# REGULATION ON THE CONTENT AND WAY OF DOCUMENTING CYBER SECURITY MEASURES

Version 2.0
(Changed)

Approved by Order No. 10 date 02/14/2022 (Amended by Order No. 184, Date 20.07.2023)

# ABOUT THE REGULATION AND NAECCS

This regulation aims to define the objectives and measures for the guarantee and operation of information systems and communication networks in Critical Information Infrastructure Operators (CIIO) and Important Information Infrastructure Operators (IIIO).

The regulation also defines the basic obligations and measures that CIIO and IIIO must undertake to minimize or prevent security incidents in communication networks and information systems, as well as defines standardization in the evaluation and reporting of security incidents and measures. The regulation lists 20 security objectives, divided into technical and organizational measures, based on international standards.

For each of the security objectives, more detailed security measures are listed, along with how to document them. Security measures and the way of documentation make up the list of minimum requirements for CIIO and IIIO.

## NAECCS

The object of the authority's activity is the supervision and implementation of the legislation in force in the field of cyber security, as well as the by-laws issued in its implementation.

NAECCS functions related to cyber security:

- defines cyber security measures;
- acts as the central point of contact at the national level for responsible operators in the field of cyber security and coordinates the work to resolve cyber security incidents;
- administers incident reports in the field of cyber security and ensures their storage and registration;
- provides methodical assistance and support to responsible operators in the field of cyber security;
- conducts analyzes of identified vulnerabilities in the field of Internet security;
- carries out awareness and education activities in the field of cyber security;
- acts in the capacity of the national CSIRT.
- coordinates its activities with security and defense institutions and cooperates with sectoral CSIRTs and international authorities in the field of cyber security, through joint agreements, in accordance with the legislation in force.

The authority and legislation are based on the models of ENISA which is the agency dedicated to achieving a high common level of cyber security in the EU.

# ABOUT ENISA

The European Union Agency for Cyber Security, ENISA, is the agency dedicated to achieving a common high level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, increases the reliability of ICT products, services and processes with cybersecurity certification schemes , collaborates with Member States and EU bodies and helps Europe prepare for tomorrow's cyber challenges. Through knowledge sharing, capacity building and awareness raising, the Agency works together with key actors to increase trust in the shared economy, to increase sustainability in the European Union's infrastructure and ultimately to keep Europe's society and citizens safe in the digital space. More information about ENISA and their work can be found at www.enisa.europa.eu

# TABLE OF CONTENTS

# 1. DEFINITIONS AND TERMINOLOGY

## 1.1 Definitions

### *Cybersecurity incidents*

"Cyber security incident" is defined as a cyber security event during which the security of information services or systems and communication networks is breached and has a real negative effect.

### *Security measures*

"Security measures" include the set of actions to increase the security of information in information systems and the availability and reliability of services and communication networks in cyberspace.

### *Critical information infrastructure*

"Critical information infrastructure" is the totality of networks and information systems, the violation or destruction of which would have a serious impact on the health, safety, and/or economic well-being of citizens and/or the effective functioning of the economy in the Republic of Albania. Critical assets should (obviously) be protected with priority.

### *Personnel and key personnel*

In this document the term "personnel" refers to employees, contractors and third party users. We use the term "key personnel" to refer to key roles in the organization that are related to network and information systems security. Operators are not all the same and job profiles are different, but especially roles such as CEO, CIO, CISO, business continuity manager and critical systems administrators would be included here.

### *Operator of critical information infrastructure (CIIO)*

“CIIO" is a legal entity, public or private, that administers the critical information infrastructure.

### *Operator of important information infrastructure (IIIO)*

“IIIO" is a public legal entity, which administers important information infrastructure.

# 2. INTRODUCTION

Operators of important information infrastructures and operators of critical information infrastructures must notify the National Authority on Electronic Certification and Cyber Security (the Authority) without delay of a cyber security incident that has had a significant impact on communication networks and systems of information.

In order to determine the importance of the impact of a cyber security incident, when possible, the following parameters should be taken into account in particular:

a) the number of users affected by the cyber security incident;
b) the duration of the cyber security incident;
c) the geographical extent of the area affected by the cyber security incident;
d) the degree to which the operation of communication networks and information systems is affected;
e) extent of impact on economic and social activities.

Where appropriate, the Authority should inform the competent authorities in other EU Member States and ENISA. The authority may inform the public or require operators to do so, when they judge that disclosure of the cyber security incident is in the public interest. Once a year, the Authority prepares a summary report on notifications received and actions taken in accordance with this paragraph.

The authority must ensure that in the event of a potential threat of a cyber security incident in the operators of important information infrastructures and the operators of critical information infrastructures must inform their users potentially affected by such a threat, about the measures or protections means possible that can be taken by users. Where possible, operators will also inform their users about the threat itself.

Operators of important information infrastructures and operators of critical information infrastructures shall immediately provide to the Authority:

a) Information necessary to assess the security of communications networks and their information systems, including documented security policies; if they have it and,
b) Submission of a cyber security audit report carried out by a qualified independent body or a competent authority and making these results available to the Authority; the cost of the audit will be paid by the operator.

The Authority provides, whenever requested, the assistance of a computer security incident response team ("CSIRT") designated in accordance with Law No. 2/2017 "On Cyber Security" and Article 9 of Directive (EU) 2016/1148 as related to matters included in the tasks of CSIRTs in accordance with point 2 of Annex I of that Directive.

**The authority, before the start of the control process (onsite) at CIIO and IIIO for the implementation of security measures, officially announces the infrastructure that will be controlled, for carrying out the process of scans of networks and information systems that have public access, for vulnerabilities of possible, in the framework of the verification of weaknesses and the implementation of technical cyber security measures.**

**The Authority, with the prior approval of the Operators of Critical and Important Information Infrastructures to be controlled, performs tests, simulations and cyber analysis (penetration test) of their networks and information systems.**

# 3. CYBER SECURITY MEASURES

## 3.1. STRUCTURE OF CYBER SECURITY MEASURES

This document lists 20 security measures derived from a set of international standards.

For each of the security objectives, more detailed security measures are listed which must be implemented by the operators to achieve the cyber security objective. For each of the security objectives we also list detailed documentation (evidence) that can show that the measures are in place.

Cyber security measures are grouped into **3 (three)** levels, as follows:

| SECURITY LEVEL | Description of security levels |
|---|---|
| **1 and 2** | Level 1 and 2 (Measures that are mandatory for CIIO and CIIO)<br>Low and medium level security measures should be implemented to achieve security objectives.<br>Documentation that low and medium level security measures have been implemented.<br>Low and medium level security measures to achieve the objective and an ad-hoc review of the implementation, after changes or incidents.<br>Documenting low- and medium-level security measures and documenting implementation reviews after changes or incidents. |
| **3** | Third level (Measures that are mandatory for CIIO)<br>High-level security measures and continuous monitoring of implementation, review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures.<br>Documenting the advanced implementation of security measures, documenting a structural review process and documenting proactive steps to improve the implementation of security measures. |

**NOTE:**

**The first and second level of security measures must be implemented and documented by Critical Information Infrastructure Operators, while the third level, including the first and second level, must be implemented and documented by Critical Information Infrastructure Operators.**

## 3.2. CYBER SECURITY MEASURES

Listed below are 20 low, medium and high level security measures (MS1, MS2, etc.), grouped into 2 categories (K1, K2).

For each category of security measures, the detailed security measures that must be implemented by the operators are listed, as well as the type of documents that will be taken into consideration.

Below the two categories of measures and the 20 measures for reference are listed:

## K1: ORGANIZATIONAL MEASURES

MS1: Security policy

1.1Information security policy

MS2: Risk management

MS3: Organizational security

MS4: Security requirements for third parties

MS5: Security of human resources and access of persons

5.1 Background Checks

5.2 Knowledge and training

5.3 Personnel changes

5.4 Treatment of violations

MS6: Asset Management

6.1 Asset Management

6.2 Operating procedures

6.3 Change management

MS7: Security events and cyber security incident management

7.1 Incident management procedures

7.2 Incident detection capability

7.3 Incident reporting and communication

MS8: Work continuity management

8.1 Service continuity strategy and contingency plans

8.2 Disaster recovery capacities

8.3 Use of contingency plans

MS9: Information security management

MS10: Control and audit

## K2 : TECHNICAL MEASURES

MS1: Physical security

1.1 Physical and environmental security

1.2 Security of supplies

MS2: Access authorization management

2.1 Threat Awareness

2.2 Informing users about threats

MS3: Cryptographic devices

3.1 Protecting critical security data

MS4: Cyber security event detection

MS5: Cybersecurity event tracking and assessment tools

5.1 Monitoring and recording policies

MS6: Protection of the integrity of communication networks

6.1 Network and information systems testing

6.1 Safety assessments

MS7: User identity verification

MS8: Activity of administrators and users

MS9: Security of applications

MS10: Security of industrial systems

# 4. ORGANIZATIONAL MEASURES

## 4.1. MS1: Security policy

Security policy covers security objectives related to the governance and management of security risks of communication networks and information systems.

