (15) policy tools and develop their individual Toolkit building the security framework of their Organization. The Toolkit shall be updated by security officers in consistent modus aiming to address any evolvement in the global cybersecurity landscape.

As initial version, D6.3 focuses on feeding the connected Tasks of WP6 to design the components of CYBERWISE and CYBERG Platform including the Training Plan, the Immersive Cybersecurity Game and the Real-time Compliance Oversight Tool as well as the connected WP8 Tasks on the planning and demonstration of CYberSynchorny Platform on three comprehensive Use Cases on CyberHealth, Public Administration and Universities sectors.

The D6.7 iteration version will incorporate (a) any advancements on cybersecurity landscape, (b) the outputs of the D6.5 ‘Cyber Awareness Platform’, D6.6 ‘Gamified Training Modules’ and D6.8 Compliance Monitoring and (c) the lessons learned from the testing of Policy Toolkit components throughout the demonstration of CYberSynchorny Platform into CyberHealth, Public Administration and Universities sectors.

© CYberSynchorny, 2024

8 References

[1] Digital Security Authority of Cyprus. Cybersecurity Policy Toolkit. Retrieved on 26-11-2025 from URL: https://dsa.cy/activities/toolkit

[2] Hellenic National Intelligence Service (2025). Retrieved on 26-11-2025 from URL: https://www.nis.gr/en/information-security/infosec

[3] European Parliament and the Council (2022). NIS 2 Directive. Retrieved on 26-11-2025 from URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[4] ENISA (2025). Cybersecurity Standards. Retrieved on 08-12-2025 from URL: https://www.enisa.europa.eu/audience/national-eu-authorities

[5] European Parliament and the Council (2016). General Data Protection Regulation. Retrieved on 26-11-2025 from URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[6] European Parliament and the Council (2024). Cyber Resilience Act. Retrieved on 26-11-2025 from URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[7] International Organization for Standardization (2022). ISO/IEC 27001:2022 (Information Security Management Systems). Retrieved on 26-11-2025 from URL: https://www.iso.org/standard/27001

[8] ENISA (2025). EU Legislative Landscape. Retrieved on 08-12-2025 from URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies

© CYberSynchorny, 2024

Annex I: Summary (from Grant Agreement)

CYberSynchrony introduces a cybersecurity coordination and resilience framework that supports improved threat detection, intelligence sharing, preparedness, response capacity, and workforce development across Europe.

The project integrates advanced technologies, operational tools, governance mechanisms, and human-centric training resources to enhance coordination and response capabilities.

WP6 "Cybersecurity Consciousness: Empowering Society Through Awareness (CYBERWISE) and Cybersecurity Standardization and Compliance Reinforcement (CYBERGOPLUS)."

WP6 Objectives:

(1) Engage diverse societal segments with cybersecurity awareness.

(2) Utilize gamification techniques to make learning impactful.

(3) Measure the effectiveness of awareness campaigns using data analytics.

(4) Cultivate a culture prioritizing secure online behaviour.

(5) Support comprehensive cybersecurity policy implementation.

(6) Establish unified standards across various sectors.

(7) Monitor and audit adherence to established cybersecurity standards.

(8) Ensure industry-wide compliance with regulations.

Task 6.5 - Tailored Cybersecurity Policy Tools (Leader: KETYAK; Participants: IANUS, DSA, BYTE) [M12-M27]

Recognizing the dynamic nature of the cyber landscape, this task focuses on the development of adaptable tools and templates. These will assist in the creation and revision of cybersecurity policies and regulations. By streamlining the process, it ensures that the regulatory framework remains current, robust, and aligned with the evolving threat landscape. The tools are designed to be intuitive, catering to policymakers and regulators alike. This task emphasizes that policies should not be static; they need to evolve to address new challenges, ensuring the digital landscape remains secure.

© CYberSynchorny, 2024

Annex II: Consortium Members

Table 17: Consortium Members

No	Short Name	Organization	Country
1	MAG	MAGGIOLI SPA	IT
2	eBOS	EBOS TECHNOLOGIES LIMITED	CY
3	IANUS	IANUS CONSULTING LTD	CY
4	TRUST	TRUSTILIO BV	NL
5	UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER	EL
6	DSA	ARCHI PSIFIAKIS ASFALEIAS (DSA)	CY
7	KETYAK	ETHNIKI YPIRESIA PLIROFORION	EL
8	FP	FOCAL POINT	BE
9	BYTE	BYTE COMPUTER S.A	EL
10	EGL	DIMOS EGALEO	EL
11	MER	MERIDIAN SRL	IT
12	AMC	SAMOUTIS & ASSOCIATES	CY

© CYberSynchorny, 2024