Draft REGULATION

No._____, dated ____.____.2025

"ON ORGANIZATIONAL AND TECHNICAL MEASURES TO GUARANTEE THE SECURITY OF ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES"

Approved by Decision of the Steering Council (DSC/VKD) of AKEP, No. 24, dated 03.11.2025

Article 1
Purpose

This regulation establishes the obligation of undertakings operating for the provision of public electronic communications networks and/or services to take appropriate technical, organizational and proportionate measures to prevent and minimize the impact of security incidents on users of interconnected networks.

Article 2
Object

The regulation aims to determine:
a. The objectives and measures to guarantee the functioning of the network infrastructure and/or electronic communications services by undertakings providing access to public communications networks and/or public communications services, in respect of confidentiality, integrity and uninterrupted provision of services.
b. The basic obligations and measures that undertakings must take to minimize or prevent the occurrence of security incidents in electronic communications networks and/or services, and to report them if they occur.
c. The conditions that a security breach or incident must meet, in order for the entrepreneur's obligation to inform AKEP about this security breach or incident to arise.
d. Standardization in the assessment and reporting of security incidents and security measures undertaken by undertakings.
e. The manner and content of reporting security measures and security incidents to be submitted to AKEP.
f. The application of sanctions, administrative measures in the event that undertakings fail to comply with the obligations set out in this regulation.

Article 3
Scope

This regulation applies to undertakings providing public electronic communications networks and/or publicly available electronic communications services in the territory of the Republic of Albania.

Article 4
Legal basis

The Regulation is drafted in accordance with Law No. 54/2024 “On electronic communications in the Republic of Albania”.

Article 5
Definitions

The terms used in this Regulation shall have the same meaning as in Law No. 54/2024 “On electronic communications in the Republic of Albania”.

Article 6
Criteria for assessing the impact of security incidents

1. Undertakings are obliged to carry out an impact assessment of each security incident on public electronic communications networks and/or services, according to the criteria and assessment matrix presented in Annex 2 to this Regulation. The impact assessment table must be updated whenever there are significant changes in the main parameters of the incident.
2. In the final impact assessment, if at least one of the parameters of Annex 2 classifies the incident as having a high impact, then the incident is considered a high impact incident.
3. Within 30 (thirty) working days from the end of the security incident, the undertakings are obliged to submit to AKEP, a final assessment of the impact of the incident, which must contain verified data and measures taken to reduce the consequences.

Article 7
Measures to increase network security

1. In order to prevent and minimize the impact of security incidents, the undertakings of networks and public electronic communications services are obliged
a. To have internal security regulations, approved, published and regularly updated.
b. To prepare and implement a service continuity plan, which is activated immediately in the event of a security incident.
c. To publish on their website user guides on the most common security incidents, preventive measures and actions to be followed after the occurrence of incidents.
d. To appoint at least one authorized person responsible for monitoring the implementation of security obligations and for communicating with AKEP in case of incidents.
2. Taking into account the provisions of point 1, other detailed security measures are according to Annex 3, which is attached to this regulation.
3. To take protective measures regarding the personal data of users:
a. to ensure that personal data are accessible only by authorized personnel for specific, clearly defined and legitimate legal purposes;
b. to protect personal data that are stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and against unauthorised or unlawful storage, processing, access or disclosure;
c. to ensure the implementation of security policies regarding the processing of personal data.

4. Electronic communications undertakings shall take all necessary measures to ensure the full availability of voice communications services and internet access services. Undertakings providing access to a public electronic communications network may temporarily restrict or interrupt access to their services, without the consent of users, where this is necessary for the improvement, modernisation, maintenance, or in the event of faults or damage to the network.