### 4.1.1. Information security policy

Establish and maintain an appropriate information security policy.

| | | Security measures | | Documentation |
|---|---|---|---|---|
| 1 | a)<br>b) | Establish a high level of security policy that addresses the security of communication networks and information systems.<br>Make key personnel aware of the security policy. | i. ii. | Documented security policy, including communications networks and information systems within the scope, the critical assets that support them, and cybersecurity objectives.<br>Key personnel are aware of the security policy and its objectives. (interview) |
| 2 | c)<br>d)<br>e) | Define detailed information security policies for critical assets and work processes.<br>Make all personnel aware of the security policy and what it means for their work.<br>Review the security policy after incidents. | iii.<br>iv.<br>v. | Documented information security policies approved by senior management staff, including applicable law and regulations, accessible to staff.<br>Personnel are aware of the information security policy and what it means for their work (interview).<br>Reviewing comments or change logs for the policy. |
| 3 | f) | Periodically review information security policies and take into account breaches, exceptions, past incidents, previous tests/exercises and incidents affecting other (similar) operators in the sector. | vi.<br>vii.<br>viii. | Information security policies are updated and approved by senior management staff.<br>Documentation of policy exceptions, approved by relevant roles.<br>Documenting the review process, taking into account previous changes and incidents. |

## 4.2. MS2: Cyber risk management

Establish and maintain an appropriate risk management framework to identify and address cyber risks on communications networks and information systems.

| | | Security measures | | Documentation |
|---|---|---|---|---|
| 1 | a)<br>b) | Make a list of the main risks to the security of communication networks and information systems, taking into account the main threats to critical assets.<br>To make key personnel aware of the main risks and how they can be minimized. | i.<br>ii. | List of key risks described at a high level, including the underlying threat(s) and their potential impact on the security of communication networks and information systems.<br>Key personnel recognize key cyber risks (interview). |

| | | |
|---|---|---|
| 2 | c) Establishing a risk management methodology and/or tools based on industry standards.<br>d) Ensure that key personnel use risk management methodology and/or tools.<br>e) Review risk assessments after changes or cyber incidents.<br>f) Ensure residual risks are accepted by management staff.<br>g) Cyber insurance "Cyber Insurance" Insurance of computer systems and networks (information infrastructures) in order to avoid damage or loss/theft of information.<br>- Carry out cyber risk insurance of critical information infrastructure and important information infrastructure. | iii. Documented risk management methodology and/or tools.<br>iv. Guidance for staff on cyber risk assessment.<br>v. A list of cyber risks and updates/revisions documents.<br>vi. Review comments or change logs for risk assessments.<br>vii. Approval of management staff regarding accepted risks.<br>viii. Document the insurance of the infrastructure through an insurance policy in a local or foreign insurance company (one of the EU and/or NATO countries). |
| 3 | h) Periodic review of risk management methodology and/or tools, taking into account changes and previous incidents. | ix. Documentation of review process and updates to cyber risk management methodology and/or tools |

### 4.3. MS3 : Organizational security

Create and maintain an appropriate structure of security roles and responsibilities.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Assign security roles and responsibilities for personnel.<br>b) Ensure security roles are accessible in the event of cyber security incidents. | i. List of security roles and contact information.<br>ii. Information Security Management System Plan.<br>iii. Information security objectives.<br>iv. Human resources requirements for hiring personnel.<br>v. Personnel security clearance requirements.<br>vi. Document of termination of employment relations.<br>vii. User management and access document. |
| 2 | c) Personnel are formally appointed to security roles.<br>d) Make staff aware of security roles in your organization and when they should be contacted. | viii. Document of safety and use of technological equipment.<br>ix. Physical security document.<br>x. List of appointments and description of responsibilities and duties for security roles.<br>xi. Employee awareness and information materials explaining security roles and how/where they should be contacted. |

| | | |
|---|---|---|
| 3 | e) The structure of security roles and responsibilities is regularly reviewed and improved, based on changes and/or previous incidents. | xii. Updated documentation of security role task structure and responsibilities.<br>xiii. Documenting the review process, taking into account previous changes and incidents. |

## 4.4. MS4: Cyber Security Requirements for Third Parties

Establish and maintain a policy with security requirements for contracts with third parties to ensure that connections with third parties do not adversely affect the security of communications networks and information systems.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Include security requirements in contracts with third parties, including confidentiality and secure transfer of information. | i. Clear security requirements in contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centers, interconnection, shared equipment, etc.. |
| 2 | b) Establish a security policy for contracts with third parties.<br>c) Ensure that all procurement of services/products from third parties follow this policy.<br>d) Review security policy with third parties after cyber incidents or changes.<br>e) Require specific security standards in third-party supplier processes during procurement.<br>f) Mitigate/reduce residual risks not addressed by third parties. | ii. To document the security policy for contracts with third parties.<br>iii. List of contracts with third parties.<br>iv. Third-party service contracts contain security requirements, in accordance with procurement manuals/procedures.<br>v. Reviewing comments or changing policy logs.<br>vi. Contracts with equipment suppliers contain requirements that you adhere to security best practices and industry standards.<br>vii. The remaining risks as a result of dependence on third parties are listed and reduced. |
| 3 | g) Keep track/records of cyber security incidents related to or caused by third parties.<br>h) Periodically review and update the security policy for third parties at regular intervals, taking into consideration previous incidents, changes, etc. | viii. List of cyber security incidents related to or caused by engagement with third parties.<br>ix. Documenting the policy review process. |

## 4.5. MS5 : Security of human resources and access of persons

Security of human resources and access of persons covers security objectives related to personnel.

**4.5.1. Background checks** Conduct appropriate background checks of personnel for their duties and responsibilities.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Check professional references of key personnel (system administrators, security officers, guards, etc.). | i. Documentation of professional reference checks of key personnel. |

| | | |
|---|---|---|
| 2 | b) Conduct background checks/examinations for key personnel, when necessary and when legally permitted.<br>c) Establish a policy and procedure for background checks. | ii. Policy and procedure for background checks.<br>iii. Instructions for staff on when/how to perform background checks. |
| 3 | d) Review and update policies/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents. | iv. Reviewing comments or changing policy/procedure logs. |

## 4.5.2. Cyber security knowledge and training

Ensure that personnel have sufficient knowledge and appropriate periodic cyber security training.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Training and necessary materials for cyber security issues should be provided to key personnel. | i. Key personnel have attended cyber security training and have sufficient cyber security knowledge (interview). |
| 2 | b) Implement a training program, ensuring that key personnel have sufficient and up-to-date knowledge of cyber security.<br>c) Organize training and awareness sessions for staff on cyber security topics that are important to your entity. | ii. Personnel have participated in awareness sessions on cyber security topics.<br>iii. Documented program for staff skills training on cyber security, including objectives for different roles and how to achieve them (for example, training, awareness raising, etc.). |
| 3 | d) Periodically review and update the training program, taking into account changes and previous incidents.<br>e) Test staff's knowledge of cyber security. | iv. Updated cyber security awareness and training program.<br>v. Results of personnel tests on cyber security knowledge.<br>vi. Review comments or change logs. |

## 4.5.3. Personnel changes

Create and maintain a process for changes in their roles and responsibilities.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) After changes in personnel, revoke access rights, badges, equipment, etc., if they are no longer needed or allowed.<br>b) Inform and train new staff on applicable policies and procedures. | i. A document that personnel changes are followed by the revocation of access rights, badges, equipment, etc.<br>ii. A document that new personnel have been informed and trained about the policies and procedures in force. |

| | | |
|---|---|---|
| 2 | c) Implement policies/procedures on personnel changes, considering timely revocation of access rights, badges and equipment.<br>d) Implementation of policies/procedures for education and training of personnel in new roles. | iii. Documenting the process for personnel changes, including responsibilities for change management, description of rights of access and ownership of assets by role, procedures for informing and training personnel in new roles.<br>iv. Documentation that personnel changes are carried out according to procedures and that access rights are updated in a timely manner (eg checklists). |
| 3 | e) Periodically check that policies/procedures are effective.<br>f) Review and evaluate policies/procedures on personnel changes, taking into consideration previous changes or incidents. | v. Documentation of access rights controls etc.<br>vi. Updated policies/procedures for managing personnel changes.<br>vii. Review comments or edit logs. |

### 4.5.4. Treatment of violations

Establish and maintain a disciplinary process for personnel who violate security policies and have a broader process that covers cybersecurity incidents caused by personnel violations.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Personnel are responsible for cybersecurity incidents caused by policy violations, for example through the employment contract. | i. Personnel rules, including responsibilities, code of conduct, policy violations, etc., possibly as part of employment contracts. |
| 2 | b) Establish procedures for policy violations by personnel. | ii. Documentation of procedures, including the types of violations that may be subject to disciplinary action and what disciplinary action should be taken. |
| 3 | c) Periodically review and update the disciplinary process, based on changes and previous incidents. | iii. Review comments or edit logs. |

## 4.6. MS6: : Asset management

This security measure covers asset management, operational procedures and change management.

