Minimum Mandatory Cyber Security Standards for Government Institutions

Republic of North Macedonia

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

Republic of North Macedonia
Ministry of Digital Transformation

DAI
Shaping a more livable world.

TAG International

Document Title: Minimum Mandatory Cyber Security Standards for Government Institutions

Document History:

Publication Date	Version No.	Description
26 January 2025	5.0	Fifth draft

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This product is prepared within the programme Western Balkan Cyber Security funded by the UK Government with the support of the British Embassy Skopje. The content of this publication does not necessarily reflect the position or the opinions of the UK Government.

Овој производ е подготвен во рамки на проектот Сајбер безбедност во Западен Балкан, Рефинансиран од Владата на Обединето Кралство, со поддршка на Британската амбасада Скопје. Мислењата и ставовите наведени во оваа содржина не ги одразуваат секогаш мислењата и ставовите на Британската Влада.

Ky produkt është përgatitur në kuadër të programit Siguria kibernetike në Ballkanin Perëndimor i financuar nga Qeveria e Mbretërisë së Bashkuar me mbështetjen e Ambasadës Britanike Shkup. Përmbajtja e këtij publikimi nuk pasqyron domosdoshmërisht qëndrimin ose mendimet e Qeveria e Mbretërisë së Bashkuar.

Table of Contents

Foreword

Recognizing the critical role of government institutions in the security of sensitive data and critical services, a standardized framework of cybersecurity standards has been designed to ensure the protection of digital assets, enhance human security, national security and the continuity of national essential functions. The process involved an established multi-stakeholder platform comprising government agencies and representatives from the private sector and academia. This platform facilitated trust building, information sharing and collaboration, leading to shared decision-making and cross-sector involvement. National experts mentored the group to develop, maintain and upgrade state-of-the-art standards tailored to the unique requirements of various government institutions. A comprehensive guidance document was created to help understand and effectively implement these standards, covering risk assessment, compliance monitoring and best practices.

These minimum cybersecurity standards consist of baseline cybersecurity requirements, guidelines and practices to implement in North Macedonia Government Institutions.
Each chapter from *1* to *18* describes one security control family.
The standard contains requirements on 3 levels of cybersecurity maturity. Selection and implementation per level depend on the organisation's size.

- Level 1 is the set of basic cybersecurity requirements to be implemented by all organisations that primarily provide services supported by ICT systems.
- Level 2 is the set of industry-standard requirements for an operator that serves a significant number of citizens, and the service is crucial for social and economic factors of the nation. These requirements are mandatory for an provides a service to at least 250.000 unique users and/or beneficiaries
- Level 3 is the set of advanced cybersecurity requirements for an organization processing critical information or/and data, which could severely impact social and economic factors of the nation, should it fail.

Compliance with these requirements is necessary to minimize the risk of disrupting the functioning of the Government Institutions.
It is necessary to remember that all these factors will change over time.

Note 1:	Government Institutions have the authority to waive requirements that are technically or organizationally impossible to implement. Additionally, if a risk assessment determines that a requirement doesn't apply, or if the specified objective can be achieved through alternative security measures, it may be waived. Justification for waiving specific requirements is essential.
Note 2:	The order in which the requirements appear in this document does not indicate their relative importance or the sequence in which they should be implemented. The numbering serves only for ease of reference.
Note 3:	The requirements in this document apply only to Government Institutions located within the territory of the Republic of North Macedonia.
Note 4:	This standard applies to infrastructure (including network devices, hosts, endpoints, etc.), software, services, and data under the possession of Government Institutions.
Note 5:	Government Institutions are advised not to restrict implementation controls solely to their assigned tiers. Instead, they should strive to implement the highest level of security measures to enhance resilience.

Terms, definitions and abbreviated terms.

Terms and definitions

Term	Definition
Access Control	Measures that restrict access to resources to only those who are authorized.
Accountability	The concept that individuals are responsible for their actions and may be held accountable.
Asset	Any resource, device, or information that is valuable to an organization.
Authentication	The process of verifying the identity of a user, process, or device.
Authenticity	Ensuring that information or data is genuine and from a verified source.
Availability	Ensuring that information and resources are accessible to authorized users when needed.
Baseline Security	Minimum set of security controls required for safeguarding an organization's assets.
Business Continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incidents.
Chief Information Security Officer (CISO)	A senior-level executive responsible for establishing and maintaining the organisation vision, strategy, and program to ensure information assets are adequately protected.
Computer Security Incident Response Team (CSIRT)	A team responsible for receiving, reviewing, and responding to computer security incidents.
Communication Infrastructure	The physical and virtual resources used to transmit data, including networks, servers, and software.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Control	A safeguard or countermeasure to avoid, detect, counteract, or minimize security risks.
Countermeasure	Actions, devices, procedures, or techniques that reduce a threat, vulnerability, or attack by eliminating or preventing it.
Critical Infrastructure	Key assets and systems that require stringent safeguarding measures to protect against threats and ensure resilience.
Cybersecurity Strategy	Strategic documents outlining national and organizational cybersecurity strategies, including short-term and long-term goals.
Security Control	Specific measures or mechanisms to mitigate security risks.
Security Measures	Various strategies and actions taken to protect information systems from threats.
Safeguard	Protective measures implemented to counter threats and vulnerabilities.
Information Asset	Any information or data, and associated systems, that have value to the organization.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations.

Security Incident	An event that may indicate that an organization's systems or data have been compromised.
Information Security Event	Identified occurrence of a system, service, or network state indicating a possible breach of information security policies or failure of safeguards.
Information Security Management System (ISMS)	A systematic approach to managing sensitive company information so that it remains secure, involving people, processes, and IT systems.
Information Security Policy	A set of rules and practices that regulate how an organization manages, protects, and distributes information.
ICT Infrastructure	Information and Communication Technology components and systems used to manage and communicate information.
Integrity	Ensuring that information is accurate and complete and that it has not been altered in an unauthorized way.
Internal Audits	Internal checks carried out following best practices, potentially by employees or approved third parties, with documentation of all reports from audits.
Media	Physical or electronic methods of storing data, including paper, disks, USB drives, etc.
Non-repudiation	Assurance that someone cannot deny the validity of something, ensuring actions or events can be proven to have occurred.
Non-privileged Account	A user account with limited access rights to systems and data.
Privileged Account	An account with elevated access rights that can perform administrative tasks.
Reliability	The ability of a system or component to consistently perform its required functions under stated conditions for a specified period of time.
Risk	The potential for loss or harm related to the exploitation of vulnerabilities.
Risk Assessment	The overall process of risk identification, risk analysis, and risk evaluation.
Risk Analysis	The systematic use of information to identify and evaluate risks to the organization's operations and assets.
Risk Evaluation	Comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk Identification	The process of finding, recognizing, and describing risks.
Risk Management	Coordinated activities to direct and control an organization with regard to risk.
Risk Treatment	The process of selecting and implementing measures to modify risk.
Security Zone	Distinct areas within a managed space designed based on security requirements and risk assessments.
Service-Level Agreement (SLA)	A contract between a service provider and a customer specifying the level of service expected during its term.
Information System	A system comprised of people, processes, and information technology designed to manage and process information.
Telecommunication Service Provider	A company that provides telecommunication services such as internet, phone, and data communication.

Table 1 – Terms and definitions

Abbreviations

API	Application Programming Interface
BYOD	Bring Your Own Device
CDP	Continuous Data Protection
CCTV	Closed-Circuit Television
CSIRT	Computer Security Incident Response Team
DAST	Dynamic Application Security Testing
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
ESP	Essential Service Provider
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IDE	Integrated Development Environments
IOC	Indicators Of Compromise
IoT	Internet of Things
IPS/IDS	Intrusion Prevention System/Intrusion Detection System
IPX	Internetwork Packet Exchange
ISAC	Information Sharing and Analysis
ISMS	Information Security Management System
ISP	Information Security Policy
LAN	Local Area Network
LLMNR	Link-Local Multicast Name Resolution
MAC	Media Access Control address
MFA	Multifactor Authentication

NAC	Network Access Control
NGFW	New Generation Firewall
NPI	Non-public Information Note 1: The categories of data requiring protection in ESPs can be classified following the model presented in ICT Implementation Guidelines for GoR issued by RISA, sub-chapter 5.2. Note 2: Personal data (articles 11, 37 and 38 of [Law 058/2021]) should be included in NPI.
OSI	Open Systems Interconnection
OSINT	Open Source Intelligence
PII	Personally Identifiable Information / Personal Data
RDP	Remote Desktop Protocol
RA	Risk Assessment
SAST	Static Application Security Testing
SIEM	Security Information and Event Management
SME	Subject Matter Experts
SOC	Security Operation Center
SSH	Secure Shell protocol
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WAF	Web Application Firewall
WPAD	Web Proxy Auto-Discovery Protocol

Table 2 – Abbreviations

1. ACCOUNT MANAGEMENT & ACCESS CONTROL

LEVEL	SECURITY MEASURES
1	***1.1.*** Maintain a comprehensive inventory of all system users, processes, and devices as the foundation for access control and security management. ***1.2.*** Authenticate the identity of users, processes, and devices before granting access to organizational systems to ensure only authorized entities gain entry. ***1.3.*** Restrict system access exclusively to authorized users, processes, and approved devices, including interconnected systems, forming the cornerstone of access control. ***1.4.*** Enforce strict guidelines for password complexity and mandate periodic password changes to enhance security measures. ***1.5.*** Establish a comprehensive procedure for timely removal of access rights for departing or resigning personnel, ensuring security integrity ***1.6.*** Adhere to the principle of least privilege, granting users only specific security functions and privileged accounts necessary for their roles, minimizing the risk of unauthorized access and misuse of privileges. ***1.7.*** Enforce account timeout lockout after a few unsuccessful login IP bound. ***1.8.*** Implement multifactor authentication mechanisms for local and remote access.
2	***1.9.*** Immediately revoke access rights in response to malicious activity by an employee or contractor, preventing further unauthorized actions and limiting security breaches' impact. ***1.10.*** Mandate immediate password changes from temporary to permanent upon system login, ensuring password integrity and reducing the risk of unauthorized access. ***1.11.*** Disable inactive identifiers after a defined period to mitigate the risk of dormant accounts being exploited by unauthorized users, ensuring proactive security measures.
3	***1.12.*** Employ cryptographic protection for all stored and transmitted passwords, maintaining their unreadable state even if intercepted, thus enhancing security against unauthorized access attempts. ***1.13.*** Implement authentication feedback obscuration as an additional security measure, preventing potential attackers from inferring information about the authentication process and enhancing overall security posture. ***1.14.*** Regularly check logs / monitor for successful, failed and locked out important/admin accounts for detection of suspicious activities. ***1.15.*** Brake glass account – administrative backup account with highest privileges used in emergencies.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P1.01	
Establishment of Secure Transfer and Storage Procedures	• Identify confidential credentials such as passwords, cryptographic keys, and data stored in hardware tokens. • Enforce uniqueness for temporary/default passwords, mandating changes upon first use. • Store password hashes only, limiting retrieval mechanisms to secure environments like vaults or safes.
Secure Logging into Critical ICT Systems	• Adapt authentication methods to suit system nature and data sensitivity, conducting risk assessments. • Automatically log all remote access sessions, including those by employees and external technical personnel. • Implement encryption solutions like VPN, SSH, or similar technologies to safeguard data transmission. • Mandate multifactor authentication in ICT systems supporting critical processes for added security.
Effective Password Management Procedures	• Enforce a procedure for creating strong passwords and mandate changes in case of compromise or administrative need. • Implement password expiration policies to ensure regular updates and mitigate prolonged exposure risks. • Manage local administrative accounts to prevent unauthorized access and misuse. • Eliminate potential security vulnerabilities by managing built-in local administrative accounts in operating systems. • Utilize password managers or hardware-encrypted flash drives for systems not covered by directory services.
PRINCIPLE P1.02	
Regular Review of Access Logs for Privileged Accounts	• Conduct regular reviews of access logs for privileged accounts to identify and document abnormal behaviours. • Utilize proactive monitoring to detect and mitigate potential security breaches or unauthorized access attempts. • *Utilise alarms in case of non-regular use of a privileged account*
Implementation of Centralized Access Management Solution	• implement a centralized solution for managing and controlling access to critical systems and resources. • Enforce strong authentication, authorization, and auditing mechanisms for privileged accounts.
PRINCIPLE P1.03	
Establishment of Procedures for Granting User Authorizations	• Establish procedures for granting, amending, withdrawing, and registering user authorizations. • Maintain up-to-date documentation of user access rights and promptly revoke or update access privileges in response to changes.
Unique User Identifiers	• Assign unique identifiers to establish accountability and traceability in the ICT system.