Article 8
Obligations of undertakings to notify in the event of an incident

1. Electronic communications network and service undertakings shall be obliged to immediately notify AKEP and the authority responsible for cybersecurity of any incident that has a high or medium impact on the functioning of networks, systems and services, according to the form in Annex 1.
2. The incident may take one of the following forms:
i. Denial of service (DoS/DDoS)
ii. Compromise of Information Systems
iii. Unauthorized manipulation or modification of electronic data
iv. Malicious software under the direct control of the electronic communications undertaking (viruses, spyware, etc.)
3. Undertakings of public electronic communications networks and services are obliged to immediately inform their users of a specific risk:
a. on the manner in which the risk may be reduced by users, as well as the potential costs to be borne by the user where the occurrence of the risk is beyond the measures that the undertaking can take;
b. in the event of a breach of personal data that may adversely affect the data and privacy of the subscriber.
4. The notification must describe the nature of the personal data breach, the designation of a contact person so that the subscriber has as detailed information as possible.
5. In cases of failure to notify the subscriber by the undertaking, AKEP, based on the impact of the breach, requires the undertaking to fulfill the obligation related to the notification of the subscriber.
6. Undertakings shall keep records of personal data breaches, their impact and the regulatory measures taken, sufficient to enable the competent national authorities to verify compliance with the obligation to notify subscribers of the incident.
7. Undertakings shall inform AKEP and notify subscribers of service restrictions or interruptions.
a. at least 48 hours in advance, in the case of planned network improvement, modernization or maintenance works lasting more than 30 minutes;
b. as soon as possible, but in no case later than 48 hours after the occurrence of the restriction or interruption caused by network defects or damage, when the interruption or restriction simultaneously impacts a significant number of users.

8. Upon request of AKEP, the undertaking shall:
a. provides the information necessary to assess the security and integrity of services and networks, including documented security policies;
b. makes available the results of the security audit, carried out by a certified and independent body.
9. In the event of a security breach, or when the results of the audit under point 8/b show that sufficient security measures have not been taken, AKEP shall by decision, determine the measures and time limits within which the undertaking must take and implement such measures.

Article 9
AKEP's obligations

1. In relation to the protection of national security interests and ensuring the preservation of the integrity and security of public electronic communications networks, AKEP:
a. informs the authority responsible for cybersecurity in the Republic of Albania of all cybersecurity incidents and, where appropriate, informs the European Commission and ENISA in accordance with the provisions on data protection.
b. informs the public or requests providers to do so, when it determines that disclosure of the security incident is in the public interest.
c. exchanges information regarding the security breach with the European Commission and the European Union Agency for Cybersecurity (ENISA), as well as with the competent authorities of other countries, in accordance with the requirements of data protection law for international transfers.
d. cooperates with the authority responsible for personal data protection, to ensure the implementation of security policies regarding the processing of personal data.

Article 10
Reporting on security measures and audits

1. Electronic communications undertakings are obliged to submit to AKEP the information necessary for the assessment of the security of their networks and services, including documented security policies, 1 (one) time per year, no later than January for the previous year, according to the format set out in Annex 3 of this regulation.
2. After receiving the information, if AKEP determines that the reported data requires in-depth verifications, it has the right to request from undertakings that have generated annual revenues from electronic communications over 100,000,000 ALL in the previous year, the submission of a Security Audit Report carried out by an independent, certified body or by the competent state authority for cybersecurity
3. The cost of the security audit is in any case borne by the undertaking itself.
4. If it is determined that the security incident occurred due to structural weaknesses, and/or the audit report highlights insufficient security measures, AKEP shall, by decision, oblige the

entrepreneur to implement security measures, determining the minimum requirements according to Annex 3, and the concrete deadlines for their implementation, according to Annex 4.

Article 11
Reporting Security Incidents

1. Undertakings are obliged to notify AKEP and submit the form of Annex 1 and Annex 2, no later than 24 hours from the moment of the identification of the security incident, after a preliminary assessment of its impact. Notification is mandatory only if the incident is classified as having a medium or high impact.
2. The initial notification must contain at least the following data:
a. Assessment of the public communication networks or services that have been affected by the security incident;
b. The geographical area affected or potentially affected;
c. The segment of users affected and/or at risk by the incident;
d. A preliminary assessment of the cause or causes believed to have led to the incident.
e. An assessment of the recovery plan and measures taken up to the moment of reporting;
3. If, after the initial notification, there is a significant change in the reported data, the entrepreneur is obliged to immediately submit a new, updated notification to AKEP.
4. Within 10 working days from the occurrence of the security incident, undertakings are obliged to submit to AKEP a final notification, with complete and verified data, by completing the form in Annex 1 again, according to the requirements set out in point 2 of this article.
5. Notifications under this article shall be sent to AKEP, through the dedicated official address incidente.raportimi@akep.al and in written form to AKEP.
6. AKEP may request additional information on the security incident at any time, beyond the data specified in the form. For this reason, undertakings are obliged to retain all data related to the incident for a period of no less than 12 months, starting from the date of submission of the final notification.

Article 12
Administrative infringements

Violations of this regulation, when they do not constitute a criminal infringement, are considered administrative infringements and are punishable by a fine according to point 1, letter a/xii of article 184 of law no. 54/2024 “On electronic communications in the Republic of Albania”.