### 4.6.1. Asset management

Establish and maintain asset management procedures and configuration controls in order to manage the availability of critical assets and the configurations of communications networks and information systems.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Identification of critical assets and configurations of critical systems. | i. List of critical assets and critical systems. The list should include all critical assets and critical systems of communication networks and information systems, operational and security assets, including relevant third-party assets. |

| | | |
|---|---|---|
| 2 | b) Implementation of policy/procedures for asset management and configuration control. | ii. Document policy/procedures for asset management, including roles and responsibilities, assets and configurations that are the subject of the policy, asset management objectives.<br>iii. An inventory or several asset inventories, containing critical assets and dependencies between assets.<br>iv. An inventory or several configuration control inventories, containing configurations of critical systems. |
| 3 | c) Periodic review and update of the asset management policy, based on changes and previous incidents. | v. Updated asset management policies/procedures, review comments and/or change logs.. |

## 4.6.2. Operating procedures

Establish and maintain operational procedures for the operation of critical communication networks and information systems by personnel.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Establish operational procedures and assign responsibilities for the operation of critical systems. | i. Documenting operational procedures and responsibilities for key networks and information systems. |
| 2 | b) Implement a systems operations policy to ensure all critical systems are operated and managed in accordance with established procedures. | ii. Documentation of policies for the operation of critical systems, including a topology of the network and information systems within the scope. |
| 3 | c) Review and update policies/procedures for the operation of critical systems, taking into account incidents and/or changes. | iii. Update policies/procedures for critical systems, review comments and/or change log changes. |

## 4.6.3. Change management

Të vendosen procedurat e menaxhimit të ndryshimeve për rrjetet kritike dhe sistemet e informacionit në mënyrë që të minimizohet mundësia e incidenteve kibernetike që vijnë nga ndryshimet.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) To follow predetermined methods or procedures when making changes to critical systems. | i. Documentation that describes the predetermined methods or procedures followed when changes are made to critical systems. |

| | | |
|---|---|---|
| 2 | b) Implement change management policies/procedures to ensure that changes to critical systems are always performed in a pre-defined manner.<br>c) Document change management procedures and record the procedural steps followed for each change. | ii. Documentation of change management policies/procedures, including systems subject to the policy, objectives, rollback procedures, etc..<br>iii. For each change, keep a report describing the steps and the result of the change. |
| 3 | d) Regularly review and update change management procedures, taking into account previous changes and incidents. | iv. Update change management procedures, review comments and/or change logs. |

## 4.7. MS7: Security events and cyber security incident management

Security events and cyber security incident management include cyber incident detection, response, reporting and communication.

### 4.7.1. Cyber security incident management procedures

Create and maintain procedures for managing cyber security incidents and forwarding them to relevant personnel (selection).

| Security measures | | Documentation |
|---|---|---|
| 1 | a) Ensure that personnel are ready and prepared to manage and handle cyber security incidents.<br>b) Keep records of all major cyber security incidents. | i. Personnel are familiar with how to handle cyber security incidents and when to escalate it.<br>ii. Inventory of major cyber incidents and for each, the impact, cause, actions taken and lessons learned. |
| 2 | c) Implementation of cyber security incident management policy/procedures. | iii. Cyber incident management policy/procedure, including, types of incidents that may occur, objectives, roles and responsibilities, detailed description, for the type of incident, how to manage the incident, when escalated to senior management staff ( eg CISO) etc. |
| 3 | d) Investigating major cyber incidents and drafting final incident reports, including actions taken and recommendations to reduce the likelihood of such incidents occurring in the future.<br>e) Evaluate cyber incident management policy/procedures based on previous incidents. | iv. Individual reports for handling major cyber incidents.<br>v. Updated cyber incident management policies/procedures, comments review and/or changed logs. |

### 4.7.2. Cyber incident reporting and communication

Establish and maintain appropriate cyber incident reporting and communication procedures, taking into account national legislation for reporting cyber incidents to governmental authorities.

| Security Measures | Documentation |
|---|---|

|  |  |  |
|---|---|---|
| 1 | a) Communicate and report current or past cyber incidents to third parties, customers and/or government authorities, when necessary. | i. Document previous cyber incident communications and reports. |
| 2 | b) Implement policies and procedures for communication and reporting of cyber incidents. | ii. Documentation of policies and procedures related to communication and reporting of cyber incidents, description of reasons/motives for communication or reporting (business, legal, etc.) types of incidents within the scope, required content of communications, notifications or reports, communication channels to be used, as well as the roles responsible for communication, notification and reporting.<br>iii. Templates for cyber incident reporting and communication. |
| 3 | c) Evaluate previous communications and cyber incident reports.<br>d) Review and update reporting and communication plans, based on changes and previous incidents. | iv. List of incident reports and previous incident communications.<br>v. Updated incident response policy and communications, review of comments and/or change logs. |

## 4.8. MS8: Work continuity management

“Business Continuity Management" covers continuity strategies and emergency plans to prevent major damage and natural or man-made disasters.

### 4.8.1. Service continuity strategy and contingency plans

Create and maintain emergency plans and a strategy to ensure the continuity of communication networks and information systems.

|  | Security measures | Documentation |
|---|---|---|
| 1 | a) Implement a service continuity strategy for communication networks and/or information systems. | i. Documented service continuity strategy, including recovery time for key services and processes. |
| 2 | b) Implement emergency/backup plans for critical systems.<br>c) Monitoring activities and implementing contingency plans, recording successful recovery attempts and failures.<br>d) Implement contingency plans for dependent and interdependent critical sectors and services. | ii. Contingency plans for critical systems, including clear steps and procedures for known threats, triggers for activation, steps and recovery times.<br>iii. The decision-making process for the activation of emergency plans.<br>iv. Documentation of activation and implementation of contingency plans, including decisions made, steps taken, full recovery time.<br>v. Mapping of critical sectors and essential and/or dependent services for the continuity of network and service operations and contingency plans to prevent impact on dependent and dependent sectors and services interdependent . |
| 3 | e) Periodic review and control of the service continuity strategy.<br>f) Review and control of emergency plans, based on changes and previous incidents. | vi. Updated continuity strategy and contingency plans, review feedback and/or change logs. |

### 4.8.2. Disaster recovery capacities

To create and maintain adequate capacities for the return to the normal state of communication networks and information systems in the event of natural or major disasters.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) To prepare for the return to normal state of information systems in the next potential disaster. | i. Measures taken to deal with disasters, such as "failover site" in other regions, remote backups of critical data. |
| 2 | b) Implement policies/procedures for deploying disaster recovery capacities.<br>c) Implement industry standard recovery capacities, or make them available from third parties (such as national emergency networks). | ii. Documented procedures/policies for deploying recovery capabilities, including a list of natural and/or major disasters that may affect information systems, and a list of capabilities (those from third parties but also internal).<br>iii. Implementation of industry standard capacities in case of disasters, such as mobile devices, mobile site, failover site etc.. |
| 3 | d) To create recovery capacities for the reduction of natural and major disasters.<br>e) To continuously check and update the capacities, taking into account the changes that occur, previous incidents, the results of tests and exercises. | iv. Recovery capacities, such as prevention and failover mechanisms to handle natural and/or major disasters.<br>v. Updated capacity documentation for the return to the normal state of the situation, review of comments and / or change of logs. |

### 4.8.3. Use of contingency plans

| | Masat e sigurisë | Dokumentimi |
|---|---|---|
| 1 | a) To monitor the compliance of standards with legal requirements.. | Raportet që përshkruainë rezultatet e monitorimit të<br>i. Reports describing the results of compliance monitoring. |

| | | |
|---|---|---|
| 2 | b) Implement policies/procedures for compliance monitoring and auditing. | ii. Documented policies/procedures for compliance monitoring and auditing, including (assets, processes, infrastructure), frequency, instructions on who will conduct audits (internal or external), relevant security policies that are subject to compliance monitoring and auditing, objectives and high level of alignment of monitoring and auditing compliance, models for audit reports.<br>iii. Detailed monitoring and audit plans, including planning high-level long-term objectives. |