	• Periodically check and delete or block unused identifiers, ensuring each identifier is assigned only once.
Authorization and Access Requests	• Authorize access to ICT systems only after approval of access requests. • Immediately revoke or update access when roles change, or users leave the organization.
PRINCIPLE P1.04	
Limiting Unsuccessful Logon Attempts	• Define the number of unsuccessful logon attempts based on system/application requirements. • Enhance security by limiting unsuccessful logon attempts to recommended values.
Identification and Limitation of Privileged Access	• Identify privileged access rights by system or process, limiting access to the necessary minimum for tasks performed. • Carefully control administrative rights to operating systems, databases, and applications.
Regular Review of Administrative Rights	• Quarterly review and verify administrative rights, ensuring proper access control. • Conduct reviews at least every 6 months, or more frequently if needed to align with organizational requirements.

2. INVENTORY CONTROL OF ASSETS (HARDWARE & SOFTWARE)

LEVEL	SECURITY MEASURES
1	***2.1.*** Compile comprehensive inventory of all organisation assets storing or processing data, including essential details like network address, hardware address, and approval status on a central location. ***2.2.*** Ensure inventory that covers assets connected physically, virtually, remotely, and within cloud environments, even if not directly controlled. ***2.3.*** Establish detailed inventory of all licensed software installed on organisation assets, documenting essential software information. ***2.4.*** Implement basic procedures to identify unauthorized software and take appropriate action.
2	***2.5.*** Initiate implementation of technical controls like application allowlisting to enforce execution of only authorized software. ***2.6.*** Strengthen documentation practices to include comprehensive details such as asset specifications, configuration information, and installed software. ***2.7.*** Integrate with existing IT management systems to enhance efficiency and accuracy in tracking and managing assets organization-wide. ***2.8.*** Define clear roles and responsibilities for maintaining the software inventory among personnel, ensuring accountability and consistency.
3	***2.9.*** Utilize active and passive discovery tools to identify assets connected to the network infrastructure, ensuring thorough coverage. ***2.10.*** Maintain a weekly process to detect and manage unauthorized assets within the network infrastructure. ***2.11.*** Implement automation and real-time monitoring mechanisms to streamline asset discovery, inventory updates, and status changes, ensuring efficiency and accuracy. ***2.12.*** Promptly take necessary actions upon identification of unauthorized assets, such as removal, denial of remote access, or quarantine, to mitigate potential risks effectively. ***2.13.*** Configure the active discovery tool to execute daily and regularly review and passive scans to update the asset inventory, ensuring its accuracy and completeness on a weekly basis.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P2.01	
Comprehensive Inventory Compilation	• Compile a comprehensive inventory of all organisation assets capable of storing or processing data. • Record essential details such as network address, hardware address, machine name, organisation asset owner, department, and approval status for network connectivity.
Documentation Strengthening	• Strengthen documentation practices to include comprehensive details such as asset specifications, configuration information, and installed software.

	• Integrate with existing IT management systems to enhance efficiency and accuracy in tracking and managing assets.
Weekly Detection and Management of Unauthorized Assets	• Maintain a weekly process to detect and manage unauthorized assets within the network infrastructure. • Promptly take necessary actions such as removal, denial of remote access, or quarantine to mitigate potential risks.
PRINCIPLE P2.02	
Deployment of Active and Passive Discovery Tools	• Employ active and passive discovery tools to identify assets connected to the network infrastructure. • Configure the active discovery tool to execute daily, while DHCP logging is reviewed and utilized to update the asset inventory weekly.
Regular Reviews for Asset Inventory Updates	• Conduct regular reviews of passive scans to update the asset inventory, ensuring accuracy and completeness. • Review passive scans at least weekly to maintain an up-to-date inventory of network assets.
PRINCIPLE P2.03	
Establishment of Comprehensive Software Inventory	• Initiate the process of establishing a comprehensive inventory of all licensed software installed across organisation assets. • Document essential information for each software entry, including title, publisher, initial install/use date, and business purpose.
Unauthorized Software Identification and Management	• Establish procedures to identify unauthorized software across the organization's assets. • Take appropriate action to address unauthorized software, conducting reviews monthly or more frequently if needed.
Implementation of Application Allowlisting	• Initiate the implementation of technical controls such as application allowlisting to enhance security. • Regularly review and update policies governing software library loading to accommodate changes in system requirements and security best practices.
Control of Software Library Loading	• Establish policies to specify approved libraries permitted to load into system processes. • Implement automated tools or scripts to expedite data collection and updates in the software inventory.
Role Definition and Maintenance	• Define roles and responsibilities for maintaining the software inventory among personnel. • Conduct regular maintenance and updates of software inventory tools to ensure optimal performance and data integrity.

3. SECURE CONFIGURATION & PATCH MANAGEMENT (ASSETS)

LEVEL	SECURITY MEASURES
1	***3.1.*** Utilize the built-in firewall capabilities of the server's operating system to restrict incoming and outgoing network traffic based on predefined rules, ensuring network security. ***3.2.*** Regularly review and update firewall rules to align with the organization's security policies and requirements, adapting to evolving threats and business needs. ***3.3.*** Enable logging for firewall activities and regularly monitor logs for any suspicious or unauthorized access attempts, facilitating timely detection and response to potential security breaches. ***3.4.*** Immediately change default passwords for accounts upon deployment to mitigate the risk of unauthorized access. ***3.5.*** Maintain documentation detailing default accounts and passwords, and ensure relevant personnel are aware of the importance of changing these defaults during deployment, enhancing security awareness and compliance. ***3.6.*** Disable default accounts not required for system operation or administrative tasks to prevent potential misuse or exploitation, bolstering account security.
2	***3.7.*** Deploy a firewall solution to provide advanced network security features such as application-level filtering and intrusion detection, enhancing overall network protection. ***3.8.*** Implement network segmentation using the firewall to divide the server environment into separate zones based on trust levels, containing, and mitigating the impact of security breaches. ***3.9.*** Implement Role-based Access Control (RBAC): Assign privileges and access rights based on job roles to limit access to critical functions and data, enhancing security and minimizing the risk of unauthorized access.
3	***3.10.*** Install and configure a third-party firewall agent on each server to strengthen security by adding extra protection layers beyond the default operating system firewall. ***3.11.*** Implement continuous compliance monitoring to ensure firewall configurations remain in line with industry standards and regulatory requirements, maintaining adherence to security best practices. ***3.12.*** Implement solutions to detect any unauthorized attempts to access default accounts or changes made to default account configurations in real-time, enabling swift response to potential security incidents.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P3.01	
Built-in Firewall Utilization	• Utilize the built-in firewall capabilities of the server's operating system (e.g., Windows Firewall, iptables) to regulate incoming and outgoing network traffic based on predefined rules. • Implement rules to control access to specific ports and protocols, minimizing the attack surface and enhancing network security.
Regular Review and Update	• Regularly review and update firewall rules to ensure alignment with the organization's security policies and requirements. • Conduct periodic audits to identify and remove unnecessary or outdated rules, optimizing firewall performance and effectiveness.
Logging and Monitoring	• Enable logging for firewall activities and establish processes for regularly monitoring logs to detect any suspicious or unauthorized access attempts. • Implement alerting mechanisms to notify security personnel of potential security incidents or policy violations in real-time.
PRINCIPLE P3.02	
Measures for securing accounts	• Implement measures such as strong password policies, multi-factor authentication (MFA), and account lockout mechanisms to secure accounts against unauthorized access, reducing the risk of credential-based attacks. • Immediately change default passwords for accounts such as 'root', 'administrator', or any other pre-configured vendor accounts upon deployment of the asset or software. • Utilize strong and unique passwords to prevent unauthorized access and potential exploitation of default account credentials.
Documentation and Awareness	• Maintain comprehensive documentation detailing default accounts and their passwords, ensuring that relevant personnel are aware of the importance of changing these defaults during deployment. • Provide training and awareness sessions to educate administrators and users about the risks associated with default accounts and the importance of password hygiene.
Regular Auditing and Enforcement	• Conduct regular audits to identify any instances where default accounts have not been changed and take corrective actions promptly. • Implement automated enforcement mechanisms to ensure compliance with password change policies and mitigate the risk of unauthorized access.
PRINCIPLE P3.03	
Advanced Network Security Features	• Deploy firewall solutions to provide advanced network security features, including application-level filtering, intrusion detection, and VPN support. • Leverage these features to enhance the organization's overall security posture and protect against evolving cyber threats.

Network Segmentation	• Implement network segmentation using the firewall to divide the server environment into separate zones based on trust levels (e.g., DMZ, internal network). • Isolate critical infrastructure components from less secure areas to contain and mitigate the impact of security breaches and unauthorized access attempts.
Integration with Security Automation	• Integrate the firewall with security automation tools to automate responses to detected threats, such as blocking malicious IP addresses or triggering alerts for further investigation. • Streamline incident response processes and enhance the organization's ability to detect and mitigate security incidents in real-time.

4. VULNERABILITY MANAGEMENT & PENETRATION TESTING

LEVEL	SECURITY MEASURES
1	***4.1.*** Establish vulnerability management process in place of assets. ***4.2.*** Periodical assessment of the organizational systems to determine if the security controls are effective in their application. ***4.3.*** Penetration testing program integrated into the broader incident response framework. - Regular penetration testing is required, a least once in two years, or after significant changes or introduction of new systems. ***4.4.*** Establish patch management process.
2	***4.5.*** Processes and tools in place to remediate detected vulnerabilities in software monthly, following established remediation procedures based on vulnerability severity level. ***4.6.*** Scans for vulnerabilities in organizational ICT systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
3	***4.7.*** Employ a separate penetration testing team (red team) to perform penetration testing on the system or system components. ***4.8.*** Automate vulnerability scans on quarterly basis of externally exposed assets using a vulnerability scanning tools. ***4.9.*** Employ a penetration testing process that covers attempts to bypass or circumvent controls associated with physical access points to the facility.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P4.01	
Monitor and obtain information on technical vulnerabilities of the ICT systems used on an ongoing basis and assess the organization's exposure to them, as well as take appropriate measures to counteract the related risk(s)	• A register of identified ICT resources supporting critical services is a prerequisite for vulnerability management. • Critical updates and fixes (after confirming that they are free of bugs) should be introduced immediately after their publication, especially regarding the elimination of 0-day vulnerabilities. • Applications should be used in the latest version possible and updated regularly. This applies in particular to, e.g., web browsers, Microsoft Office software, and PDF readers. From the moment of their publication (and confirmation that they are error-free), the patch/correction/update of applications responsible for supporting critical processes carried out by the operator should be installed without undue delay. • Operating systems should be used in an up-to-date, version and kept up-to-date along with network devices. It is not recommended to use versions that are no longer supported. From the moment of their publication (and confirmation that they are error-free), the patch/correction/update of operating systems responsible for supporting critical processes carried out by the operator should be installed without undue delay.
Managing technical	• software provider data, • version number,