Article 13
Repeals

Regulation no. 37 dated 29.10.2015 “On technical and organizational measures to ensure the security and integrity of electronic communications networks and/or services” is repealed.

Article 14
Entry into force

This Regulation shall enter into force on the date of its approval by the AKEP Steering Council.

ANNEX 1 – Security Incident Reporting Form

Section	Field	Content / Description
I. Contact Information	Undertaking details	
	First and last name of the person responsible for handling security incidents and/or integrity breaches	
	Job position	
	Address	
	Phone / Email	
II. Description of the Security Incident and/or Integrity Breach	Type of incident	Describe the nature of the incident (e.g. DDoS, infrastructure outage, system compromise, etc.)
	Date and time of occurrence	
	Date and time of detection	
	Date and time of recovery	
	Affected service or network	
	Affected geographic area	
	Number of affected users	
	Duration of the incident	
	Preliminary cause of the incident	Describe the possible cause (e.g. technical error, attack, failure, etc.)
	Impact on network and services	o Low o Medium o High
	Immediate measures taken	Actions undertaken for recovery and impact minimization
	Planned preventive measures	
	Impact assessment	Completed according to Annex 2
III. Additional Information	Attached technical evidence	Logs, audit reports, screenshots, etc.

IV. Contact Representative	Name, position, date, and signature	

Instructions for completing and submitting the form:
• The form must be completed within 24 hours from the detection of the incident.
• Annex 2 (impact assessment) and any technical evidence must be attached.
• Documentation must be sent to incidente.raportimi@akep.al after being signed by the person responsible for cybersecurity.

ANNEX 2 – Security Impact Assessment

Parameter	Unit of Measurement / Description	Low Impact	Medium Impact	High Impact
Duration of disruption	Total time of service interruption or degradation	< 1 hour	1 – 6 hours	> 6 hours
Number of affected users	Absolute number or percentage of users impacted by the incident	≤ 0.2% of total or ≤ 1000 users	0.2 – 5% of total	≥ 5% or ≥ 1000 users
Geographic scope	Area where the effect of the incident was felt	< 5 km² (local area)	5 – 20 km² (regional area)	> 20 km² (national area)
Impact on network and services	Whether the incident affects critical public communications services	No impact	Limited / partial impact	Direct impact on critical services

ANNEX 3 – Cybersecurity Measures

Organizational Measures

Organizational cybersecurity measures are administrative and procedural actions undertaken by undertakings of critical and important information infrastructures. These include, among others, the separation of roles and responsibilities for security, drafting and approving security policies and procedures, cyber risk management, awareness and training of human resources, as well as establishing a dedicated organizational structure for cybersecurity.

A1: Security Policy

The security policy includes security objectives related to governance and risk management of communication networks and information systems.

Security Measure	Documentation / Implementation Verification
A. Establishment of a high-level policy approved by management, addressing the security of communication networks and critical infrastructures, with periodic review at least once a year or after any cybersecurity incident or major infrastructure change.	A1. Information Security Policy Approved document containing objectives, scope, and security principles. Version, approval date, etc. A2. Periodic Review Reports Evidence showing review dates and details of changes made.

A2: Cyber Risk Management

An appropriate risk management framework shall be created and implemented to identify and address risks to communication networks and information systems.

Security Measure	Documentation / Implementation Verification
A. Development of a cyber risk management methodology reviewed at least annually and/or after major infrastructure changes.	Evidence showing review dates and details of changes made.
B. Drafting a list of security risks considering main threats to critical assets, reviewed at least annually and/or after incidents or major changes.	B1. Risk Assessment List Including risks from third parties. B2. Notification to Management Decision taken regarding risk treatment. B3. Risk List Review Evidence Dates and changes made.
C. Drafting a plan for treatment of identified risks.	C1. Risk Treatment Plan Document C2. Updates to the Risk Treatment Plan

A3: Organizational Security

An appropriate structure of security roles and responsibilities shall be established and implemented.

Security Measure	Documentation / Implementation Verification
A. Assignment of roles and responsibilities for information security management.	A1. List of Security Roles Detailed responsibilities for each role (e.g. CISO, ISO, DPO, DBA, SYSADM, etc.). A2. Organizational Chart Showing hierarchy and links between security roles. A3. Contact List Names, positions, and contact details of responsible persons.

A4: Cybersecurity Requirements for Third Parties

A security policy with requirements for third-party contracts shall be established and implemented to ensure that third-party relationships do not negatively affect the security of communication networks and information systems.