Use and maintain policies for testing and exercising backup and emergency plans, in collaboration with third parties, when necessary.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Use and test backup and emergency plans to ensure that systems and processes work and that personnel are prepared in the event of major damage and emergencies. | i. Reports of previous backup and emergency plan exercises. |
| 2 | b) Implement a program to regularly exercise backup and emergency plans, using realistic scenarios that cover a range of different scenarios over time.<br>c) Ensure that the issues and lessons learned from these exercises are addressed by the responsible persons and update the relevant processes and systems accordingly. | ii. Using the program for backup and emergency plans, including types of emergencies, frequency, roles and responsibilities, models and procedures for conducting exercises, models for exercise reports.<br>iii. Reports on exercises and drills showing the implementation of emergency plans, including lessons learned from these exercises.<br>iv. Addressing by the responsible persons the problems and lessons learned from the previous exercises. |
| 3 | d) Reviewing and updating exercise plans, taking into account changes, previous incidents and contingencies not covered by the exercise program.<br>e) Involvement in exercises of suppliers and other third parties, such as business partners and customers. | v. Updating exercise plans, reviewing comments, and/or changing logs.<br>vi. Data from suppliers and other third parties involved in improving exercise scenarios. |

## 4.9. MS9: Information security management

Create and maintain a policy for monitoring compliance of standards with legal requirements

| | | |
|---|---|---|
| 3 | c) To evaluate policies/procedures for compliance and auditing.<br>d) Review and update compliance and audit policies/procedures, taking into account changes and past incidents. | iv. List of all compliance reports and audits.<br>v. Updated policy/procedures for compliance and auditing, review of comments, and/or change logs. |

## 4.10. MS10: Control and audit

| | Security measures | Documentation |
|---|---|---|
| 1 | a) To implement the monitoring of logs for information systems.<br>b) Implement event and systems monitoring policy.<br>c) Establish tools for monitoring information systems.<br>d) Establish tools to collect and store information systems logs. | i. ii. Performance evaluation procedure.<br>iii. Internal audit procedure.<br>Management review of information systems security management.<br>iv. v. vi. Internal audit report. Report of<br>management reviews.<br>Logs and monitoring reports of communication network and information systems.<br>vii. Documented policies for monitoring and events, including minimum requirements for monitoring and events, retention period, and overall retention objectives. |
| 2 | e) Review and update monitoring policies/procedures, taking into account changes and previous incidents. | viii. Documentation of monitoring and event policies / procedures, documented. |

# 5. TECHNICAL MEASURES

**5.1 MS1: Physical security** Physical security covers the physical and logical security of information networks/systems and equipment.

### 5.1.1. Physical and environmental security

Establish and maintain appropriate physical and environmental security of information networks/systems and equipment.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Prevent unauthorized physical access to equipment and infrastructure and establish appropriate environmental controls to protect assets against unauthorized access, theft, fire, flood, etc. | i. Basic implementation of physical security measures and environmental controls, such as door and cabinet locks, intruder alarm, fire alarms, fire extinguishers, etc. |
| 2 | b) Implementation of a policy for physical security measures and environmental controls.<br>c) Implementation of industry standards of physical and environmental controls.<br>d) Apply reinforced physical access controls to critical assets. | ii. Documented policy for physical security measures and environmental controls, including description of scoped equipment and systems.<br>iii. Physical and environmental controls, such as electronic access control and audit logs, segmentation of spaces according to authorized levels, automated fire extinguishers with halocarbon gases, etc.<br>iv. The policy includes a list of critical assets and reinforced physical controls to access these assets. |
| 3 | e) Evaluate the effectiveness of physical and environmental controls periodically.<br>f) Review and update the policy on physical security measures and environmental controls taking into account changes and previous | v. Updated policy on physical security measures and environmental controls.<br>vi. Documentation of environmental control assessment, review comments or change logs. |

|  |  |  |
|---|---|---|
|  | incidents. |  |

### 5.1.2. Security of supplies (equipment)

Establish and maintain adequate security of critical supplies (eg: electricity, fuel, cooling, etc)

| | | Security measures | Documentation |
|---|---|---|---|
| 1 | a) | To guarantee the safety of critical supplies. | i. Security of critical supplies is protected in a basic way, for example UPS and/or backup fuel is available. |
| 2 | b) | Implementation of a security policy critical supplies. | ii. Documented policy for the protection of critical supplies such as electricity, fuel, etc., describing the different types of supplies and the security measures that protect these supplies. |
| | c) | Implement industry standard security measures to protect critical supplies and support equipment (eg passive cooling, automatic restart after power failure, battery backup power, diesel generators, backup fuel, etc.). | iii. Documentation of industry standard measures to protect the security of critical supplies. |
| 3 | d) | Implementing advanced security measures to protect critical supplies (such as active cooling, UPS, sustainable power generators, SLAs with fuel distribution companies, redundant cooling and power backup systems). | iv. Documenting advanced measures to protect the security of critical supplies. |
| | e) | Review and update policies and procedures to regularly secure critical supplies, taking into account changes and past incidents. | v. Updated Critical Supplies and Support Equipment Provisioning Policy, review comments and/or changelogs. |

## 5.2. MS2: Access authorization management

Create and maintain appropriate (logical) access controls to access communications networks and information systems.

|  | Security measures | Documentation |
|---|---|---|
| 1 | a) Users and systems have unique IDs and are authenticated before accessing services or systems.<br>b) Implementing logical access control mechanisms for networks and information systems to allow only authorized use. | i. Access logs show unique identifiers for users and systems when access is granted or denied.<br>ii. An overview of authentication and access control methods for systems and users. |
| 2 | c) Implementing policies for protecting access to networks and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. | iii. Access control policy which includes description of roles, groups, access rights, procedures for granting and revoking access.<br>iv. Different types of authentication mechanisms for different types of access. |

|  |  |  |
|---|---|---|
|  | d) Choose the appropriate authentication mechanisms, depending on the type of access.<br>e) Monitor access to networks and information systems, have a process for approving exceptions and logging access violations.<br>b) Strengthen controls for remote access to critical network and information systems assets by third parties. | v. Log of violations and exceptions to access control policies approved by the security officer.<br>vi. The principles of least privileged and segregation of duties are documented and applied where possible.<br>vii. Remote access to critical assets by third parties is minimized and subject to strict access controls, including advanced authentication, authorization and audit controls, especially for privileged accounts. |
| 3 | g) Evaluating the effectiveness of access control policies and procedures and implementing verification of controls in access control mechanisms.<br>e) The access control policy and access control mechanisms are reviewed and where necessary corrected. | viii. Test reports (security) of access control mechanisms.<br>ix. Tools for detecting abnormal use of systems or abnormal behavior of systems (such as intrusion detection and anomaly detection systems).<br>x. Logs of intrusion detection and anomaly detection systems.<br>xi. Access control policy updates, review comments or log changes.<br>xii. Documented risk analysis on the recording and storage application.<br>xiii. Procedures to ensure that access controls are in place at all times and that they evolve along with the network. |

### 5.2.1. Cyber threat awareness

"Cyber threat awareness" covers security objectives related to "threat intelligence" and end-user awareness in order to share information regarding major security threats to communication networks and information systems.

#### 5.2.1.1 Threat intelligence

Establish and maintain a mechanism for monitoring and gathering information about relevant threats to the security of communication networks and information systems

|  | Security measures | Documentation |
|---|---|---|

|  |  |  |
|---|---|---|
| 1 | a) Informing end users of communication networks and information systems about cyber security threats that may affect them. | i.<br>ii. Security bulletin, a dedicated cyber threat information website, or another documented and tested mechanism for contacting end users in the event of significant threats.<br>Documented lists of best practices and security recommendations for end users to minimize typical risks (eg encryption, secure authentication, updates, backups, user awareness). |

|  | Security measures | Documentation |
|---|---|---|
| 1 | a) Carry out continuous monitoring of cyber threats | i.<br>Continuous monitoring of external threat intelligence sources (OSINT, commercial intelligence, security research) with a recorded log of significant threat events.<br>ii. Relevant informal and ad hoc sharing of "threat intelligence" with relevant organizations on a bilateral basis. |
| 2 | b) Implement the program i“threat intelligence”. | iii. Documented and implemented "threat intelligence" program that includes roles, responsibilities, procedures and mechanisms for gathering information related to significant threats and relevant preventive measures.<br>iv. The program also includes mechanisms for systematically sharing threat intelligence with relevant organizations on a bilateral and multilateral basis using a dedicated threat intelligence sharing platform (eg MISP).<br>v. Existence of an appropriate information logging scheme to facilitate the sharing of threat-sensitive information (eg TLP). |
| 3 | c) To review and update the "threat intelligence" program..<br>d) The "threat intelligence" program uses the latest "threat intelligence" systems”. | vi.vii<br>Updating the threat intelligence program, reviewing comments, and/or changing logs.<br>Using the threat intelligence platform (TIP) with the latest functionality (eg consolidation of threat intelligence mechanisms from different sources, automation, security analysis and integration with other security tools, etc.) |