vulnerabilities requires specific information, such as:	• on which system the software is installed, • the duration of technical support and licenses of the software manufacturer. • Information on vulnerabilities and threats can be obtained from computer incident response teams, e.g., MKD-CIRT and Government CIRT.
PRINCIPLE P4.02	
Regular –biennial Penetration Testing Schedule and Compliance	• Set a consistent schedule for conducting annual penetration testing from external independent company. • Align the schedule with organizational goals, compliance requirements, and industry best practices. • Create remediation procedures for the detected vulnerabilities.
Monitor Compliance	• Implement mechanisms for monitoring compliance with the annual penetration testing schedule. • Use automated reminders, progress tracking tools, or periodic reviews by security governance bodies. • Regularly assess adherence to the schedule and take corrective actions as needed to ensure timely and planned penetration testing activities.
PRINCIPLE P4.03	
Establish a structured and documented approach to identify, assess, prioritize, and mitigate vulnerabilities across all assets within the organization's infrastructure	• Develop a comprehensive framework outlining the steps involved in vulnerability management, including identification, assessment, prioritization, and mitigation. Ensure that this framework is well-documented and easily accessible to relevant personnel. • Schedule routine vulnerability assessments using both automated scanning tools and manual methods. Ensure that these assessments cover all assets within the organization's infrastructure and are conducted regularly to identify new vulnerabilities and changes in the risk landscape.
Develop a clear procedure outlining the vulnerability management process for assets	• Create a detailed procedure document that outlines the organization's approach to vulnerability management, including roles and responsibilities, assessment procedures, prioritization criteria, and mitigation strategies. Ensure that this policy is reviewed regularly and updated as needed to reflect changes in technology or business requirements. • Once the policy is finalized, communicate it effectively to all relevant stakeholders within the organization. Provide training and resources to ensure that employees understand their roles and responsibilities in the vulnerability management process and are aware of the importance of adhering to the policy guidelines.
PRINCIPLE P4.04	
Classify assets, apply tailored access controls, automate vulnerability scans for comprehensive risk mitigation	• Evaluate each asset within the organization's infrastructure to determine its criticality and importance. Classify assets into different categories based on factors such as their value, sensitivity, and impact on organizational objectives. • Once assets are classified, implement access controls and security measures tailored to their respective classifications. Restrict access to critical assets to authorized personnel only and enforce stricter security measures to protect sensitive or high-value assets from unauthorized access or manipulation.
Implement automated vulnerability	• Select and deploy automated vulnerability scanning tools capable of scanning and identifying vulnerabilities across all assets within the organization's

scanning tools to continuously monitor assets for vulnerabilities	infrastructure. Configure these tools to run regular scans and generate reports detailing identified vulnerabilities and associated risks. • Integrate Scanning Tools with Asset Inventory: Integrate vulnerability scanning tools with the organization's asset inventory system to ensure comprehensive coverage and visibility. Automatically update asset inventory records based on scan results, allowing for accurate tracking of vulnerabilities and their associated assets.
Schedule regular scans to ensure comprehensive coverage	• Define a regular schedule for vulnerability scans based on the organization's risk profile, operational requirements, and compliance obligations. Ensure that scans are conducted frequently enough to provide timely insights into the organization's vulnerability posture without causing undue disruption to business operations. • In addition to regular scans, perform ad-hoc scans in response to significant changes in the organization's infrastructure, such as system updates, new deployments, or security incidents. These targeted scans help ensure that vulnerabilities are promptly identified and addressed as they arise.
PRINCIPLE P4.05	
Conduct regular risk assessments to evaluate the potential impact of identified vulnerabilities	• Assess the potential impact of identified vulnerabilities on the organization's assets, systems, and operations. Use risk assessment methodologies and tools to analyse the likelihood and severity of exploitation, considering factors such as asset criticality, attack vectors, and existing security controls. • Prioritize vulnerabilities for remediation based on their risk scores, focusing on those with the highest likelihood and potential impact of exploitation. Allocate resources and attention to addressing critical vulnerabilities first, followed by those with lower risk levels, to maximize the effectiveness of mitigation efforts.
Prioritize vulnerabilities based on severity and potential impact	• Define a set of criteria for assessing the severity of vulnerabilities, taking into account factors such as exploitability, impact, and affected assets. Develop a scoring system or scale to rank vulnerabilities based on their severity levels, ranging from low to critical.
PRINCIPLE P4.06	
Establish procedures for promptly applying security patches and updates to mitigate identified vulnerabilities	• Create documented procedures for identifying, testing, and deploying security patches and updates across the organization's infrastructure. Define roles and responsibilities for each step of the patch management process, ensuring clear accountability and coordination.
Develop a process for testing patches before deployment to minimize disruptions	• Create a dedicated testing environment where patches can be safely deployed and evaluated before being rolled out to production systems. Mimic the organization's production environment as closely as possible to ensure that testing results accurately reflect real-world conditions. • Test patches for compatibility with existing systems, applications, and configurations to identify any potential conflicts or issues that could arise post-deployment. Perform regression testing to verify that the patches do not introduce any new vulnerabilities or unintended consequences.
Define procedures for responding to and remediating	• Define escalation procedures for critical vulnerabilities requiring immediate attention or remediation. Establish criteria for escalating vulnerabilities to senior

critical vulnerabilities	management or executive leadership for prioritized action and resource allocation. • Establish emergency patching protocols for critical vulnerabilities posing an imminent threat to the organization's security or operations. Develop procedures for expedited patch testing, approval, and deployment to minimize the window of exposure and reduce the risk of exploitation.
Generate regular reports on the organization's vulnerability posture and remediation progress	• Generate regular reports summarizing the organization's vulnerability posture, including the number of identified vulnerabilities, their severity levels, and the status of remediation efforts. Customize reports to meet the needs of different stakeholders, providing relevant insights and metrics to support decision-making and prioritization. • Distribute vulnerability management reports to relevant stakeholders within the organization, including executive leadership, IT management, and security teams. Schedule regular meetings or presentations to discuss report findings, address concerns, and track progress towards vulnerability remediation goals.

5. AUDIT LOGGING & MANAGEMENT

LEVEL	SECURITY MEASURES
1	***5.1*** Identify the types of events that the system is capable of logging in support of the audit function. ***5.2*** Define the process for managing audit logs, including requirements for collection, review, and retention of logs for assets that will enable monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. ***5.3*** Actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. ***5.4*** Regular review and update the event types selected for logging.
2	***5.5*** Constant review of the relevant logged events. ***5.6*** System capability to compare and synchronize internal system clocks with an authoritative source to generate time stamps for audit records. ***5.7*** Protect audit information and audit logging tools from unauthorized access, modification, and deletion. ***5.8*** Incorporate tools for automated collection and analysis of monitoring data and logs. ***5.9*** Collect service provider logs, where supported, including events such as authentication and authorization, data creation and disposal, and user management.
3	***5.10*** Audit logs consistently collected across all assets. ***5.11*** Limit management of audit logging functionality to a subset of privileged users. ***5.12*** Defined alert and response to audit logging process failures.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P5.01	
Identify the Types of Events That the System Can Log	• Compile a list of all events currently logged by the system (e.g., access logs, configuration changes, security alerts). • Compare existing logs with industry standards and regulatory requirements to identify missing logs. • Adjust system settings or integrate new tools to capture required events • Test the updated system to confirm it logs new events accurately • When needed review logging capabilities to adapt to new threats and regulatory changes.
PRINCIPLE P5.02	
Audit logs and records should meet the following requirements	• An event logging system in networks and ICT systems should be implemented. • Procedures for archiving the collected logs should be developed for a period of at least 12 months and in line with GDPR and/or organisational requirements.
The event log should contain a set of minimum	• A unique user ID, • date, time and details of key events, e.g., timestamps of system events including successful and failed login attempts, • changes in system configuration,

information including:	• use of privileges, • changes to privileges, • use of selected system tools and applications, • network addresses, • alarms raised by the access control system, • activation and deactivation of protection systems, e.g., anti-virus software.
System administrators should not be authorised to delete modify or deactivate audit logs	• those which contain records of their own activities, or key system events • for systems where this is impossible, a mechanism for copying to an external repository such as audit log servers or SIEM systems should be provided • Where modifications of logs are made (for example to remove PII or other data in line with GDPR or other legislative requirements) this activity must also be fully auditable, with records and events captured and such activity should be underpinned by a formal organisational policy and approval process.
Where proportionate, and deemed necessary, the organization should extend the scope of logged events.	• Expanding logged events enhances security monitoring, ensures compliance, improves risk management, aids incident response, facilitates forensic analysis, and enables performance evaluation.
PRINCIPLE P5.03	
Establish a periodic review and analysis process of audit logs and records to identify trends, anomalies, or potential security incidents.	• Developing a schedule for regular log review and assigning responsibility to specific personnel. • Establishing criteria for identifying suspicious or unusual activity within the logs. • Implementing automated tools or processes to assist in log analysis and identification of potential issues.
PRINCIPLE P5.04	
SIEM tools or equivalent systems can be used to store, correlate, normalise and analyse log information and to generate alerts.	• Have a clear understanding of data schemes, data asset libraries and data and other log sources • Consider A/B testing for baselining and tuning rules and alerts. • Avoid “hard coded” rules where possible. • Document use cases and KPIs for evaluation an efficacy. • Ensure any tooling and alerting protect the confidentiality, integrity and availability of stored logs. • Ensure the appropriate storage, retention and alerting policies are in place and defined. • Ensure that all relevant staff have the appropriate training and that training levels are maintained.
PRINCIPLE P5.05	
Ensure accuracy of time sources and avoid clock skew	• Configure at least two synchronized time sources across organisation assets • Where possible, consider utilizing well established sources (e.g. time servers of pool.ntp.org)

6. EMAIL & BROWSER PROTECTIONS

LEVEL	SECURITY MEASURES
1	***6.1.*** Establish a policy mandating the use of only fully supported browsers and email clients within the organisation, ensuring compatibility and security. ***6.2.*** Implement DNS filtering services on all organisation assets to block access to known malicious domains, enhancing overall network security. ***6.3.*** Conduct an inventory of all browser and email client plugins, extensions, and add-on applications installed across organisation assets, identifying potential security vulnerabilities. ***6.4.*** Configure basic rules on the email gateway to block inbound emails containing file attachments with specified file extensions, reducing the likelihood of malware infiltration through email channels.
2	***6.5.*** Use group policies or configuration management tools to enforce compliance with the policy, ensuring consistent application across all devices and users. ***6.6.*** Establish clear policies and guidelines regarding the installation and usage of browser and email client plugins, extensions, and add-on applications, minimizing the risk of introducing vulnerabilities or unauthorized software.
3	***6.7.*** Implement controls to prevent the execution of unsupported browsers and email clients within the organisation network, reducing security risks associated with outdated or vulnerable software. ***6.8.*** Use group policies or configuration management tools to enforce compliance with the policy, ensuring consistent application across all devices and users. ***6.9.*** Customize DNS filtering rules based on the specific needs and risk profile of the organization, optimizing protection against malicious domains and threats. ***6.10.*** Enhance email server anti-malware protections with advanced detection techniques, such as heuristic analysis and behaviour monitoring, improving the detection and mitigation of sophisticated malware threats.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P6.01	
Formulate Clear Guidelines	• Define which browsers and email clients are considered fully supported based on compatibility and security standards. • Specify criteria for determining supported software, considering factors like vendor support and vulnerability patching.
Scope Specification	• Clearly outline the policy's applicability to all employees, contractors, and third-party vendors accessing organisation systems. • Ensure that the policy covers both company-owned and personally owned devices used for work purposes.

Consequences of Non-Compliance	• Clearly communicate the repercussions of non-compliance with the policy, such as restricted access to organisation resources or disciplinary action. • Ensure that consequences are enforced consistently across all levels of the organization.
Regular Review Procedures	• Establish procedures for regularly reviewing and updating the list of supported browsers and email clients. • Define roles and responsibilities for conducting reviews, including IT personnel responsible for monitoring vendor support updates and security advisories.
PRINCIPLE P6.02	
Communication of Requirements	• Clearly communicate the requirement for using the latest versions of supported browsers and email clients to all stakeholders. • Provide ongoing reminders and updates to ensure awareness and compliance.
Guidance on Updates	• Provide detailed guidance on how users can check for and install updates, including instructions for configuring automatic updates where available. • Offer training sessions or resources to assist users in updating their software effectively.
Monitoring Compliance	• Implement mechanisms for monitoring compliance, such as automated scans for outdated software versions or regular audits of installed applications. • Establish thresholds for acceptable compliance levels and define escalation procedures for addressing non-compliance issues.
Handling Exceptions	• Establish procedures for handling exceptions, such as legacy applications that require specific browser or email client versions. • Define criteria for granting exceptions and ensure that risks associated with legacy applications are adequately mitigated through alternative controls.
PRINCIPLE P6.03	
Evaluation of Filtering Solutions	• Conduct a thorough evaluation of DNS filtering solutions, considering factors such as threat intelligence feeds, customizable filtering policies, and ease of integration. • Involve stakeholders from IT, security, and operations teams in the evaluation process to ensure alignment with organizational needs.
Integration and Configuration	• Integrate DNS filtering into the organization's network infrastructure and configure filtering policies to block access to categories of websites known to host malware, phishing content, or other malicious activity. • Test configurations in a controlled environment before full deployment to ensure compatibility and effectiveness.
Monitoring and Investigation	• Implement monitoring processes to track DNS traffic for signs of suspicious or unauthorized access attempts.