Security Measure	Documentation / Implementation Verification
A. Establishment of a security policy for procurement/contracts with third parties, reviewed periodically at least once per year and/or after any cybersecurity incident or major infrastructure change.	A1. Security policy for procurement/contracts with third parties (version, publication date, approval). A2. Periodic review reports and changes implemented.
B. Inclusion of security requirements in third-party contracts, including confidentiality and secure information transfer.	B1. Clear security requirements in third-party contracts. B2. Confidentiality agreements for information protection with third parties.
C. Keeping records of cybersecurity incidents related to or caused by third parties.	C1. Register of third-party related cyber incidents (date, cause, impact, actions).

A5: Human Resources and Access Security

A policy for human resources security awareness and access control shall be established and implemented based on personnel-related security objectives.

Security Measure	Documentation / Implementation Verification
A. Establishment of a security policy for human resources.	A1. Human resources security policy covering all phases: pre-employment, during employment, disciplinary processes, and termination.

	A2. Integrity verification document for key personnel (criminal record certificate, references, certifications, CV, etc.). A3. Procedure for personal data protection.
B. Implementation of a cybersecurity training program (reviewed at least once per year).	B1. Detailed training program adapted to employee roles and responsibilities. B2. List of participants and training dates. B3. Evidence of awareness/training campaigns on common attacks such as phishing, malware, etc.
C. Training and informing new employees on current cybersecurity policies and procedures.	C1. Training evidence for new employees. C2. Signed forms acknowledging policies and procedures. C3. Signed confidentiality agreement forms (NDA – Non-Disclosure Agreement).
D. Testing employee cybersecurity knowledge at least once per year (or more often depending on incidents).	D1. Questionnaires and test results on employee cybersecurity awareness.

A6: Asset Management

Asset management procedures and configuration controls shall be established and implemented to ensure the availability of critical assets and the configurations of communication networks and information systems.

Security Measure	Documentation / Implementation Verification
A. Measures for identifying and effectively managing assets (at least once per year and/or after major infrastructure changes).	A1. Full IT asset inventory including category, serial number, IP address, location, age, and status. A2. Classification of asset impact based on confidentiality, integrity, and availability.
B. Establishment and implementation of asset management policies/procedures.	B1. Detailed policies/procedures including roles, responsibilities, scope, objectives, and asset destruction (review at least annually). B2. Detailed network and information system topology.
C. Measures for replacing or isolating end-of-life (EOL) systems.	C1. Evidence identifying EOL systems and replacement/isolation planning. C2. Evidence of replacement/isolation of assets reaching EOL. C3. System verification evidence.

D. Performing automatic/manual patch updates on endpoint systems and across IT/OT infrastructure.	D1. Patch management procedure including frequency, responsibilities, and records. D2. Verification of tools/systems and evidence.
E. Establishment and implementation of security controls for personal devices used to access infrastructure systems and data (BYOD).	E1. Policy/procedure for use of personal devices (telephone, laptop, tablets etc.) and inventory of authorized devices that will be used in intern infrastructure of systems and networks . E2. Evidence of minimum-security configurations according to policy.

A7: Cybersecurity Incident Management

Plans and procedures for managing cyber incidents shall be developed and implemented, including detection, response, reporting, and communication.

Security Measure	Documentation / Implementation Verification
A. Drafting detailed plans and procedures for cybersecurity incident management (reviewed at least once per year and/or after any incident or major infrastructure change).	A1. Cyber Incident Management Plan Document (version, date, approval). A2. Procedures for identification, classification, and handling of incidents (playbooks), and list of incident response team members.
B. Maintaining records of all cybersecurity incidents.	B1. Incident register including date, cause, impact, and corrective actions. B2. Individual incident training reports and lessons learned analyses.
C. Defining and implementing communication and reporting of cyber incidents with authorities, and notifying third parties and customers.	C1. Incident reporting forms for authorities as required by cybersecurity legislation. C2. Inventory of communications and reports.

A8: Change Management

Policies and processes for change management shall be defined and implemented through planning, assessment, approval, communication, implementation, and monitoring of infrastructure changes.

Security Measure	Documentation / Implementation Verification
A. Ensuring that every change in IT systems and processes within	A1. Change management policy (including description, date, responsibilities, expected

critical/important infrastructure is managed in a controlled and documented manner.	impact, implementation plan, etc.) reviewed at least once per year. A2. Change management procedure (steps from proposal to approval and implementation). A3. Request for Change (RFC) form.