### 5.2.1.2. Informing users about cyber security threats

Inform users about network and information systems cyber security threats that may affect end users and the measures they can take to protect the security of their systems.

| | | |
|---|---|---|
| 2 | b) Implementation of policy/procedures for continuous information of end users regarding security threats of communication network and information system that may affect them. | iii. Documented and implemented policy of contact with end users with defined roles and responsibilities, mechanisms and criteria for identifying significant threats and procedures, tools and methods for timely and appropriate information of end users.<br>iv. The policy includes mechanisms for identifying and disseminating recommendations and best practices to end users for minimizing specific threats. |
| 3 | c) Review and update policies/procedures for continuous information of end users on communication network and system security threats that may affect them. | v. Updated contact policy, reviewing comments, and/or changing logs. |

## 5.3. MS3: Cryptographic devices

Ensure adequate use of encryption to prevent and/or minimize the impact of cyber security incidents on users, communication networks and information systems.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) When it is appropriate to prevent and/or minimize the impact of cyber security incidents on users, networks and other services, to encrypt data during their storage and/or transmission through networks. | i. Description of the main data transferred (data flow), as well as the encryption protocols and algorithms used for each transfer.<br>ii. Description of justified exceptions and limitations in encryption implementation. |
| 2 | viii. Implementation of encryption policy.<br>ix. Use industry standard encryption algorithms, with corresponding recommended encryption key lengths. | iii. Documentation of encryption policies including details about cryptographic algorithms and associated cryptographic keys, according to international best practices and standards.<br>iv. Documentation of justified exceptions that provide rationale when data is not encrypted, including relevant impact assessment. |
| 3 | d) Reviewing and updating encryption policies.<br>e) Use advanced encryption algorithms. | v. Updated encryption policy, review comments and/or change logs.<br>vi. The encryption policy includes details on the advanced cryptographic protocols used. |

### 5.3.1 Protecting the security of critical data

Ensure that the cryptographic key and secret authentication information are adequately protected.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Ensure that the cryptographic key and authentication secret information (including the cryptographic key material used for authentication) are not disclosed or tampered with.<br>b) Access to private keys is controlled and monitored in strictly. | i. The cryptographic key and secret authentication information are protected using best security practices and standards for protection mechanisms (such as split knowledge and double checking, encryption, hashing, secure hardware, etc.).<br>ii. Description of mechanisms for controlling and monitoring access to private keys. |

| | | |
|---|---|---|
| 2 | c) Policy implementation for cryptographic key management.<br>d) Policy implementation for managing user passwords. | iii. Key management policy including roles, responsibilities and controls for the use, protection and lifetime of cryptographic keys throughout their life cycle, including access controls as well as backup and recovery of private keys.<br>iv. Policy for managing user passwords including processes, methods and techniques for more secure storage of user passwords using industry best practices. |
| 3 | e) Key management policy review and update.<br>f) Review and update of user password management policies. | v. Updated key management policy, review comments and/or change logs.<br>vi. Updated user password management policy, review of comments and/or change logs. |

## 5.4. MS4: Cyber security event detection

Create and maintain cyber security incident detection capabilities that identify incidents.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Establishing processes or systems for cyber incident detection. | i. Documented examples of previous incidents that have been detected and reported in a timely manner to the appropriate persons. |
| 2 | b) Implementation of systems and procedures based on recognized international standards for the detection of cyber incidents.<br>c) Implementation of systems and procedures for recording and timely delivery of incidents to the appropriate persons. | ii. Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, personnel security assistance, reports and advisories from Computer Emergency Response Teams (CERT), anomaly detection tools, etc. iii. Network Operations Centers (NOCs) and/or Security Operations Centers (SOCs) to provide transparency and effective network monitoring, to detect anomalies, identify and avoid threats. |
| 3 | d) Periodic review of systems and processes for detecting incidents and updating them taking into account changes and previous incidents.<br>e) Implementation of advanced systems and procedures for the detection of cyber security incidents. | iv. Updated documentation of cybersecurity incident detection systems and processes.<br>v. Documentation of the cybersecurity incident detection process review, feedback review and/or change logs.<br>vi. Use of advanced NOC/SOC solutions - e.g. SOAR (Security Orchestration, Automation and Response), providing integration with threat and vulnerability management, incident response, automation of security operations, etc. |

## 5.5. MS5: Cybersecurity Event Assessment Tracking Tools

Cybersecurity event assessment tracking tools include monitoring, testing and auditing of network and information systems and equipment.

### 5.5.1. Installation and registration policies

Create and maintain systems and functions for monitoring and recording relevant security events in critical networks and information systems.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) To implement monitoring and recording of critical systems. | i. Critical network and information systems monitoring logs and reports. |
| 2 | c) To implement the policy for registration and monitoring of critical systems.<br>d) Establish tools for monitoring critical systems.<br>e) Implement tools to collect and store logs of critical systems. | ii. Documented monitoring and recording policies, including minimum monitoring and recording requirements, retention period, general storage objectives, data monitoring and logs.<br>iii. Tools for system monitoring and log collection.<br>iv. List of monitored data and log files, in accordance with the policy. |
| 3 | f) Implement tools for automated grouping and review of monitored data and logs.<br>g) Reviewing and updating logs and monitoring policies/procedures, taking into account changes and previous incidents. | v. Tools to facilitate recording and structural analysis of monitoring and logs.<br>vi. Updated documentation of monitoring and logging policies/procedures, review comments and/or changed logs. |

## 5.6. MS6: Protection of the integrity of communication networks

Establish and maintain the integrity of networks and information systems and protect against viruses, code injections and other malware that may alter the functionality of the systems.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Ensuring that network and information systems software is not tampered with or altered, for example by using access controls and firewalls.<br>b) Check for malware on network (internal) and information systems. | i. Software and data on networks and information systems are protected using access controls, firewalls, encryption and signing.<br>ii. Malware detection systems are in place and up to date. |
| 2 | c) Implement industry-standard security measures, providing detailed protection against intrusions and changes to systems.<br>d) Apply consolidated software integrity, update and debug management controls for critical assets in virtualized networks. | iii. Documentation of how software and data protection is implemented in the network and information system.<br>iv. Tools for detecting abnormal use of systems or abnormal behavior of systems (such as intrusion detection and anomaly detection systems).<br>v. Logs of intrusion detection and anomaly detection systems.<br>vi. Adequate tools and processes to ensure software integrity when performing software updates and applying security patches to critical assets in virtualized networks. |
| 3 | e) Put advanced controls in place to protect the integrity of systems.<br>f) Evaluate and review the effectiveness of measures to protect the integrity of systems. | vii. Advanced controls to protect systems integrity, such as signature, tripwire, etc.<br>viii. Documenting the process for checking the logs of anomaly and intrusion detection systems. |

### 5.6.1. Testing of networks and information systems

Establish and maintain policies for testing networks and information systems, especially when connecting to new networks or systems.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) To test networks and information systems before their use and connection with existing systems. | i. Network and information systems testing reports, including testing after major changes or deployment of new systems. |
| 2 | b) Implement policies/procedures for network and information systems testing.<br>c) Implement tools for automated testing. | ii. Policies/procedures for network and information systems testing, including when to perform these tests, test plans, test cases, test reporting templates. |
| 3 | d) Review and update policies/procedures for testing, taking into account changes and previous incidents. | iii. List of test reports.<br>iv. Updated network and information systems testing policies/procedures, feedback review, and/or change log. |

### 5.6.2. Safety assessments

Establish and maintain an appropriate policy for network and information systems security assessment.