	• Establish procedures for investigating anomalies and responding to potential security incidents identified through DNS filtering alerts.
PRINCIPLE P6.04	
Development of Educational Materials	• Develop educational materials, such as training modules, presentations, or informational videos, that explain the purpose and benefits of DNS filtering in plain language. • Tailor educational materials to different user groups, providing relevant examples and scenarios that resonate with their roles and responsibilities.
PRINCIPLE P6.05	
Comprehensive Inventory	• Utilize automated inventory tools or scripts to perform a comprehensive inventory of all browser and email client plugins, extensions, and add-on applications installed across organisation assets. • Document essential details for each plugin, including name, version, vendor, installation date, and permissions/access levels.
Necessity Assessment	• Develop criteria or guidelines for assessing the necessity and authorization status of plugins and add-ons, considering factors such as business function, security impact, and compliance requirements. • Review each plugin against the established criteria to determine whether it aligns with organizational needs and contributes to productivity without compromising security.
Authorization Procedures	• Obtain appropriate approvals or authorizations from relevant stakeholders, such as IT administrators, department heads, or security officers, for installing or retaining authorized plugins and add-ons. • Document the rationale behind decisions to authorize or deny specific plugins and add-ons, ensuring transparency and accountability in the authorization process.
PRINCIPLE P6.06	
Identification and Removal Procedures	• Develop procedures or workflows for systematically identifying unauthorized or unnecessary plugins and add-ons based on the results of the inventory and assessment process. • Implement automated or manual methods for removing unauthorized plugins and add-ons from endpoint devices, email clients, and web browsers
Communication with Users	• Communicate with affected users to explain the reasons for plugin removal and provide guidance on alternative solutions or approved alternatives. • Offer training or support resources to help users transition to approved plugins and add-ons seamlessly.
PRINCIPLE P6.07	
Identification of Threats:	• Identify common file types associated with malware, ransomware, or other security threats that may be transmitted via email attachments.

	• Use threat intelligence feeds and security advisories to stay updated on emerging threats and file-based attack vectors.
Configuration of Gateway Rules:	• Configure email gateway rules to automatically reject or quarantine inbound emails containing file attachments matching the specified file extensions associated with known threats. • Regularly review and update the list of blocked file extensions based on emerging threats, industry trends, and security intelligence sources.

7. MALWARE DEFENCE (& ANALYSIS)

LEVEL	SECURITY MEASURES
1	***7.1.*** Choose a reputable anti-malware solution suitable for the organization's needs, considering factors such as compatibility, effectiveness, and ease of management. ***7.2.*** Deploy the chosen anti-malware software on all organisation assets to ensure comprehensive coverage across various devices. ***7.3.*** Enable automatic updates for the anti-malware software to keep it current with the latest threat definitions and security patches, ensuring optimal protection against evolving threats. ***7.4.*** Establish a policy mandating the automatic update of anti-malware signature files on all organisation assets, ensuring consistency and adherence to security best practices.
2	***7.5.*** Regularly verify that automatic updates are enabled and functioning correctly on all assets to maintain the effectiveness of the anti-malware solution. ***7.6.*** Configure regular and scheduled malware scans on all assets to proactively detect and remove any malicious software or potential threats, enhancing overall security posture. ***7.7.*** Develop and implement Change Management process.
3	***7.8.*** Implement centralized management capabilities for the anti-malware solution to streamline deployment, configuration, and monitoring across all organisation assets, ensuring consistency and efficiency in managing security measures. ***7.9.*** Enable real-time protection features of the anti-malware software to actively monitor and block malicious activities in real-time, providing immediate defence against emerging threats. ***7.10.*** Schedule updates during off-peak hours to minimize disruption to end-users while ensuring timely protection against emerging threats, maintaining security without disrupting productivity. ***7.11.*** Integrate the anti-malware solution with Security Information and Event Management (SIEM) systems or Security Orchestration, Automation, and Response (SOAR) platforms for enhanced threat detection and response capabilities, enabling efficient handling of security incidents. ***7.12.*** Implement advanced malware detection techniques, such as behavioural analysis and sandboxing, to identify and mitigate zero-day threats and sophisticated malware variants, enhancing the ability to detect and respond to emerging threats.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P7.01	
Reputation and Suitability	• Select a reputable anti-malware solution tailored to the organization's requirements, considering factors such as compatibility, effectiveness against known threats, and ease of management. • Prioritize solutions with a proven track record in addressing malware threats relevant to the organization's industry and operating environment.
Scalability and Flexibility	• Choose a solution capable of scaling with the organization's growth and adaptable to evolving security needs, including support for diverse endpoints and network environments. • Evaluate solutions that offer flexibility in deployment options, such as cloud-based, on-premises, or hybrid deployments, to align with the organization's infrastructure preferences.
PRINCIPLE P7.02	
Universal Coverage	• Ensure comprehensive coverage by deploying the chosen anti-malware software across all organisation assets, including desktops, laptops, servers, mobile devices, and any other relevant endpoints. • Implement deployment procedures that account for different operating systems and device types to maintain consistency and effectiveness across the organization's ecosystem.
Thorough Implementation	• Adhere to standardized deployment practices to ensure uniformity and completeness in the installation process, minimizing the risk of gaps or oversights in protection coverage. • Verify successful deployment on each asset and conduct validation checks to confirm proper functioning and integration with existing security infrastructure.
PRINCIPLE P7.03	
Automatic Updates	• Enable automatic updates for the anti-malware software to ensure timely delivery of the latest threat definitions, security patches, and software enhancements. • Implement mechanisms to automate the update process across all organisation assets, reducing reliance on manual intervention and minimizing update-related vulnerabilities.
Policy Enforcement	• Establish and enforce policies mandating the automatic update of anti-malware signature files on all organisation assets, ensuring consistent adherence to security best practices. • Regularly review and refine update policies to accommodate changes in threat landscapes, technology advancements, and organizational requirements.
PRINCIPLE P7.04	
Policy Development	• Develop and document policies mandating the disablement of autorun and autoplay functionality for all removable media on organisation assets to mitigate the risk of malware propagation. • Clearly communicate policy guidelines to end-users through training sessions, awareness campaigns, and written materials to promote understanding and compliance.

8. NETWORK INFRASTRUCTURE MANAGEMENT

Level	Security measures
1	***8.1*** Physical access to equipment and monitored to detect potential cybersecurity events. ***8.2*** Special admin computers are kept apart from the main network, without access the internet. ***8.3*** Only authorized and certified personnel should carry out repairs and service equipment. ***8.4*** Maintain up-to-date inventory of network devices, including hardware and software configurations, firmware versions, and network topology diagrams.
2	***8.5*** Maintain and update architecture diagrams and network system documentation, especially after significant changes. ***8.6*** Implement network segmentation controls, such as firewalls, VLANs (Virtual Local Area Networks), and access control lists (ACLs), to isolate and segregate network traffic between different zones. ***8.7*** Segment the network into distinct zones or segments based on trust levels, business functions, and security requirements. ***8.8*** Use of strategies like segmentation, limiting access, and ensuring the network it's always running ***8.9*** Apply the principle of least privilege to restrict communication between network segments, minimizing the impact of security incidents and limiting lateral movement by attackers.) ***8.10*** Details of internal network and system configuration, employee or device related directory services and other sensitive technology are not publicly disclosed or enumerable by unauthorized personnel.
3	***8.11*** Implement change management controls to review, approve, and track changes to network configurations, ensuring that only authorized and documented changes are implemented.

To implement these security measures, the principles should be considered but not limited to:

Principle P8.01	
Ensure physical security measures are in place to detect and respond to potential cybersecurity threats	• Equip critical areas with CCTV cameras to monitor and record activities around sensitive or critical infrastructure. • Use card readers, biometric scanners, and secure badges to control access to sensitive locations, ensuring only authorized personnel can enter. • Implement strict policies and procedures for managing visitors, including escorts in secure areas and logging all entry and exits. • Conduct regular physical security checks to identify and rectify potential vulnerabilities such as unsecured entry points or outdated camera systems. • Ensure physical security logs (e.g., access logs, video footage) are reviewed in conjunction with cybersecurity systems to detect correlated events. • Regularly train security personnel on recognizing security threats and conducting emergency response drills to improve preparedness for physical security breaches.

	• Incorporate physical security breach protocols into the broader cybersecurity incident response plan, ensuring a coordinated response to incidents that span both domains.
Principle P8.02	
Segregate Admin / Control Systems	• Where possible designate computers and/or control systems for administrative tasks that have the appropriate boundaries with the main network to prevent cross-contamination. • Ensure these admin computers do not have Internet access to mitigate the risk of external threats or, if that is not possible, limit such connectivity as much as reasonably possible. • Apply the highest security settings, including the use of firewalls and restricted user permissions. • Conduct yearly audits to ensure compliance with the isolation policies and verify no unauthorized connections have been established.
Principle P8.03	

Adoption and implementation of protective measures to the management networks	• dedicated networks are used for management devices, i.e. implement a separate management VLAN, or physically separate infrastructure,
	• secure channels e.g., by using VPNs, SSH, etc.
	• Networks are designed and configured to limit opportunities of unauthorized access to information transiting the network infrastructure. Organizations **SHOULD** use as many of the following technologies to meet this requirement:
	  ○ port security on switches to limit access and disable all unused ports.
	  ○ routers and firewalls segregating parts of the network on a need-to-know basis.
	  ○ IPSEC/IP Version 6
	  ○ application-level encryption
	  ○ network edge authentication.
	  ○ Restrict and manage end-user devices communicating to organization network through various filtering techniques
	  ○ IPS/IDS to detect/prevent malicious activity within the network.
	• Ensure network infrastructure is kept up to date. Example implementations include running the latest stable release of software. Review software versions monthly, or more frequently, to verify software support.
	• Establish and maintain a secure network architecture which must address segmentation, least privilege, and availability, at a minimum.
	• Review and update documentation annually, or when significant organisation changes occur that could impact this Safeguard.
	• Ensure documentation of the network is appropriately isolated and backed up in line with your disaster recovery and business continuity plans.
	• Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the organisation's primary network and not be allowed internet access.
	• Trunking/port mirroring MUST NOT be used on switches managing VLANs of differing classifications (e.g. enter national classification types here)

Principle P8.04	
Adoption and implementation of protective measures to the management networks	• Ensure secure network segmentation and access control mechanisms to protect sensitive assets and minimize the impact of security incidents. • Divide the network into distinct zones or segments based on trust levels, business functions, and security requirements. • Classify assets and resources based on their sensitivity and access requirements. • Apply the principle of least privilege to restrict communication between network segments, ensuring that only necessary connections are allowed. • Use firewall rules, VLANs, and access control lists (ACLs) to enforce communication restrictions and limit lateral movement by potential attackers. • Implement change management controls to review, approve, and track changes to network configurations. • Maintain an up-to-date inventory of network devices and configurations to facilitate change management processes. • Ensure that details of internal network and system configurations, as well as employee or device-related directory services, are not publicly disclosed or enumerable by unauthorized personnel. • Implement measures such as network hardening, encryption, and access controls to protect sensitive information from unauthorized access or disclosure.

9. NETWORK MONITORING & DEFENCE

Level	Security measures
1	***9.1*** Regular review and analyse of security logs, network traffic patterns, and system activity to identify indicators of compromise (IOCs) and potential security breaches. ***9.2*** Implement host-based intrusion prevention solutions.
2	***9.3*** Prevent unauthorized and unintended information transfer via shared system resources. ***9.4*** Ensure remote devices utilize a VPN when connecting to the core infrastructure. ***9.5*** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
3	***9.6*** Implement advanced Security Information and Event Management (SIEM) systems and incident response. ***9.7*** Establish and manage cryptographic keys for cryptography used in organizational ICT systems. ***9.8*** Traffic filtering between different parts of the network. ***9.9*** Deploy network intrusion prevention solutions and port-level access control, including any specific technologies or protocols. ***9.10*** Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunnelling). ***9.11*** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. ***9.12*** Prohibit remote activation of collaborative computing devices (networked whiteboards, cameras, and microphones) and provides the information to the users when the device is enabled. Protection of the authenticity of communications sessions. ***9.13*** Protect web application(s) against cyber threats that are inherent in web technologies.