A9: Business Continuity Management

Emergency plans and a clear strategy shall be established and implemented to ensure continuity of communication networks and information systems.

Security Measure	Documentation / Implementation Verification
A. Development and implementation of a Business Continuity Plan (BCP) to ensure continuous operation of critical processes in case of cyber incidents, natural disasters, or operational disruptions (reviewed at least annually and/or after incidents or major changes).	A1. Service continuity strategy policy including activation conditions, recovery time, crisis communication, incident scenarios, action plan, testing rules, etc. A2. Business Impact Analysis (BIA), identification of critical processes, and definition of Recovery Time/Priority Objectives (RTO/RPO). A3. Emergency contact list – information for crisis contact points.
B. Establishment of a backup policy/procedure (reviewed at least annually and/or after incidents or major changes).	B1. Backup policy/procedure document including frequency, types, data, and services. B2. List of performed backups and recovery/integrity testing reports.
C. Avoidance of Single Points of Failure in critical and important services.	C1. Technical verification of single points of failure. C2. Evidence of service redundancy.
D. Implementation of infrastructure according to High Availability (HA) service schemes.	D1. Infrastructure scheme document with HA availability, support levels (L1, L2, L3), and firewall perimeter.
E. Implementation of a second environment for disaster recovery and continuity of IT system operation after a cyber incident (DRS – Disaster Recovery Site).	E1. DRS strategy and detailed configurations (reviewed at least annually and/or after incidents or major changes). E2. Disaster Recovery Plan procedures for IT recovery and infrastructure (tasks, responsibilities, key systems/assets list). E3. Test reports of the disaster recovery environment (at least once per year and/or after incidents or major changes).

	E4. Verification and evidence.

A10: Legal Compliance Management

A policy for monitoring compliance of standards with legal requirements shall be established and implemented.

Security Measure	Documentation / Implementation Verification
A. Monitoring compliance of standards with legal requirements.	A1. Policy/procedure for monitoring compliance with standards and legal requirements. A2. List of applicable standards and legal requirements for the infrastructure. A3. Review of ISMS policies and procedures at least once per year and/or after incidents or major infrastructure changes.

A11: Control and Auditing

Policies and procedures for conducting internal and external controls and audits shall be established and implemented to monitor compliance and ensure continuous improvement of information security.

Security Measure	Documentation / Implementation Verification
A. Policy/procedure for internal information security audits and periodic review (at least once per year and/or after incidents or major changes).	A1. Audit policy/procedure document (version, date, approval by management).
B. Conducting internal or third-party audits for information security and critical systems (at least once per year and/or after incidents or major changes).	B1. Internal audit reports and deficiency treatment plan (date, methodology, results). B2. Third-party audit reports for information security. B3. List of corrective actions taken after audits and evidence of implementation.

Technical and Operational Measures

Technical cybersecurity measures are technological solutions and mechanisms that ensure the protection and integrity of communication networks and information systems. These include access control, authentication and authorization, data encryption, monitoring and logging of security events, protection against cyberattacks, and technologies for detection and prevention of cybersecurity incidents. Operational cybersecurity measures are the daily processes, practices, and activities carried out to ensure information security and stable operation of critical and important

systems, including incident management, service continuity, disaster recovery, change management, and reporting/communication with responsible authorities.

B1: Physical Security

Appropriate physical and environmental security of information networks/systems and equipment shall be established and implemented.

Security Measure	Documentation / Implementation Verification
A. Implementation of physical security measures and environmental controls.	A1. Evidence of implementation of physical security measures (locks, cabinets, electronic access control). A2. Audit logs of access to authorized spaces and alarms for unauthorized entry. A3. Operation and maintenance reports of alarm systems and fire extinguishers. A4. Ensuring segmentation of physical spaces into zones based on authorization levels, including a detailed topology and clear evacuation plan.
B. Implementation of a policy for physical security measures and environmental controls.	B1. Physical security and environmental controls policy document (version, date, approval, review).

B2: Access Authorization Management

Appropriate access authorization controls for communication networks and information systems shall be established and maintained.

Security Measure	Documentation / Implementation Verification
A. Implementation of access control and protection policies for networks and information systems (reviewed at least annually and/or after major infrastructure changes).	A1. Access policy document (roles, groups, rights, procedures for granting and revoking access). A2. Access rights granting form. A3. Access rights revocation form and asset return form. A4. Evidence of deletion of generic accounts and periodic access control reports.
B. Application of traffic filters for remote system access and encryption of traffic using secure protocols.	B1. Technical verification and evidence of traffic filtering and encryption.