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Ensuring that critical systems undergo regular security scans and security tests, especially when introducing new systems and changes. | i. Reports from previous security scans and tests. |
| 2 | b) Implement security assessment and testing policies/procedures. | ii. Documented policy/procedures for security assessments and testing, including which assets, under what circumstances, type of security assessment and testing, frequency, approved parties (internal or external), levels of confidentiality for the assessment, results of testing and the objectives of security assessments and tests. |
| 3 | c) Evaluate the effectiveness of policies/procedures for security assessments and security testing.<br>d) Review and update policy/procedures for security assessments and testing, taking into account changes and past incidents. | iv. List of reports on security assessments and security testing.<br>iv. Follow-up reports on security assessments and testing.<br>v. Updated policies/procedures for security assessments and security testing, feedback review, and/or change logs. |

## 5.7. MS7: User identity verification

| | Security measures | Documentation |
|---|---|---|

| | | |
|---|---|---|
| 1 | a) To implement the monitoring of critical data.<br>b) Implement event policy and critical systems monitoring.<br>c) Establish tools for monitoring critical systems. | i. Critical network and information systems monitoring reports.<br>ii. Requirements for the verification of the image of users.<br>iii. Access Requests Document. |
| 2 | d) Establish tools to collect and store critical data logs. | iv. Documented policies for monitoring and events, including minimum requirements for monitoring and events, retention period, general retention objectives, data monitoring and logs. |

## 5.8. MS8: Activity of administrators and users

| | Security measures | Documentation |
|---|---|---|
| 1 | a) Assign safety roles and responsibilities to personnel.<br>b) Ensure that security roles are accessible in the event of cyber security incidents.<br>c) Officially appoint personnel to security roles.<br>d) Make staff aware of security roles in the organization and when to contact them. | i. List of appointments (CISO, DPO, etc.) and description of responsibilities and duties for security roles (CISO, DPO, etc).<br>ii. Awareness and briefing materials for staff explaining security roles and when/how they should be contacted.<br>iii. List of security positions (business continuity manager, etc.) |
| 2 | e) Regularly review the structure of security roles and responsibilities, as a result of changes and/or previous incidents. | iv. Documentation of the review process, and possible changes and incidents should be considered. |

## 5.9 MS9: Security of applications

| | Security measures | Documentation |
|---|---|---|
| 1 | a) To carry out security assessments of the web application by security personnel delegated or employed or contracted by the institution. All findings that have been deemed confidential must be shared with persons with a "need to know". Distribution of findings outside the institution is strictly prohibited, unless approved by superior. | i. Security Assessments Document. |
| 2 | b) Any relationships within the applications will be included in the evaluation unless explicitly limited. | ii. Security Assessments Document. |

## 5.10 MS10 Security of industrial systems

|  |  |  |
|---|---|---|
| 1 | a) Industrial systems control, including data surveillance control, systems control, and other control system configurations such as logic program control. | i. Industrial systems control update, threats and vulnerabilities.<br>ii. Update on risk management in industrial systems, recommended practices and architecture.<br>iii. Update on current activities in industrial systems security. |
|  | b) Handling unique performance, reliability and security requirements. | iv. Update on security capabilities and tools for industrial systems, additional alignment with other security standards and guidelines.<br>v. New standards and guidelines for industrial systems.<br>vi. Developing security policies, procedures, training and educational materials that specifically apply to IS.<br>vii. Considering security policies for industrial systems and procedures based on threat level. viii. Addressing security throughout the lifecycle of industrial systems from architectural design to installation procurement to system maintenance.<br>ix. Implementing a network topology for industrial systems that has multiple layers, with the most critical communications located at the most secure and reliable layer.<br>x. Design critical systems for degradation (part of tolerance) to prevent catastrophic events.<br>xi. Disable ports and services on unused SHKB devices after testing to ensure that this will not affect ICS operation.<br>xii. Limitation on physical access to network and equipment of industrial systems<br>xiii. Restricting user rights to only those needed to do the job (ie, setting up configuration-based access control for each key role) in industrial systems<br>xiv. Use of special authentication mechanisms and credentials for network users on industrial systems and corporate network (ie, network accounts industrial systems do not use corporate network user accounts). |

## ANNEX 1

## Additional technical measures

| | | | Implementation Deadline | |
|---|---|---|---|---|
| **Nr.** | **Minimum Security Measures** | **METHODOLOGY** | **Important Infrastructure** | **Critical Infrastructure** |
| **1** | Install network perimeter devices that perform deep traffic analysis based not only on access list rules but also on its behavior (Firewalls). | This measure refers to the improvement of the network perimeter. The network perimeter protected by access rule analysis techniques configured by the network administrator is inadequate and easily bypassed. Recent technological developments require the development of techniques based on the analysis of traffic behavior by integrating firewalls with IDS/IPS services. These types of firewalls are called Next Generation Firewalls, making an analysis from the 1st layer of the OSI architecture to its 5th layer, eliminating the possibility of traffic with unusual behavior. | 6 months | 3 months |
| **2** | Consider "High-Availability" schemes in "core-network" equipment at the perimeter level (firewall), at the routing level (L3) and packet switching (L2) and at the level of physical lines (L1). | High availability schemes here refer to the pyramid of devices at the network level, starting from the outer perimeter level to the inside of the local area network, called the LAN.<br>More concret:<br>1. Provision of two or more firewalls or routers in the Active-Passive (Fail-Over) or Active-Active (Load Balancing) model.<br>2. Switches in Active-Passive and Active-Active models<br>3. Internet and data provision from two or more different providers | 6 months | 3 months |
| **3** | Take measures to use data mirroring techniques (RAID 1/5/6/10) to avoid the loss of sensitive data. | All service data generated by your institution in the data at rest model, stored in storage devices configured with mirroring techniques known as RAID - Redundant Array Independent Disk in one of the following models: | 3 months | 1 month |

| | | | | |
|---|---|---|---|---|
| | | 1. RAID 1 - This would require a doubling of resources<br>2. RAID 5 - This would require the use of a minimum of three different physical drives for each configuration<br>3. RAID 6 - Like RAID 5 but also requires the presence of a Spare disk known as HOT Spare<br>4. RAID 1+0 - Like RAID 1 but doubles the speed of searching data in the storage, compared to the RAID 1 technique.<br><br>This template should be required for all services:<br>a. Provided by the institution itself<br>b. Hosted by third parties at your institution. | | |
| **4** | Take measures to avoid "Single Point of Failure" in your critical and important services | This point refers to the architecture of services.<br><br>Critical and important services should be located in two or more hosting environments that replicate data in real time. This architecture is called Active-Active.<br><br>Meanwhile this architecture relies on real-time data replication for:<br><br>a. Services that are hosted on one host are replicated with downtime = 0 on another host<br>b. Critical and important database should be replicated from one host to another host (RAID 1,5,6,10 techniques do NOT cover this requirement).<br>. | 6 months | 3 months |
| **5** | Apply traffic filters in case of remote access to hosts (employees/third parties/customers). | The remote access technique aims to provide service to another location.<br>This technique must be performed securely through encryption tunnels using techniques: | 12 months | 6 months |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | 1- IPSEC or SSL.<br>2- IPSEC tunnels must be configured using the IKEv2 format and at least symmetric encryption should be implemented using AES 256 algorithms and RSA 2048-bit asymmetric keys.<br>3- Meanwhile, remote accesses must be accompanied by:<br>a. Traffic fluctuation analysis<br>b. Authentikimi me 2FA<br>c. Implementation of zero-trust architecture. |  |  |
| **6** | Implement solutions that filter, monitor and block malicious traffic between Web applications and the Internet, Web Application Firewall (WAF). | Knowing that the most frequent attacks end up at the Application layer, such as those called OWASP, Next Generation Firewall protection techniques, regardless of doing Depth-Analysis, cannot filter and analyze traffic at the Session/Presentation and Application layer. In this case, the inclusion of an additional layer would bring better traffic filtering for those services that are accessible via the Web, called Web-Service. | 18 months | 12 months |
| **7** | Conduct traffic analysis at the "behaviour" level for end devices. | The protection of end systems by means of traditional anti-malware systems based only on "signatures" is very easily manipulated. The requirement to have these systems analyzing traffic behavior would be an added value and increase security in end systems such as Servers or employee end stations. We refer to these systems as EDR - Endpoint Detection and Response.<br>This type of system also controls files that are uploaded from the economic operator's own systems to another system anywhere.<br>It would be preferable to see the behavior in matrix form if XDR is installed, which collects all the EDR activities installed on the end systems. | 3 months | 1 month |

| | | | | |
|---|---|---|---|---|
| | | Look at the feature that analyzes traffic at the "behaviour" level for end devices. | | |
| **8** | To design the solution for user access management "Identity Access Management" to control the identity and privileges of users in real time according to the "zero-trust" principle. | The implementation of this measure is divided into two phases:<br>1- Setting up a central system for the administration of all configured users using LDAP techniques such as Windows Active Directory. These systems must be version 2016 and above, as they offer additional security features such as: SMB v3.2- Installation of a central Identity Access Management which verifies the identity level of each user and his rights relying on the 0-trust and 2 FA architecture. Modern IAMs have built-in special features, such as PAM (Privilege Access Management). It would be recommended to set up the Single Sign ON technique not only for privileged users but also for ordinary users.<br>This technique is planned to be designed for 3 months for critical infrastructures and up to 6 months for important infrastructures. Meanwhile, its implementation time can vary from 6 months to 18 months depending on the number of users and the infrastructure if it is critical or important.<br>1- If the number of users is <50 and the number of services is <100 -> Average implementation time varies from 6 months to 12 months for critical infrastructures and 12 months – 18 months for important infrastructures.<br>2- If the number of users is 51-150 and the number of integrated services is 101-500 -> The average time of | Design time 6 months<br>Implementation time 12-18 months for <50 users and the number of integrated services <100<br>Implementation time 15-24 months for 51-150 users and the number of integrated services 101-500 | Design time 3 months<br>Implementation time 6-12 months for <50 users and the number of integrated services <100<br>Implementation time 12-15 months for 51-150 users and the number of integrated services 101-500 |