To implement these security measures, the principles should be considered but not limited to:

Principle P9.01	
Continuously monitor and analyse security logs, network traffic, and system activities to detect indicators of compromise (IOCs) and prevent security breaches.	• Establish a routine (e.g., continuously, hourly, daily, weekly, monthly) for reviewing security logs, network traffic, and system activity. Tailor the frequency based on the sensitivity of the information and system criticality. • Create guidelines and checklists for identifying abnormal activities and potential IOCs such as unusual outbound traffic, spikes in data access, or unauthorized access attempts. • Document clear process maps for triage and escalation, including runbooks for when adverse events are identified. • Periodically simulate security incidents to test the effectiveness of your monitoring and analysis protocols and adjust them based on findings.

Principle P9.02	
Oversee and manage the networks	• The appropriate solutions must be introduced (e.g., firewall, VLAN type), allowing for filtering and separation of traffic to ICT systems responsible for supporting critical processes carried out by the operator. • Direct access to the Internet from ICT systems responsible for supporting critical processes carried out by the operator should be prevented and where it is allowed, the rationale and approach should be documented as part of internal policies. • Web content should be filtered - access to malicious domains and IP addresses, advertisements and anonymous networks should be registered, monitored and blocked. Where approved appropriate “good/allowed lists” should be created and regularly reviewed. • By default, any unnecessary and unauthorized (incoming or outgoing) network traffic **must** be blocked (e.g., using IPS/IDS solutions and application firewalls), including those generated by untrusted applications. • Utilise only trusted DNS servers, and detailed filtering of DNS queries should be carried out. • Network traffic to and from the computers where vital data is stored or those which are responsible for supporting critical processes performed by the operator and/or traffic crossing the perimeter of the organization's network, should be captured and remain auditable for incident detection and analysis. • The "port security" functions should be used on network switches. • Disable unused services that are not required/necessary for work on a given workstation, e.g., RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR, WPAD and protocols e.g., DHCP, IPv6, IPX, etc
Principle P9.03	
Separate the information service networks, users and information systems	• Division into separated network domains is one method of supervising the security of large networks. Separation can be done physically or logically. Regardless of the distribution method, the boundaries of each domain and the access requirements for each domain must be clearly defined. • Cross-domain access is possible but controlling it with devices such as a firewall or filtering router is recommended. Attempts to connect other than defined should be monitored and analysed; • Restrict low-trust devices (e.g., IoT and BYOD devices) and restrict network access to drives and data repositories based on function, and where these are allowed, the rationale and approach should be documented as part of internal policies. • Network Layer L3 (OSI model) switches are used to separate LAN into VLANs. A Layer 3 switch can perform inter-VLAN routing at wire speed with predictable performance, but it may not provide the same level of security and policy control as a Next-Generation Firewall (NGFW).

Principle P9.04	

Implement a Demilitarized Zone (DMZ) Network for Enhanced Organizational Security	• The organisation should create a DMZ (demilitarized zone) as a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.
	• A Demilitarized zone network allows an organization to access untrusted networks, such as the Internet, while ensuring its private network or LAN remains secure.
	• Where possible, organisations should store at least the following in the DMZ:
	  ○ external-facing services and resources,
	  ○ servers for the Domain Name System (DNS),
	  ○ File Transfer Protocol (FTP),
	  ○ e-mail,
	  ○ proxy,
	  ○ and web servers.
	• These servers and resources should be isolated and given limited access to the LAN to ensure they can be accessed via the internet, but the internal LAN cannot.

Principle P9.05	
Implement a comprehensive and layered security approach for API protection	• Use HTTPS protocol instead of HTTP for secure communication. HTTPS encrypts the data in transit between the client and server, preventing eavesdropping and tampering with the data. • Implement a secure authentication and authorization mechanism to ensure only authorised users can access the API. Consider using tokens, OAuth2 protocol, or API keys. • Validate all user input to prevent any malicious activity via API access. • Validate all input data to prevent injection attacks such as SQL injection or Cross-Site Scripting (XSS) attacks. • Implement rate-limiting to prevent DoS attacks by limiting the number of requests a user can make in a given time period. This might be done by configuring the network devices. • Keep logs of all requests and responses to the API and monitor them for any suspicious activity. • Use the latest security standards: Ensure that the API is using the latest security standards and protocols, such as TLS 1.2 or higher, and avoid using deprecated or weak cryptographic algorithms. • Conduct regular security tests and audits to identify any vulnerabilities or weaknesses in the API and promptly address them.
Principle P9.06	

Apply defence in depth for WebApps	• Develop web applications with security best practices in mind.
	  ○ Secure Execution Platforms:
	  ○ Deploy applications on trusted application servers (e.g. Apache, Glassfish, WebSphere, and WebLogic)
	  ○ Ensure platforms are consistently updated and patched.
	• Regular Security Assessments:
	  ○ Conduct penetration testing to uncover new vulnerabilities.
	  ○ Include security reviews as part of the development lifecycle.
	  ○ Follow appropriate and established guidance (eg OWASP top 10)
	• Implement WAFs to provide an additional security layer.

10. SECURITY AWARENESS AND SKILLS TRAINING

LEVEL	SECURITY MEASURES
1	*10.1.* Establish and maintain cyber security awareness program. *10.2.* Ensure personnel are made conscious of the applicable security standards, policies, and procedures and associated security risks related to their activities within the system. *10.3.* Ensure personnel are being regularly trained to perform their role-specific cybersecurity duties and responsibilities in line with relevant legislation, policies and procedures.
2	*10.4.* Provide security awareness training on recognizing and reporting potential indicators of insider threat.
3	*10.5.* Conduct a campaign to promote and raise cyber security awareness among relevant contractors, clients and third-party stakeholders.

To implement these security measures, the principles should be considered but not limited to:

Principle P10.01	
Overall cybersecurity awareness program	• A cyber security awareness program should be tailor-defined along with adequate budgets allocated for its implementation. • Develop and document awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Develop and document procedure to facilitate the implementation of the awareness and training policy. • Include several awareness-raising activities via appropriate physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules, intranet and e-mails. • Review and update the awareness and training program once a year. • The organization' management should have a cybersecurity awareness program extended according to the position held (e.g., supervision of employees, specific roles and responsibilities, etc.). • Frequently send topical messages and notifications about security to the employees, for example: strong password-use that coincides with a media report of password dump, the rise of phishing during tax time, or increased awareness of malicious package delivery emails during the holidays.
PRINCIPLE P10.02	
Overall cybersecurity training program	• All personnel of the government organization and, where relevant, contractors, clients and third-party users or stakeholders should receive appropriate security awareness training regarding the organization's policies and procedures, relevant for their job function, roles, responsibilities and skills. • Prepare an annual plan for the implementation of the cyber security trainings. • Plan and implement an initial awareness training program for each new employee or in each case of employee' transfer from another organization. • Identify appropriate trainings for technical teams whose roles require specific skill sets and expertise.

	• Senior executives and management of the organization should be trained specifically in line with their roles and responsibilities.
	• The training program should consider different forms/formats, such as:
	  ○ lectures or self-studies, being mentored by expert staff or consultants,
	  ○ rotating staff members to follow various activities,
	  ○ recruiting already skilled people,
	  ○ hiring consultants.
	• Trainings should be designed to include interactive elements, particularly as:
	  ○ Presentation of real examples of attacks.
	  ○ Developing security-themed games or competitions that challenge personnel to apply their knowledge in various scenarios.
	  ○ Incorporating simulations or exercises that mimic real-life situations allowing personnel to practice their skills in a controlled environment.
	  ○ Offering incentives or rewards for successfully completing training modules or achieving high assessment scores.
	  ○ Privileged users understand their roles and responsibilities
	• Provide relevant trainings for third-party stakeholders (e.g., suppliers, customers, partners) to understand their roles and responsibilities before they are engaged.
	• Train employees to recognize social engineering attempts on them and not disclose any information that could violate the Organization's security policies, such as during social gatherings, public events, and training events.

PRINCIPLE P10.03	
Mechanisms and KPIs for monitoring and evaluation	• Establish mechanisms and key performance indicators for monitoring and evaluating the effectiveness and efficiency of awareness and training programs. • Review and update regularly the content of the security training and awareness to reflect properly new risks, contemporary threats, prospect challenges and changes to the organization's information technology infrastructure or applicable legislation and regulations. • Each training should be followed with an assessment, to ascertain the effectiveness of the programme, including maintaining of records of attendance of security awareness programmes.

11. SERVICE PROVIDER (& CONTRACTOR/3RD PARTY) MANAGEMENT

Level	Security measures
1	*11.1.* Develop, document and disseminate Supply chain risk management policy, encompassing minimum security requirements for contracts with third parties. *11.2.* Establish and agree information security requirements, in cooperation with the competent authority (where applicable), with each supplier/service provider based on the type of relationship with the supplier/service provider. *11.3.* Define and enact processes and procedures alongside with a competent authority where applicable to govern information security risks associated with the ICT products and services in supply chain management *11.4.* Monitor, review and audit on a regular basis all services provided by third parties.
2	*11.5.* Regularly monitor, review and evaluate, in collaboration with the competent authority where applicable, changes in a supplier's information security practices and service delivery. *11.6.* Keep track record on security incidents related to or caused by third party. *11.7.* Review and update Supply chain risk management policy once a year, considering past incidents, changes, etc.
3	*11.8.* Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide.

To implement these security measures, the principles should be considered but not limited to:

Principle P11.01	
Supply Chain Risk Management Policy and Procedures	• Develop, document, and disseminate supply chain risk management policy, which will at minimum define the following: Purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The policy must be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. • Define and implement procedures for managing information security risks associated with the ICT products and services in supply chain management, in line with the policy. • Designate an official or staff member to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures.
Principle P11.02	
Supply Chain Risk Management Plan	• Prepare a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the systems, system components or system services. • Review and update it regularly or in case of need to address threat, organizational or environmental changes.

Principle P11.03	

Service Contracts	• Specify security mechanisms, service levels and management requirements in all service contracts (in collaboration with the competent authority where applicable). If outsourcing services are used, the service provider should be obliged to implement an event logging system in networks and ICT systems and develop procedures for archiving the collected logs (at least for a period of 12 months).
	• Each contract with third party should contain provisions requiring the party to regularly report on the outsourced service'(s) security posture, including any incidents.
	• The following risk factors should be taken into consideration during the preparation of contracts with providers of ICT services and products:
	  ○ The current financial and economic situation of the prospect service provider (when selecting a service provider).
	  ○ The ownership structure, if possible, including the identification of real beneficiaries (when selecting a service provider).
	• Every relationship with a new partner should start with a confidentiality agreement, providing for real sanctions for any violation. Particular attention should be paid to relations with suppliers of ICT solutions or products containing computer software that may affect the operational capacity of the institution's IT infrastructure.
	• Alongside with the ordinary elements, the contract should contain, at least, the following specific elements:
	  ○ description of the expected scope of cooperation of the service provider, including third parties acting on its behalf, and co-participating in the provision of the service with the institution in the event of fixing failures. This scope should include but is not limited to the provision of specific infrastructure, personnel and availability of such personnel.
	  ○ rules for removing reported errors, in the form of the so-called Service Level Agreement (SLA), containing indicators regarding cooperation procedures, timeliness of removing reported errors as well as sanctions for delays in removing errors and their failure to remove them.
	  ○ Service contracts with software developers/producers should include additional SLAs regarding the removal of detected vulnerabilities, the use of which may cause the risk of disrupting the functioning of the institution's ICT infrastructure.
	  ○ The contract for the supply or maintenance of software should contain provisions regarding the procedure for managing changes in this software and the method of determining the service provider's remuneration for this.
	  ○ The contract for the supply of software and hardware should contain provisions increasing security against ICT threats.
	  ○ In the case of ICT systems supporting critical processes, the requirement for the supplier to have an insurance policy against losses caused by improper performance of the contract.
	• Each concluded contract should be subject to risk analysis regarding the so-called vendor lock (VL), i.e., dependence on one supplier. VL is usually associated with unfavourable intellectual property provisions regarding the possibility of developing or using products (usually software) in the event of the supplier's bankruptcy or termination of cooperation by the supplier.
	• The contract should not contain provisions completely excluding the supplier's liability or limiting its liability to amounts that do not correspond to the risk associated with the delivery of a product or service that does not meet the contract conditions.