C. Verification of firewall configuration with authorized/block lists (Whitelist/Blacklist) of allowed or blocked IP addresses.	C1. Verification and evidence of firewall configurations.
D. Use of random password management policies for users and local administrators.	D1. Password management policy document and evidence of implementation of solutions such as LAPS or similar technologies.
E. Establishment and implementation of an Identity and Access Management (IAM) solution to ensure security, authorization, and auditing of user activities in critical systems.	E1. Technical verification and evidence.
F. Implementation of a Privileged Access Management (PAM) solution.	F1. Technical verification and evidence.
G. Implementation of Zero Trust Network Access (ZTNA) security service.	G1. Technical verification and evidence.

B3: Cryptographic Devices

Sufficient use of encryption shall be ensured to prevent and/or minimize the impact of cybersecurity incidents on communication networks and information systems.

Security Measure	Documentation / Implementation Verification
A. Implementation of encryption policies, including details about cryptographic algorithms and keys.	A1. Encryption policy document including algorithms such as AES, RSA, ECC, TLS, IPSec, SSH, etc. A2. List of cryptographic keys (type, validity period, generation and storage methods).
B. Encryption of data (in transit and at rest).	B1. List of encryption configurations for data and applications (on-prem, hybrid, cloud). B2. Technical verification and evidence.

B4: Cybersecurity Incident Detection

Capabilities for detecting cybersecurity incidents shall be established and maintained.

Security Measure	Documentation / Implementation Verification
A. Implementation of an automated system for security information and event/incident management (SIEM – Security Information and Event Management).	A1. Technical verification and configuration evidence of the SIEM system, including alerting rules and log filtering for incident detection.

B5: Collection and Processing of Cyber Threat Intelligence

A mechanism for monitoring, collecting, and analyzing information related to cybersecurity threats in communication networks and information systems shall be established and maintained.

Security Measure	Documentation / Implementation Verification
A. Continuous monitoring of external cyber threat intelligence sources.	A1. Periodic reports from cyber threat intelligence monitoring tools. A2. List of sources used for threat information collection.
B. Implementation of a cyber threat intelligence program including roles, responsibilities, and procedures.	B1. Cyber threat intelligence program document (including role/responsibility structure). B2. Procedures for collection, processing, analysis, and dissemination of cyber threat information.

B6: Monitoring and Logging of Cybersecurity Events

Systems and functions for monitoring and logging security events in critical networks and information systems shall be established and maintained.

Security Measure	Documentation / Implementation Verification
A. Implementation of policies for monitoring and logging cybersecurity events.	A1. Policy document for monitoring and logging activities (minimum requirements, retention period, objectives, approval, updates).
B. Deployment of tools for collecting logs and activities from critical systems.	B1. List of implemented tools for collecting logs (log servers, etc.). B2. Technical verification and evidence.

B7: Protection of Communication Network Integrity

The integrity of networks and information systems shall be ensured and protected against viruses, code injections, and other malware that may alter system functionality.

Security Measure	Documentation / Implementation Verification
A. Installation of devices to monitor, control, and restrict inbound/outbound traffic using a Next Generation Firewall (NGFW).	A1. Technical verification of NGFW configuration. A2. Technical verification and evidence.
B. Monitoring, detection, and analysis of suspicious behavior on endpoint devices (computers, laptops, servers).	B1. Technical verification and evidence of traffic analysis.

C. Network segmentation into subnets at the micro-segmentation level.	C1. Technical verification and evidence of documented network topology.
D. Placement of computers and servers into different zones/subnets/VLANs with Access Control Lists based on the principle of least privilege.	D1. List of implemented VLANs and network subdivisions including ACLs. D2. Technical verification and evidence.
E. Isolation of the wireless network from the rest of the network.	E1. Technical verification and evidence of wireless isolation configuration.
F. Use of switch port security techniques to limit MAC addresses (1 for regular users, limited number for IT/security experts).	F1. Technical verification of switch configuration applying Port Security.
G. Implementation of hardening techniques and standards for all network devices.	G1. Hardening manual for devices (PC, server, router, firewall). G2. Technical verification and evidence.
H. Logical isolation of databases and web services (e.g., in separate VLANs).	H1. VLAN list and technical verification of logical isolation configuration.
I. Implementation of DNS_SEC to prevent DNS Amplification and DNS Poisoning.	I1. Technical verification and evidence.
J. Implementation of protection against DoS/DDoS attacks.	J1. Technical verification of DoS/DDoS protection mechanisms (rate limiting, WAF, anti-DDoS tools).
K. Implementation of a Network Access Control (NAC) solution/system for endpoint security parameter control.	K1. Procedure for defining minimum security baseline parameters. K2. Technical verification and evidence.