| | | | | |
|---|---|---|---|---|
| | | Implementation varies from 12 months to 15 months for critical infrastructures and 15-24 months for important ones.<br>3- If the number of users is >150 and the number of integrated services is >500 -> The average implementation time varies from 15 months to 18 months for critical infrastructures and 18-24 months for important ones. | Implementation time 18-24 months for >150 users and the number of integrated services >500 | Implementation time 15-18 months for >150 users and the number of integrated services >500 |
| **9** | To implement an automated system for the management and filtering of logs in order to identify alerts in real time. | The automated system of logs brings an advantage in their management since the quantity offered is very high. Filtering logs and scheduling playbooks created by specialists in the Monitoring sector would make the role of these platforms more efficient.<br>Often times these platforms are integrated with SOAR techniques which provide automatic response to an incident known beforehand and not only (Some of them are equipped with artificial intelligence using the Learn by Doing technique).<br>In the case when the amount of logs is over 50GB/Day, it becomes difficult and inefficient to control them manually. Installing an automated system coupled with an integrated SOAR Artificial Intelligence system would increase the efficiency of services. | 12 months | 6 months |
| **10** | If you have a development department, perform software development testing (stage-ing) in an isolated environment separated from the production environment. | Development departments due to their job profile have unlimited testing rights and privileges. For this reason, these environments should be virtually isolated using network segmentation through the VLAN technique or, in the best case, with physical separation through the Air GAP technique.<br>VLAN techniques can be set up on layer 2/3 switches or by using firewalls and filtering traffic through access lists. | 6 months | 3 months |

| | | | | |
|---|---|---|---|---|
| | | This technique is not associated with additional costs.<br>Note, this methodology does not deal with the analysis for setting up the test environment, but only the segmentation of the network of the test environment and its isolation from the business environment. Its segmentation can be accomplished by non-default VLAN due to the vulnerability known as VLAN Hopping.<br>A test environment, if it does not exist, requires an analysis by the economic operator himself and varies based on the volume of tests to be performed. Their cost is highly variable as they must be taken into account:<br>a. The number of servers that will be set up in the test segment<br>b. Number of Operating Systems required<br>c. If you need one or more virtualization platforms<br>d. If one or more integrated database systems are needed.<br>e. If a separate Network with additional equipment for testing such as:<br>I. Firewalls<br>II. Manageable switches<br>III. Routers etc | | |
| **11** | Take measures to implement a system that controls the security parameters of an end system, not allowing the latter to be | Hardening end systems by strictly defining a baseline called "hardening" would make your end systems more secure on the internal network. | | |

| | | | | |
|---|---|---|---|---|
| | part of your network if these parameters are below the "baseline" level previously given by you? (System which checks the lack of patches, Anti-Virus updates, etc.). | The baseline can be as follows:<br>a. The system must be with the Latest Patch of Windows (If it is of the Microsoft family). Otherwise, it must notify the user and the Network Administrator every hour. If there are two patches not installed then the system cannot become part of the network.<br>b. The system must be with the latest Office Patch (If on-prem). Otherwise, it must notify the user and the Network Administrator every hour. If there are two patches not installed then the system cannot become part of the network.<br>c. The system must be with Anti Malware family with the latest patch. Otherwise, it must notify the user and the Network Administrator every hour. If there are two patches not installed then the system cannot become part of the network.<br>d. The system must have the local Firewall properly configured (there must be no permit any-any rules or open rdp ports (Remote Desktop)).<br>e. Must not have Operating System and/or End-Of Life Applications installed. This system does not become part of the network.<br>f. If there are unpatched applications, it should be notified every hour to the user and the Network Administrator. If there are two patches not installed then the system cannot become part of the network. | 12 months | 3 months |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | g. For privileged systems check Power Shell. If it is not necessary to enable it as 70% of malicious scripts use Power-Shell features.<br>h. The end system must have ports 25,110,135,137,138,139,444 blocked, as well as the range of ports 1024-49151 unless any port in this range is needed as it communicates with specified services).<br>For Windows operating systems, the automatic update technique called WSUS can be used. |  |  |
| **12** | Logically isolate (in different VLANs) Database and Web services (if they are hosted in your environment). | The Web Server is public and provides access to anyone. In the case when you have hosted the Web Server in the local environment, it must:<br>1- To be divided into different segments by means of VLAN technique<br>2- To be in the same environment but with strict rules defining<br>a. Only the IP of the Web Server to communicate with.<br>b. Doing reverse path forward to the Web Server to verify its presence.<br>c. Filtering of the requests it sends according to the protocol (SOAP or REST API) by adding a Filter between the Web Server and the Data Bases, which can be performed by means of EDR or another filter at Layer 7 | 3 months | 1 month |
| **13** | To take measures to raise DNS_SEC to avoid DNS_Amplification attack and DNS_Poisoning attack. | If the DNS Server is located locally in the internal environment of the Institution, then the recursiveness of any request initiated by the DNS configured on the user's computer towards the DNS Server could have two effects: | 3 month | 1 month |

| | | | | |
|---|---|---|---|---|
| | | 1- DNS Poisoning attack – Where user-initiated requests go to a C2 (Command & Control) server managed by a malicious.<br>2- DNS Amplification attack - Fake requests are generated to the DNS Server, which generates endless responses to the client, leading to a denial of service or DoS Attack. | | |
| **14** | To implement and test the Disaster Recovery Site for the most important and critical services. | Disaster Recovery is an opportunity to have some or all of the services provided by the Primary Site also in another country in another location which must have a significant distance from the primary site. Communication between Primary Site and Secondary Site can be live or periodically, depending on the institution itself<br>The second site can be:<br>Tier 1/2 Where there is a location with some critical services stored on off servers (Cold Space). The information in them should be thrown periodically according to the backup policies:<br>a. Daily Incremental Dump – No time consumption as it copies the most recent data to the Secondary Site<br>b. Weekly Differential Dump – Saves data on a weekly basis<br>c. Full Physical Dump – This type of volume-based backup should be done at least once every 6 months | 18 months | 12 months |

| | | | | |
|---|---|---|---|---|
| | | Techniques should be with Backup Lock Retention feature or Tape in WORM (Write Only Read Many) format to avoid Ransomware.<br>Tier ¾ Services, along with Employee Positions are defined on the secondary site (Hot Space)<br>In the meantime, it is advisable to perform an Integrity Check Data every 6 months, where the copied data is verified for its integrity using the sampling model.<br>The Cold Space technique has costs based on:<br>a. Setting up Servers necessary for setting up services<br>b. Installation of critical Services<br>c. Installation of Licenses for Critical Services<br>d. Elevation of the Server Room (Technological Carpet/Anti-fire/anti-theft sensors,<br>Cooling system)<br>**e.** Other additional facilities<br>The Hot Space technique has costs several times higher than Cold Space, as it requires the services to be in the status: UP & Running and their number can be almost the same as those in the Primary Site. Costs increase even more when TIER 4 is raised as the secondary site is a copy of the primary site including employee positioning.<br>Cost analyzes require a detailed project depending on the number of services/servers/users etc | | |

| | | | | |
|---|---|---|---|---|
| **15** | Take measures to replace or isolate the "End of Life" systems installed in your equipment. | This measure is divided into two sub-issues:<br>1- EOL Operating Systems installed on Servers<br>2- EOL Operating Systems installed on end users<br>There are two scalable solutions for each:<br>I. All EOL operating systems must be isolated to the designated VLAN/VLANs (other than the Default one). Regardless of where they are located they must be isolated from the rest of the network. Isolation means segmenting the network specifically so that these EOL devices/systems do not impact the rest of the infrastructure..<br>a. If < 10 Systems identified = 1 week<br>b. If 11-50 Systems are identified = 2 weeks<br>c. If 51-75 Systems are identified = 3 weeks<br>d. If 76-100 Systems are identified = 1 month<br>e. If >100 Systems are identified = 2 months<br>If the operator has only important services, all points from a-e have a time interval to be fulfilled by the economic operator, 2 times longer than the critical ones reflected in points a-e.<br>II. All EOL systems must be replaced with new systems. In cases where they are CORE Business, and it is a big challenge to replace them, the process of communication/tendering/development of these systems MUST begin immediately and periodically (every 1 month) informing NAECCS about the status of the system. If we refer only to operating systems of hosts (not servers) EOL should be: | 2 weeks – 4 months (Isolation of EOL endpoint systems depending on the number of Systems).<br>6-16 months (replacement of EOL systems for Core Systems).<br>2-16 months (Firmware upgrade)<br>2 years (Firmware replacement)<br>Note: Systems presupposes an Operating System, or installed applications. | 1 week – 2 months (Isolation of EOL endpoint systems depending on the number of Systems).<br>3-8 months (replacement of EOL systems for Core Systems).<br>1-8 months (Firmware upgrade)<br>1 year (Firmware replacement)<br>Note: Systems presupposes an Operating System, or installed applications. |