12 SECURE TESTING & CODE REVIEW

LEVEL	SECURITY MEASURES
1	**12.1.** None
2	**12.2.** Use Up-to-Date and Trusted Third-Party Software Components
3	**12.3.** Establish and Maintain a Secure Application Development Process **12.4.** Structured approach for conducting security testing and code reviews of application software prior to deployment. **12.5.** Mechanisms to identify and remediate security weaknesses or vulnerabilities discovered during testing and code review processes. **12.6.** Static and Dynamic Application Security Testing

To implement these security measures, the principles should be considered but not limited to:

Principle – P12.01	
Secure Development Guidelines	• Develop and update clear guidelines for secure app development, covering key areas like input validation and data encryption. Make these guidelines accessible to all developers and regularly update them to match evolving threats. • Collaborate with security experts to validate and improve these guidelines, ensuring their effectiveness.
Code Reviews and Static Analysis	• Establish regular code reviews where developers inspect each other's code for security flaws, fostering a culture of accountability and awareness through peer learning and collaboration. • Integrate automated static code analysis tools into the development pipeline to automatically detect potential security issues, ensuring regular scans and providing actionable feedback to developers on addressing vulnerabilities.
Security Training and Awareness	• Hold interactive training sessions for developers on secure coding practices, vulnerabilities, and secure frameworks, reinforcing learning with practical examples. • Launch awareness campaigns within development teams via emails, posters, and newsletters, highlighting security's crucial role in the software lifecycle and sharing insights on recent incidents and best practices.
PRINCIPLE P12.02	
Static and Dynamic Application Security Testing (Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))	• Integrate SAST tools into the development pipeline for automatic code scanning, offering immediate feedback to developers. • Incorporate DAST tools in the testing phase to simulate real-world attacks and identify vulnerabilities in runtime behaviour, complementing static analysis for comprehensive security assessment.
Implement Mechanisms to identify and	• Establish procedures for identifying and remediating security weaknesses, assigning roles and deadlines.

remediate security weaknesses or vulnerabilities discovered during testing and code review processes.	• Integrate security findings into change management, documenting and addressing vulnerabilities through controlled code changes.
PRINCIPLE P12.03	
Conduct Security Testing Throughout the Software Development Lifecycle	• Integrate security testing into Continuous Integration/Continuous Deployment (CI/CD) Pipelines to automate the process of identifying and addressing security vulnerabilities throughout the software development lifecycle. Configure automated tests to run automatically whenever code changes are made, providing developers with immediate feedback on potential security issues. • Conduct security regression testing to ensure that security controls and mechanisms remain effective as the software evolves over time. Identify and address any regressions or unintended consequences of code changes that may impact the security of the application.
PRINCIPLE P12.04	
Implement Secure Coding Practices	• Establish and enforce secure coding standards and guidelines to promote the use of secure coding practices across development teams. Provide developers with training and resources to help them understand and adhere to these standards throughout the software development lifecycle. • Utilize secure development frameworks and libraries that have been vetted for security vulnerabilities and adhere to industry best practices. Encourage developers to leverage these frameworks to reduce the risk of introducing security flaws or vulnerabilities into the codebase.

13. INCIDENT RESPONSE AND DATA RECOVERY

Incident Response

LEVEL	SECURITY MEASURES
1	*13.1.* Define procedures to detect, evaluate and respond to incidents, with allocated responsibilities for managing detected cyber security incidents. *13.2.* Establish and implement an operational incident response capability to prepare for, detect, and quickly respond to a cybersecurity incident.
2	*13.3.* Perform appropriate post-incident activities. *13.4.* Ensure real-time cybersecurity detection for critical systems and their components. *13.5.* Ensure computer forensics of compromised systems, including memory analysis, network traffic analysis, and malware reverse engineering. *13.6.* Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident.
3	*13.7.* Conduct threat hunting. *13.8.* Collaborate with peers to share information on indicators of compromise, enhance its security controls and prevent malicious campaigns. *13.9.* Assure static and dynamic malware analysis via dedicated malware analysis tools (on-premises or cloud-based solutions). *13.10.* Ensure Incident analysis via dedicated analysis tools.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P13.01	
Adequate Incident Response Activities and Processes	• Undertake necessary activities including response processes and procedures. • Prepare Incident Response Plan to be executed during or after cyber incident happen. • Coordinate and properly communicate incident response activities with relevant stakeholders, both internal and external. • Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. • Set up processes or systems for incident detection and implement industry standards where appropriate. • Implement Advanced Threat Detection and Incident Response Systems. • Investigate notifications from detection systems. • Form an Incident Response Team.
PRINCIPLE P13.02	
Incident Response Procedures	The procedures should include at minimum: • reporting structure, • incident response plan, roles, responsibilities and contact information, in particular, • internal and external communication processes, • incident classification, • amount of time for human reaction to the reported incident, according to the incident type.

	• analysing, containing and eradicating processes. • Procedures for reporting and investigating security incidents related to application software, including incident analysis and mitigation strategies, should be part of the incident response procedures. • To be effective, the procedures should be supported by adequate human, technological, organizational capacity and capabilities. • Assess regularly relevant procedures considering past incidents.
Incidents analysis and reports	• Understand the impact of the incidents and categorize them consistent with response plans. • Communicate and report about on going or past incidents to third parties, customers, and/or government authorities, when necessary. • Analyse root-cause of the incident. • Conduct lessons learned – identifying areas for improvement of the security posture. • Maintain a process for the workforce to report security incidents including reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. • Conduct periodic scenario-based trainings through exploring scenario in line with the threats the organization faces with.
Roles and responsibilities	• Assign roles and adequate responsibilities manage incident handling to staff from legal, Information security, facilities, public relations, human resources, incident responders, and analysts, as applicable.
Contact information and link with relevant authorities	• Establish contact information and link with relevant authorities and parties that need to be informed of security incidents • Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. • Determine mechanisms to communicate and report during a security incident. • Maintain operational contacts channels with relevant authorities, bodies and services necessary. • Establish link with relevant law enforcement and regulatory bodies to facilitate cooperation during cyber forensics investigations and ensure compliance with legal and regulatory requirements.
Incident Response Capabilities Tests	• Perform incident response capabilities tests at least every second year and meanwhile if needed.
PRINCIPLE P513.03	

Recovery activities	• Conduct analysis to ensure effective response and support recovery activities and perform activities to prevent expansion, mitigate effects, and resolve the incident
	• Foster cross-functional collaboration:
	  ○ Encourage communication and cooperation between the incident response team, SOC personnel, IT, and other relevant teams to facilitate the sharing of information and expertise, enhancing overall security posture.
	  ○ Continuous training and awareness activities, especially for incident response, SOC analysts and other staff to ensure they remain up to date with the latest threats, tools, and best practices in the field.

14. DATA PROTECTION AND PRIVACY

14.1 Media Protection

Level	Security measures
1	*14.1.1.* Protect system media containing paper and digital non-public information. *14.1.2.* Arrange access to non-public information on system media only to authorized users. *14.1.3.* Destroy or sanitize system media containing non-public information before disposal or release for reuse. *14.1.4.* Guarantee the identification of records and their retention period, according to the legislation or regulations requirements. *14.1.5.* Prohibit usage of any portable storage devices that are not possessed by the organization, with exception of certain specified cases and circumstances *14.1.6.* Control the use of removable media on system components.
2	*14.1.7.* Mark each media with appropriate non-public information markings and limitations for distribution. *14.1.8.* Oversee access to media containing non-public information and maintain accountability for media during transport outside of controlled areas.
3	*14.1.9.* Implement cryptographic mechanisms to protect the confidentiality of non-public information stored on digital media during transport unless otherwise protected by alternative physical safeguards. *14.1.10.* Protect the confidentiality of backup non-public information at storage locations.

To implement these security measures, the principles should be considered but not limited to:

Principle P14.1.01	
Organizational and technical measures	• Develop, document and implement organizational and technical measures for protection of all media containing non-public information. • Measures should be appropriate to the media containing non-public information. • Regular review and adaptation of the measures according to the legal requirements and the contemporary needs. • The organization should limit access to non-public information on system media to authorized users through appropriate written rules and procedures, with precisely determined access authorizations according to the job position and responsibilities.
Principle P14.1.02	
Handling and availability of the media after the termination of the employment relationship	• Regulate strictly handling and availability of the media after the termination of the employment relationship. • Any employee after termination of employment must return all resources (system media containing non-public information) that have been transferred to the employee, as follows: ○ The return should cover all ICT devices issued.

	○ The return of resources should also occur in the event of a job change in a situation where the employee ceases to use a given resource as part of the performance of official duties.
Principle P14.1.03	
Sanitization or destruction of system media	• Sanitize or destroy system media containing non-public information before disposal or release for reuse. • This should be done by physical destruction methods, such as shredding, incineration, or degaussing, for paper-based and non-reusable digital media. • The whole process of media sanitization and disposal should be documented, including information about the date, media type, and personnel responsible. • Make unable to read data (by overwriting, destroying the carrier, etc.) of all data carriers permanently leaving the organization.
Identification of records and retention period	• Ensure identification of records and their retention period, considering relevant legislation. • The major legislation that should be considered as most relevant and starting point is the Law on personal data protection of the Republic of North Macedonia.
Principle P14.1.04	
Procedures for dealing with data carriers and ICT equipment withdrawn from current use	• Develop and put in practice procedures for dealing with data carriers and ICT equipment withdrawn from current use. • This should be done through: ○ Categorization of data carriers (e.g., portable and non-portable); ○ Rules of conduct for each category. ○ Procedures should address the issuance, withdrawal and transfer of media. • Procedures should include blocking unapproved CD/DVD/USB media and blocking connection to unapproved phones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices. This requirement applies to ICT systems responsible for supporting critical processes carried out by the institution.
Principle P14.1.05	
accountability for media containing non-public information during transport outside of controlled areas	• Control and maintain accountability for media containing non-public information during transport outside of controlled areas. • Secure packaging and transport methods, such as tamper-evident packaging or courier services with chain-of-custody tracking. • Encrypted communication channels when transmitting NPI electronically. • Log of media transport activities, including the sender, recipient, date, and method of transport. • Recommendation for strong cryptography mechanisms.
Control the use of removable media on system components	• Control the use of removable media on system component by: a) Establishing a policy that outlines the acceptable use of removable media, including types of media, devices, and circumstances under which their use is permitted. b) Implementing technical controls, such as endpoint security solutions, to restrict the use of unauthorized removable media on system components.

14.2. Personal Data Processing and Transparency

Level	Security measures
1	*14.2.1.* Identify and meet the requirements for guaranteeing and protecting personal data and privacy through personal data protection framework' establishment. *14.2.2.* Comply with and appropriately implement the current Law on personal data protection in the Republic of North Macedonia.
2	*14.2.3.* Develop processes and technical controls to identify, organize, securely handle, retain, and dispose of personal data. *14.2.4.* Review and update Data Protection Policy once a year or more frequently in case of need.
3	*14.2.5.* No specific requirements for Level 3.

To implement these security measures, the principles should be considered but not limited to:

Principle P14.2.01	
Integrated personal data protection management framework	• Develop and establish an integrated personal data protection management framework according to applicable laws and regulations and contractual requirements. • Develop and implement Personal Data Protection Policy. • Establish written procedures and measures that ensure personal data protection in everyday working operations. • Apply specific conditions for special/sensitive categories of personal data. • Identify and appropriately classify data in the organization and map its flow across various processes, systems, and third parties. • Regularly review and update data inventory to account for changes in data processing activities and systems. • Create and maintain a record of processing activities to document each personal data processing activity. • Use various techniques and tools to de-identify data and to decrease risks towards personal data, such as pseudonymization, data masking and encryption. • Follow the changes in the regulatory environment and update data protection policies, procedures, and controls accordingly to maintain compliance.
Access to personal data	• Regulate and adequately restrict access to personal data through implementation of need-to-know basis. • Monitor and record any unauthorized access to personal data. • Implement specific organizational and technical measures for safe storage and transfer of personal data.
Principle P14.2.02	
Mechanisms for guaranteeing rights of data subjects	• Develop and adequately implement mechanisms for guaranteeing rights of data subjects. • Provide notice to individuals about the processing of their personal data. • Implement defined tools or mechanisms for individuals to consent to the processing of their data prior to its collection that facilitate individuals' informed decision-making. • Implement mechanisms to inform data subjects about their rights, legitimate purposes for processing their personal data, or any transfers to third parties. • Develop a process for handling data subjects' access requests, including rectification, erasure, and data portability mechanisms.