B8: User Access Management

Policies for password management and access granting shall be implemented according to Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) models. Active Directory (AD) shall be used to manage privileges and restrict unauthorized access.

Security Measure	Documentation / Implementation Verification
A. Implementation of user password management policies.	A1. Password management policy document (complexity, expiration period, periodic changes).
B. Access granting models (DAC, MAC, RBAC).	B1. Technical evidence of configurations and implemented system rules.

C. Management of user access and privileges through AD service.	C1. Technical verification and evidence of AD implementation (group structures, privileges, restrictions).
D. Ensuring data protection and limiting unauthorized access to information.	D1. Verification of Clean Desk policy implementation and automatic screen lock policy after idle time.
E. Implementation of Two-Factor Authentication (2FA) at application/web/mail/device level for all critical system users.	E1. Verification and evidence.

B9: Administrator Activity and Authentication

Administrator access shall be secured by implementing Multi-Factor Authentication (MFA) across applications, web, email, and devices. Data Loss Prevention (DLP) platforms shall be used to prevent unauthorized information leakage.

Security Measure	Documentation / Implementation Verification
A. Implementation of MFA for administrators at application/web/mail/device level.	A1. Verification and evidence of MFA implementation.
B. Use of DLP methods to identify and prevent unauthorized leakage of sensitive data outside the infrastructure.	B1. Verification of DLP implementation for sensitive data leakage prevention.

B10: Application Security

Application protection shall be ensured by performing Vulnerability Assessments (VA) and Penetration Testing, and addressing identified issues.

Security Measure	Documentation / Implementation Verification
A. Conducting VA testing for applications and IT networks and drafting a remediation plan (at least once per year and/or after incidents or major changes).	A1. Vulnerability assessment report and remediation plan.
B. Verification that web services operate using secure HTTPS protocol.	B1. Technical verification and evidence (screenshots, logs, documentation).
C. Configuration of anti-spoofing mechanisms: DMARC/SPF/DKIM in email systems.	C1. Technical verification and evidence of anti-spoofing implementation.
D. Performing software staging/testing in a dedicated environment separated from	D1. Evidence of dedicated testing environment separated from production.

production (if development department exists).	
E. Implementation of a Web Application Firewall (WAF) solution for filtering, monitoring, and blocking malicious traffic.	E1. Technical verification and evidence (screenshots, logs, detailed parameter documentation).
F. Implementation of Reverse Proxy between clients and backend servers.	F1. Verification and evidence of Reverse Proxy implementation on web servers.
G. Conducting penetration tests (Black, Gray, White) and drafting a remediation plan (at least annually and/or after incidents or major changes).	G1. Penetration test reports (black, grey, white) and remediation plan.

B11: Secure Software Development

Secure software development for critical or important infrastructures includes practices and measures that enable the design, development, testing, and deployment of highly secure software to protect infrastructures from cyberattacks.

Security Measure	Documentation / Implementation Verification
A. Implementation of a security procedure for software design and development (reviewed annually).	A1. Documentation of the security procedure for software design and/or development. A2. The procedure must be approved by senior management and reviewed periodically.
B. Control and monitoring of developer and software user access.	B1. The procedure shall include specifics such as authentication, authorization, and encryption methods for developers. B2. User rights and access to software must be clearly defined.
C. Maintaining history of changes/configurations/approvals of software source code development.	C1. Technical verification and evidence (screenshots, logs, detailed documentation).
D. Risk and security analysis of software before release into production.	D1. Reports of software risk/security analysis including third-party library dependencies.
E. Handling and documenting cybersecurity incidents related to software development.	E1. Audit reports and incident logs for software development.
F. Monitoring of the software source code repository.	F1. Monitoring reports of the software source code repository.
G. Establishment of encrypted connection between application and database.	G1. Technical verification and evidence (e.g., encryption code evidence).

H. Backup of source code and integrity testing of backups.	H1. Technical verification and evidence of backups and recovery testing.
I. Automation through CI/CD pipelines for continuous integration, development, testing, and deployment.	I1. Technical verification and visual evidence of CI/CD configuration and operation (screenshots, logs, documentation).