| | | | | |
|---|---|---|---|---|
| | | a. If < 10 Systems are identified = 3 months<br>b. If 11-50 Systems are identified = 4 months<br>c. If 51-75 Systems are identified = 5 months<br>d. If 76-100 Systems are identified = 6 months<br>e. If > 101 Systems are logged in = 8 months<br>If the operator has only important services, all points from a-e have a time interval to be fulfilled by the economic operator, 2 times longer than the critical ones reflected in points a-e<br>Note that another EOL element is hardware devices that have very old and highly vulnerable firmware. These types of platforms are the ones that have been around for more than 5 years.<br>In this type of platforms it should:<br>Identify and upgrade their firmware<br>a. If identified < 50 Hardware = 1 month<br>b. If 51-100 Hardware are identified = 2 months<br>c. If 101-200 Hardware are identified = 3 months<br>d. If 201-400 Hardware are identified = 4 months<br>e. If identified 401-600 Hardware = 6 months<br>f. If >600 Hardware are identified = 8 months<br>If the operator has only important services, all points from a-e have a time interval to be fulfilled by the economic operator, 2 times longer than the critical ones reflected in points a-e | | |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | In the case when it is impossible to replace them with new platforms (devices), for critical infrastructures the necessary time<br>= 1 year<br><br>For important infrastructures, this time is twice as long.<br><br>Costs for items 1 and 2 depend on:<br><br>a. The number of EOL systems of user end devices, associated with the applications that are installed on them (Licenses are part of).<br><br>b. Number of EOL systems on servers. Here the situation is more complicated because if the servers are connected to a Database, it may also be required to calculate the replacement of the Database if it is not interoperable with a new system (Licenses are also included).<br><br>c. The number of Core or Final hardware devices that would be replaced depending on the brand they would belong to. |  |  |
| **16** | To take measures for the identification and effective management of assets and to carry out risk assessment by recording:<br><br>-Time of use/Seniority<br>- The impact of C/I/A Confidentiality/Integrity/Availability<br>-Identified Vulnerabilities (CVEs) | Through this measure, a management of the institution's assets is required. Assets should be classified into those assets related to the data divided into three categories:<br>1- Data at Rest – Storage, HDD, SAN, NAS, SDD, USB, etc.<br>2- Data in Transit – Core Network equipment such as: Switches L2, L3, Routers, Firewalls, Bridges<br>3- Data Use – All Services and Systems set up | 6 months | 3 months |

| | | | | |
|---|---|---|---|---|
| | | The format of the asset inventory may be in the form:<br>Asset_Name/ Asset_Description/ Whom the asset affects (C, I or A)/ Age/Unique_Code/Risk<br>These assets can be saved in an Excel/Word format or by a specific program. The latter would provide more flexibility and time efficiency, especially at the initial moment of building the asset table.<br>• All assets that affect confidentiality are those that, as a result of corruption, can violate the confidentiality of the data in them, such as: Active Directory, IAM appliance, eg ISE, LDAP Server in Linux, RADIUS Server, etc.<br>• All the assets that affect the integrity of the data are those that, as a result of the risk that may appear, can corrupt the transmitted data, such as: Devices that are set up IPSEC VPN Site (Firewalls)<br>• All assets that provide services only at a single point affect Availability (See requirement 2) | | |
| **17** | To draw up detailed plans and procedures for the management of cyber incidents. | Cyber incidents in the institution must be accompanied:<br>1- Incident Policy which is checked at least once a year<br>2- Procedurat dhe Rekordet e Incidenteve të ndodhura<br>Procedures and Records of Occurred Incidents: | 3 months | 1 months |

| | | | | |
|---|---|---|---|---|
| | | Name of Incident/ Asset affected/ Time/ Duration/ Person who discovered it/ Persons who reported/ Cause of incident/ Risk affected/ Controls to improve the situation/ Risk reassessment after resolution/ Comments<br>The cyber incident plan is based on the ISO standard, Annex A16. NAECCS, for its part, is renewing its plan<br>existing cyber incidents to cyber crisis, Therefore all critical infrastructures will be made aware soon. | | |
| **18** | Take measures to isolate the wireless network from the rest of the network. | If you have a Wireless network it should:<br>1- Be isolated from the institution's internal network with Air GAP or through segmentation using PrivateVLAN.<br>2- Its authentication should be through the RADIUS/TACACS technique | 12 months | 3 months |
| **19** | Conduct employee awareness campaigns regarding cyber security and the most frequent attacks such as Phishing etc. | Awareness should be raised about cyber hygiene. Employees should be briefed in small groups by information security staff periodically (at least monthly) Keep records of each employee's performance and evaluate.<br>Some of the topics may be as follows:<br>• Beware of Phishing/Smishing/Vishing/Whaling/Spear Phishing attacks<br>• Beware of Screen policy – Exit by turning off the monitor<br>• Caution when using USB devices<br>• Classification of documentation<br>• Flow of notification of an incident according to the plan written in point 17 | 6 months | 3 months |

| | | | | |
|---|---|---|---|---|
| | | • Setting long passwords and not related to specific names<br>• Beware of Social Engineering, etc. | | |
| **20** | Conduct tests to assess the security of applications and networks (penetration test) and draw up a plan for dealing with identified problems. | Penetration testing for the institution must be performed by a third party in two stages:<br>1- Black Box Penetration Testing – 1 time in 6 months<br>2- Full White Box Penetration Testing – 1 time per year<br><br>This type of testing must be done for all services provided by the institution. In the case of services hosted by third parties, but not provided by the institution, only the External Black Box test should be performed, but first by notifying the institution that hosted this service.<br><br>If the service hosted by a third party communicates with other services of the institution itself, then this third party is obliged to follow points 1 and 2 and the costs according to the agreement may be covered by:<br><br>1- The third party<br>2- The Institution itself<br><br>Penetration testing costs depend on:<br>1- Scan Area<br>2- Penetration Testing Model: Black Box, Gray Box, White Box<br>3- The number of services to be tested<br>4- Type of service (Phishing/Exploit/Social Engineering, etc).. | 12 months | 6 months |

|  |  |  |  |  |
|---|---|---|---|---|
| **21** | Conduct internal or third-party information security checks/audits on your infrastructures. | The audit is about verifying the methodical and technical procedures in your institution. Controls determine how compliant your activity is with security standards such as ISO 27001, or NIST.<br>Audit can be performed:<br>1- From within the institution called Internal Audit (Simple Form).<br>2- Nga një palë e tretë e shoqëruar me një certifikatë (Forma e Avancuar) | 12 months | 6 months |
| **22** | Check if the Email system does not have anti-spoofing features configured: DMARC/SPF/DKIM | To avoid the possibility of receiving phishing emails it is necessary to have all three features configured in the email. | 6 months | 3 months |
| **23** | Check if there is a Web Service that operates on the http protocol | If a page is using the http protocol it is very easy to intercept as it transmits text information. The same is true when the site has expired certificates.<br>Also, web services must be configured so that they do not have opportunities for OWASP-10 attacks, such as:<br>http_flag=1, the page generation session should be dynamic, there should be a limit on the number of characters and their type in input forms, etc. | 3 months | 1 month |
| **24** | Check if the firewall has a White List of allowed IP addresses | By having the White List set up, it would be possible to allow only that group of IPs that belongs to the institutions/states that are hosted and to eliminate any other request. | 6 months | 3 months |
| **25** | Use a random password policy for local users/administrators (eg Microsoft's LAPS) | The password policy in the case of logging in as a local user must be generated randomly and used only once within a certain interval.<br>Also, in the case when a page is not used for a while (idle time), the password will be changed automatically - Screening Policy | 3 months | 1 month |
| **26** | Use the Data Leakage Prevention platform to prevent information leakage. | The DLP platform would avoid the leakage of classified information to unauthorized persons or sites, as every traffic and person using that information would be tagged. | 12 months | 6 months |

|  |  |  |  |  |
|---|---|---|---|---|
| **27** | To use the protection technique against DoS/DDoS attack | This will avoid the possibility of DoS/DDoS attacks against an institution as once such traffic is seen, the randomly generated traffic will be analyzed and avoided. Using AI would reduce the number of False-Positives | 12 months | 6 months |
| **28** | To use the technique of Port Security on Switches where the maximum number of MAC Addresses is 1 for simple users and a limited number for IT or Cyber Security experts. | This would eliminate the possibility of DoS attacks from within the institution or the possibility of unauthorized connection of a user within the economic operator's own LAN. | 3 months | 1 month |