Principle P14.2.03	
Relevant trainings for employees	• Arrange standardized trainings for the protection of personal data tailored strictly in line with employees' assigned roles and responsibilities towards personal data and privacy.

15. CYBER THREAT INTELLIGENCE

LEVEL	SECURITY MEASURES
1	***15.1.*** none
2	***15.2.*** Create polices for gathering and consolidating threat intelligence. ***15.3.*** Incident response procedures when credible threat intelligence is received. ***15.4.*** Implement a threat awareness program that includes a cross-organization information sharing capability for threat intelligence
3	**15.5.** Utilize any standardized protocols (such as STIX/TAXII) for automated indicator sharing. **15.6.** Establish processes to ensure timely dissemination of actionable threat information. **15.7.** Framework to assess the severity and impact of a threat based on received intelligence. **15.8.** Adapt security controls based on threat insights. **15.9.** Ensure interoperability with other organizations' threat intelligence platforms.

To implement these security measures, the principles should be considered but not limited to:

Principle P15.01	
Regular Monitoring of External Threat Intelligence Feeds	• Subscribe to open-source intelligence (OSINT) and commercial threat intelligence feeds to stay updated on the latest threats. • Maintain a recorded log of significant threat intelligence gathered from various sources, including security researchers, to track trends and patterns.
Participation in Information Sharing Initiatives	• Participate in Information Sharing and Analysis Centers (ISACs), industry-specific groups, and government-led initiatives to exchange threat intelligence with peers. • Engage in collaborative efforts with industry partners and government agencies to address common cybersecurity challenges and share threat information effectively.
Sharing Actionable Threat Intelligence with Trusted Peers	• Share actionable threat intelligence, such as indicators of compromise (IOCs), malware samples, and attack techniques, with trusted peers and partners. • Collaborate with peers to improve situational awareness and strengthen defences against evolving threats.
Establish Secure and Confidential Threat Intelligence Sharing Mechanisms	• Establish mechanisms and protocols for secure and confidential threat intelligence sharing. • Implement access controls and encryption to ensure that sensitive information is protected and shared only with authorized parties.
Principle P15.02	
Source Verification	• Verify the credibility and reputation of the source providing the threat intelligence. • Evaluate the source's track record and reliability in delivering accurate and timely information.

Cross-Referencing	• Cross-reference incoming threat intelligence with multiple trusted sources to validate its accuracy and relevance. • Compare information from different sources to identify inconsistencies or discrepancies.
Contextual Analysis	• Analyse the contextual relevance of the threat intelligence to the organization's specific environment, industry, and threat landscape. • Determine the potential impact of the threat on the organization's assets, operations, and security posture.
Correlation with Internal Data	• Correlate incoming threat intelligence with internal data and security events to assess its alignment with known threats and vulnerabilities. • Validate the consistency of the intelligence with the organization's internal observations and incident reports.
Expert Review	• Involve subject matter experts (SMEs) or security analysts in reviewing and validating incoming threat intelligence. • Leverage their expertise to assess the credibility and relevance of intelligence based on technical analysis and domain knowledge.
Principle P15.03	
Standardization of Formats and Protocols	• Adopt industry-standard formats and protocols for exchanging threat intelligence data to ensure interoperability with other organizations' platforms. • Utilize formats such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) for seamless integration.
API Integration	• Implement Application Programming Interfaces (APIs) to facilitate the exchange of threat intelligence data between different platforms. • Ensure that APIs support common protocols and authentication mechanisms for secure communication.
Collaborative Partnerships	• Establish collaborative partnerships with other organizations and information sharing initiatives to streamline the exchange of threat intelligence. • Participate in industry-specific sharing communities and forums to foster interoperability and collective defence efforts.
Principle P15.04	
Automated Threat Feeds	• Set up automated processes to collect, analyse, and disseminate newly identified threats from various sources, including internal monitoring systems and external feeds. • Use threat intelligence platforms or Security Information and Event Management (SIEM) systems to automate the aggregation and distribution of threat feeds.
Alerting Mechanisms	• Implement automated alerting mechanisms to notify relevant stakeholders about newly identified threats in real-time. • Configure customizable alerts based on predefined criteria such as threat severity, relevance to the organization, and affected assets.

16. INFORMATION SHARING & AGREEMENTS

LEVEL	SECURITY MEASURES
1	***16.1.*** Inform end-users of communication networks and services about particular and significant security incidents that may affect them.
2	***16.2.*** Establish protocols for sharing threat information with other entities (i.e.. public sector organizations / law enforcement / private sector organizations / your supply chain or other 3rd parties/etc.) ***16.3.*** Implement technology solutions for information protection and automated sharing. ***16.4.*** Establish and Maintain Contact Information for Reporting Security Incidents (CIS)
3	***16.5.*** -. None

To implement these security measures, the principles should be considered but not limited to:

Principle P16.01	

Inform end-users of communication networks and services about particular and significant security incidents that may affect them.	• Clear and Understandable Communication
	  ○ Communicate security incidents in a clear and understandable manner, avoiding technical jargon that may confuse end-users.
	  ○ Provide actionable advice on how end-users can protect themselves and mitigate the risks associated with the identified threats.
	• Provide timely notifications to end-users about particular and significant security incident that may affect the network or service they utilize.
	  ○ Use multiple communication channels such as email, SMS alerts, and in-app notifications, social media to ensure broad reach.

Principle P16.02	
Establishment of Information Sharing protocols	• Develop formal agreements/protocols with trusted partners, vendors, and stakeholders outlining the terms and conditions of information sharing. • Define the scope of information to be shared, including data classification, sensitivity, and handling requirements, to ensure confidentiality, integrity, and availability are maintained. • Specify legal and regulatory compliance obligations, privacy considerations, and data protection requirements in information sharing agreements to mitigate risks and liabilities.
Principle P16.03	
Secure Communication Channels	• Implement secure communication channels, such as encrypted email, secure file transfer protocols (SFTP)/FTPS, virtual private networks (VPNs), and secure messaging platforms, to exchange sensitive information securely. • Configure encryption mechanisms, digital signatures, and authentication controls to protect the confidentiality, integrity, and authenticity of shared information during transit and storage. • Enforce access controls and user authentication mechanisms to restrict access to shared information based on the principle of least privilege and need-to-know.

17. SECURITY POLICY AND PROCEDURES

Level	Security measures
1	*17.1.* Develop, establish and communicate Information Security Policy (ISP) in accordance with applicable legal, statutory and regulatory requirements. *17.2.* Establish and document Operating procedures for information processing facilities.
2	*17.3.* Define, publish and communicate further appropriate topic-specific policies. *17.4.* Review the Information Security Policy and topic-specific policies regularly and if significant changes occur. *17.5.* Review and evaluate operating procedures at planned intervals, and in case when significant changes occur. *17.6.* Outline requirements for managing the security of information shared with external parties.
3	*17.7.* Review and update periodically (at least once per year or when needed) the security plans for organizational information systems. *17.8.* If the government organization activity is critical to the state, national security or public safety, or if it processes large amount of critical non-public information, then the organization recommended to implement and certify ISMS.

To implement these security measures, the principles should be considered but not limited to:

Principle P17.01	
Information Security Policy (ISP)	• The Information security policy and appropriate topic-specific policies should be clear, precise, and consistent. • The basic elements of the ISP: ○ purpose, ○ scope, ○ roles and responsibilities, ○ management commitment, ○ coordination among organizational entities, and ○ compliance. • Monitor and evaluate the implementation of policies on a regular basis, at least once a year, or in case when significant changes happen. • Review the security policy following incidents. • Arrange various activities to make key personnel aware of the security policy. • Designate an official or staff member to manage the development, documentation and dissemination of the ISP.
Principle P17.02	
Operational Procedures	• Create and implement Operational Procedures to facilitate the implementation of the security policy and the associated security controls. • Operational procedures should include at least: a) instructions for installing, configuring and updating systems and software, b) rules for recording, monitoring and handling errors or exceptions, including restrictions on the use of system tools, c) rebooting and restoring the system in case of failure (at least one per year), ISP compliance with this standard and other legal regulations should be checked.

	• Review and evaluate Operational Procedures annually or in case when significant changes occur.
Principle P17.03	
Security Plans	• Develop Security Plans with controls for the information systems and the rules of behaviour for individuals accessing the information systems. • Security Plans should be consistent and in line with the ISP and the Operational Procedures. • Security Plans should be created in close cooperation with the management of the organization.
Principle P17.04	
Audits	• Carry out the internal audits following the best practices and leading examples. • The internal audit may be carried out by the employees of public institutions with appropriate training or approved third parties. • Document and keep all the reports from occurred internal and external audits.
Principle P17.05	
International Standards	• Use international standards such as ISO/IEC 27001 [ISO27001] to implement ISMS.

18. PHYSICAL & ENVIRONMENTAL PROTECTION (& CONTINGENCY PLANNING)

LEVEL	*SECURITY MEASURES*
1	***18.1.*** Conduct comprehensive risk assessments to divide managed areas into distinct security zones tailored to specific security needs based on identified risks. ***18.2.*** Strictly control access to security zones, granting it only to authorized individuals with a legitimate need-to-have basis. ***18.3.*** Implement access control measures to restrict physical access to organizational systems, equipment, and operating environments. ***18.4.*** Grant access to authorized individuals based on official duties, regularly reviewing, and updating access permissions as necessary. ***18.5.*** Provide yearly basic physical security training to employees to enhance awareness of security risks and best practices, covering topics such as recognizing suspicious activities, reporting security incidents, and following access control procedures.
2	***18.6.*** Maintain comprehensive audit logs of all physical access activities within facilities, capturing details such as date, time, location, and individual identity, ensuring accountability and enabling forensic analysis. ***18.7.*** Actively assist and monitor visitor activities within premises to ensure security and compliance with access policies, deploying security personnel or surveillance systems to enhance overall security measures.
3	***18.8.*** Implement robust controls and management procedures for physical access devices such as badges, keys, PIN codes, and access cards to ensure secure access to facilities and sensitive areas. ***18.9.*** Enforce stringent safeguarding measures to protect Non-Public Information (NPI) processed at alternate work sites, such as Disaster Data Centers, safeguarding critical data against unauthorized access or disclosure. ***18.10.*** Provide comprehensive physical security training to all employees, including security personnel, covering advanced topics such as threat detection, emergency response procedures, and incident handling protocols, ensuring personnel are well-prepared to address diverse security challenges effectively.

To implement these security measures, the principles should be considered but not limited to:

PRINCIPLE P18.01	
Meticulous Security Zone Design	• Develop security zones meticulously to counter anticipated attack scenarios. • Aim to slow down potential attackers' actions and provide adequate reaction time.

Focus on Vulnerability Elimination	• Design each zone to focus on eliminating vulnerabilities and strengthening defenses based on comprehensive risk assessments.
Intensified Security Measures	• Implement security measures that intensify as potential attackers approach zones safeguarding critical organizational infrastructure. • Aim to deter or delay attackers, enabling timely response and threat mitigation.
PRINCIPLE P18.02	
Comprehensive Security Training	• Extend the requirement for security awareness and training to all individuals accessing the organization's premises. • Ensure that training efforts cover security protocols and individuals' roles in maintaining a secure environment.
Establishment of Access Rules and Procedures	• Outline specific instructions for entering, leaving, and moving within security zones to ensure consistent adherence to security protocols. • Document exceptions for certain individuals or services with clear guidelines for implementation.
Basic Training for All Employees	• Provide basic security training covering essential topics for crisis preparedness and response to all employees. • Cover various aspects of security and emergency preparedness, including threat identification, security protocols, and emergency evacuation procedures.
PRINCIPLE P18.03	
Maintenance of Audit Logs	• Maintain audit logs capturing physical access activities for a minimum of 12 months. • Facilitate retrospective analysis and investigation of security incidents through comprehensive audit logs.
PRINCIPLE P18.04	
Range of Technologies and Protocols	• Implement physical security measures encompassing a range of technologies and protocols to safeguard organizational assets and infrastructure. • Include personnel, barriers, access control systems, surveillance, alarms, fire detection, flood detection, air conditioning, and employee awareness initiatives.
Registration and Individualization of Access Devices	• Register and personalize physical access devices, such as badges or keys, to enhance accountability and traceability. • Label or number each device for easy identification and tracking.
Documentation of Access Rules and Procedures	• Document rules governing the storage, issuance, and exchange of access devices to ensure consistency and accountability. • Clearly define procedures for issuing cards or keys, periodic code changes, and visitor supervision.