B12: Operational Technology (OT) Systems Security

Protection of operational technology systems shall be ensured by applying least privilege access, network segmentation, and encryption of critical protocols. Measures shall be implemented for access control, real-time monitoring, and protection against cyberattacks and malware.

Security Measure	Documentation / Implementation Verification
A. Application of least privilege access principle with RBAC, ACL traffic filtering, and disabling unnecessary services in critical OT systems.	A1. Technical verification and evidence.
B. Implementation of TLS/SSL and VPN for critical protocols (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	B1. Technical verification and evidence.
C. Implementation of Hot and Cold backup techniques for data preservation.	C1. Technical verification and evidence.
D. Implementation of a remote access management solution based on Zero Trust (ZTNA).	D1. Technical verification and evidence.
E. Controlled patch and configuration management, tested first in test environments.	E1. Technical verification and evidence.
F. Implementation of endpoint protection including detection, response, and isolation mechanisms based on signatures and behavior.	F1. Technical verification and evidence.
G. Hardening of OT devices such as PLC, RTU, HMI, SCADA, BMS, etc.	G1. Technical verification and evidence.
H. Separation of IT infrastructure from OT, ensuring dedicated services (AD, Antivirus, NextGen Firewall, SIEM) for OT.	H1. Technical verification and evidence.
I. Implementation of real-time monitoring of operational activities in OT systems,	I1. Technical verification and evidence.

including logging, analysis, and notification of events based on criticality.	

B13: Security of IoT (Internet of Things) Systems

Procedures for securing IoT devices shall be developed and implemented, including mechanisms that ensure integrity and confidentiality. Secure updates shall be applied and authentication keys shall be protected on IoT devices.

Security Measure	Documentation / Implementation Verification
A. Drafting, approval, implementation, and periodic review of procedures for IoT device and system security.	A1. Procedure for IoT device and system security.
B. IoT device security measures: - Definition of minimum hardware requirements. - Use of mechanisms ensuring integrity (tamper-proof) and confidentiality (Trusted Platform Module). - Application of secure operating system and firmware updates. - Ensuring authentication key security. - Performing traffic behavior analysis where applicable.	B1. Technical verification and evidence (screenshots, logs, detailed documentation).
C. Ensuring integrity and confidentiality of data transmitted between IoT devices: - Use of secure authentication certificates (IoT Hub or IoT Central devices). - Ensuring secure communication (TLS 1.2 or higher). - Securing IoT data during transmission and storage. - Clear definition of access controls (IoT Hub and IoT Central application). - Monitoring the security of IoT solutions.	C1. Technical verification and evidence (screenshots, logs, detailed documentation).

B14: Security in Cloud Services

Cloud service security includes measures and policies that ensure the protection of infrastructure data and services, including strong authentication, data encryption, and activity monitoring. These

measures aim to guarantee integrity, availability, confidentiality, and compliance with technical requirements and agreed Service Level Agreements (SLA).

Security Measure	Documentation / Implementation Verification
A. Establishment of a governance policy/procedure for Cloud services.	A1. Cloud security policy/procedure.
B. Inclusion of technical, organizational, and security requirements in SLAs with Cloud service providers.	B1. SLA document including key performance indicators, monitoring metrics, security, and recovery.
C. Implementation of strong authentication such as MFA for access to Cloud administration platforms and services.	C1. Verification and evidence of authentication implementation in Cloud.
D. Implementation of encryption mechanisms for data at rest and in transit.	D1. Technical verification and evidence.
E. Regular backup of critical and important Cloud services.	E1. Technical verification and evidence.
F. Activation of logs and monitoring of infrastructure activities in Cloud.	F1. Technical verification and evidence.
G. Implementation of a Cloud-based unified network and security architecture, using Secure Access Service Edge (SASE).	G1. Technical verification of SASE solution implementation. G2. Verification and evidence of SASE usage by users.

ANNEX 4 – Risk Level Categorization and Corrective Measures

This annex presents the risk assessment matrix based on the combination of the probability of an event occurring and its impact on the network, service, or critical assets.

	Impact				
	Very Low	Low	Medium	High	Very High

Propability	Very Low	1	2	3	4	5
	Low	2	4	6	8	10
	Medium	3	6	9	12	15
	High	4	8	12	16	20
	Very High	5	10	15	20	25

Based on the risk assessment, the table below presents the required timeframes for addressing identified gaps according to the risk level.

Risk Level	Treatment Time
1–5 (Very Low)	No treatment required
6–10 (Low)	No treatment required
11–15 (Medium)	Treatment required within 12 months
16–25 (High)	Treatment required within 6 months