Supervised Access for Visitors	• Ensure visitors gain access to facilities under the supervision of authorized personnel throughout their visit duration. • Ensure accountability and oversight of visitor activities within protected premises.
Security Features for Access Badges	• Incorporate security elements into access badges to deter tampering or counterfeiting, enhancing their integrity and reliability. • Include contact information on badges for reporting lost badges to authorized security personnel.
PRINCIPLE P18.05	
Development of Backup Procedures	• Establish detailed procedures for backing up and testing data, software, and system images, considering any relevant, new, and changed data. • b) Outline execution frequency, storage duration, and backup type based on system nature, data significance, and change frequency.
Backup Types and Methods	• Employ various backup methods such as offline, offsite, and online backups to ensure comprehensive data protection. • Choose backup types like full, incremental, differential, mirror, snapshot, continuous data protection (CDP), and synthetic full backups based on risk analysis and data copying processes. • Establish procedures for creating and storing backups in external locations outside the organization's facilities to mitigate risks of disruption or infrastructure failure.
Secure Storage and Encryption	• Encrypt and store backup copies in dedicated spaces within the organization's network to ensure limited access and no internet connectivity. • Test backup and recovery processes regularly to ensure accuracy and effectiveness, especially after significant ICT architecture changes. • Implement redundancy in information processing facilities, including critical network devices and servers, to meet availability requirements and ensure uninterrupted operations.
Preparation of Warning and Communication Plans	• Organize a response structure to facilitate swift and coordinated actions during crisis situations, ensuring effective communication and decision-making. • Prepare warning and communication plans/procedures to disseminate timely information and instructions to relevant stakeholders during emergencies.
Creation and testing of Business Continuity Plans	• Create detailed business continuity plans and procedures, outlining steps for recovery and restoration of critical processes and resources. • Regularly test business continuity plans and procedures to validate effectiveness and identify areas for improvement. • Establish mechanisms for continuous improvement to review and enhance business continuity strategies, plans, and response capabilities based on feedback and lessons learned from testing and real-world incidents.

Annex 1. Mapping of the security controls with the international standards (NIST, ENISA, NIS2, ISO, CIS, NCSA)

Standard	ISO/IEC 27001:2022	ISO/IEC 27002:2022	ENISA	NIS2	NIST SP 800-53	CIS Controls v8	NCSA
1. Account Management & Access Control	Annex A.9 (Access Control)	Section 9 (Access Control)	Access Control Management	Articles 19-21 (Risk Management)	Access Control (AC)	Control 6 (Access Control Management), Control 16 Account Monitoring	Section 3 (Access Control Practice)
2. Inventory Control of Assets (Hardware & Software)	Annex A.8 (Asset Management)	Section 8 (Asset Management)	Asset Inventory	Articles 19-21 (Governance & Risk Management)	CM-8 (System Component Inventory)	Control 1 (Inventory of Assets), Control 2 (Software Assets)	Section 4 (Asset Inventory)
3. Secure Configuration & Patch Management (Assets & Software)	Annex A.12 (Operations Security)	Section 12 (Secure Configuration)	Secure Configuration Guidelines	Articles 19-21 (Technical Measures)	CM (Configuration Management)	Control 4 (Secure Configuration), Control 7 (Vulnerability Management)	Section 4 (Patch & Configuration Management)
4. Vulnerability Management & Penetration Testing	Annex A.12.6 (Vulnerability Management)	Section 12.6 (Technical Vulnerability Management)	Vulnerability and Patch Management	Article 19 (Risk Management)	RA-5 (Vulnerability Monitoring)	Control 7 (Vulnerability Management)	Section 4 (Penetration Testing & Vulnerability Scanning)
5. Audit Logging & Management	Annex A.12.4 (Logging and Monitoring)	Section 12.4 (Logging and Monitoring)	Logging & Monitoring Practices	Article 19 (Risk Management)	AU (Audit and Accountability)	Control 8 (Audit Log Management)	Section 7 (Audit Logging)
6. Email & Browser Protections	Annex A.13 (Communications Security)	Section 13 (Communications Security)	Email and Web Security	Articles 19-21 (Technical Measures)	SC-7 (Boundary Protection), SC-18 (Cryptographic Protection)	Control 9 (Email & Browser Protection)	Section 8 (Email and Web Protection)

Standard	ISO/IEC 27001:2022	ISO/IEC 27002:2022	ENISA	NIS2	NIST SP 800-53	CIS Controls v8	NCSA
7. Malware Defense (& Analysis)	Annex A.12.2 (Protection Against Malware)	Section 12.2 (Malware Protection)	Malware Protection and Incident Response	Articles 19-21 (Technical Measures)	SI-3 (Malware Protection)	Control 10 (Malware Defenses)	Section 9 (Malware Analysis & Defense)
8. Network Infrastructure Management	Annex A.13 (Network Security)	Section 13 (Network Security)	Network Security Management	Articles 19-21 (Technical Measures)	SC (System and Communications Protection)	Control 11 (Network Infrastructure Management)	Section 10 (Network Infrastructure Security)
9. Network Monitoring & Defense	Annex A.13.1 (Network Security)	Section 13.1 (Network Security)	Network Monitoring and Detection	Articles 19-21 (Risk Management)	SC-7 (Boundary Protection), AU-12 (Audit and Monitoring)	Control 12 (Network Monitoring)	Section 10 (Network Defense)
10. Security Awareness & Skills Training	Annex A.7 (Human Resource Security)	Section 7.2 (Awareness and Training)	Security Awareness and Education	Article 19 (Risk Management)	AT (Awareness and Training)	Control 14 (Security Awareness)	Section 5 (Security Awareness)
11. Service Provider & Contractor /Third-Party Management	Annex A.15 (Supplier Relationships)	Section 15 (Supplier Security)	Supply Chain Security	Article 24 (Supply Chain Management)	SA (System and Services Acquisition)	Control 15 (Service Provider Management)	Section 6 (Third-Party Risk Management)
12. Secure Testing & Code Review	Annex A.14 (System Acquisition, Development, and Maintenance)	Section 14 (Development Security)	Secure Development and Testing	Article 19 (Risk Management)	SA-11 (Developer Security Testing and Evaluation)	Control 16 (Application Software Security)	Section 11 (Secure Development and Testing)
13. Incident Response & Data Recovery	Annex A.16 (Incident Management)	Section 16 (Incident Management)	Incident Response Planning	Article 21 (Incident Response)	IR (Incident Response)	Control 17 (Incident Response)	Section 12 (Incident Response & Recovery)
14. Data Protection & Privacy	Annex A.18 (Compliance)	Section 18 (Compliance)	Data Protection Guidelines	Article 22 (Data Protection)	MP (Media Protection), PT (Privacy)	Control 13 (Data Protection)	Section 13 (Data Privacy & Protection)
15. Cyber Threat Intelligence	N/A	N/A	Threat Intelligence Management	N/A	SI-4 (Information System Monitoring)	N/A	N/A

Standard	ISO/IEC 27001:2022	ISO/IEC 27002:2022	ENISA	NIS2	NIST SP 800-53	CIS Controls v8	NCSA
16. Information Sharing & Agreements	Annex A.15 (Supplier Relationships)	Section 15 (Supplier Security)	Information Sharing Guidelines	Articles 19-21 (Risk Management)	CA (Security Assessment and Authorization)	N/A	Section 14 (Information Sharing)
17. Security Policy and Procedures	Annex A.5 (Information Security Policies)	Section 5 (Information Security Policies)	Policy and Strategy Management	Articles 19-21 (Governance)	PL (Planning)	Control 1 (Establish Security Program)	Section 1 (Security Policy)
18. Physical & Environmental Protection (& Contingency Planning)	Annex A.11 (Physical and Environmental Security)	Section 11 (Physical and Environmental Security)	Physical Security Guidelines	Articles 19-21 (Technical Measures)	PE (Physical and Environmental Protection)	Control 13 (Data Protection)	Section 15 (Physical & Environmental Security)

References

RESPONSIBLE MINISTRY/STANDARD NUMBER	DOCUMENT NAME AND TYPE
MINISTRY OF DIGITAL TRANSFORMATION	**Strategic documents:** Cybersecurity Strategy (2018-2022) Cybersecurity Strategy (2023-2027)* National Short-term ICT Strategy (2016-2017) National ICT Strategy (2023-2027)** **Laws and By-Laws:** Law on Security of network and Information systems and Digital transformation*** Law on Electronic Management and Electronic Services Law on Electronic Documents, Electronic Identification and Trust Services Law on Electronic Communications Law on the establishment of Macedonian Academic Research Network Law on Archive material Standards for Data Quality in State Institution systems Rulebook on standards and Rules for Safety of IT Systems used in Public administration bodies for electronic communication Guidelines for monitoring and management of incidents related to IT security Guidelines on acting upon risk assessment and management
MINISTRY OF DEFENCE	**Strategic Documents:** Cyber Defence Strategy (2020) Strategy for building resilience and dealing with hybrid threats (2021-2025)* **Laws and By-Laws:** Law on Critical Infrastructure Law on Defence
MINISTRY OF INTERIOR	**Strategic Documents:** Strategy for Cyber crime (2018-2022) Strategy for Cyber crime **Laws and By-Laws:** 3.3 Law on Communication Surveillance
DIRECTORATE FOR SECURITY OF CLASSIFIED INFORMATION	Laws and By-Laws: 5.1 Law on Classified Information By-Laws Decree on Physical Security of Classified Information Decree on Administrative Security of Classified Information Decree on Personal Security Decree on Industrial Security of Classified Information

	Decree on Information Security of Classified Information
AGENCY FOR PERSONAL DATA PROTECTION	**Laws and By-Laws:** Law on Personal Data Protection Law on the ratification of the Protocol to amend the Convention for the Protection of Persons with regard to automatic processing of personal data Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in relation to supervisory bodies and cross-border data transfers Rulebook on Data Processing Security Rulebook on the Content and Form of the act for performance of video surveillance Rulebook for amending the Rulebook on the Content and Form of the act for performance of video surveillance Rulebook on the content of the analysis of the goal, i.e. the goals for which the video surveillance is set up and the report of the periodic evaluation of the results achieved by the video surveillance system Rulebook on Data Transfer Rulebook on the Process for data protection impact assessment Rulebook on the form and content of the request for determining violation of provisions under the law on personal data protection Rulebook on the method of reporting personal data breach Rulebook on reporting personal data processing of high risk Decision on establishing standard contractual clauses for the transfer of personal data to third countries
MINISTRY OF JUSTICE CRIMINAL COURT PUBLIC PROSECUTOR'S OFFICE	Criminal Code
MINISTRY OF JUSTICE CRIMINAL COURT PUBLIC PROSECUTOR'S OFFICE	Law on Criminal Procedure
MINISTRY OF JUSTICE CIVIL COURT	Law on Civil Procedure
ADMINISTRATION AGENCY	Law on the General Administrative Procedure
MINISTRY OF JUSTICE	Law on Litigation

STATE STATISTISTICAL OFFICE	Law on State Statistics
[800-171]	NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020
[ISO27000]	ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary
[ISO27002]	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
[ISO27001]	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[ISO27005]	ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks
[ISO19011]	ISO 19011:2018 Guidelines for auditing management systems
[ISO17021]	ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
[ISO31000]	ISO 31000:2018 Risk management – Principles and guidelines
[ISO22301]	ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements
[ENISA-1]	ENISA Technical guidelines for implementation of minimum-security measures for Digital Service Providers, December 2016
[ENISA-2]	ENISA Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a, Version 2.0, October 2014
[FICIC]	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, April 16, 2018,