REPUBLIKA E SHQIPËRISË

ELECTRONIC AND POSTAL COMMUNICATIONS AUTHORITY

Regulation

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

Approved by Decision of the Steering Council (DSC/VKD) no. 8, dated 13.03.2026

Article 1
Purpose

This Regulation lays down the obligations of undertakings operating in public electronic communications networks and/or services to implement appropriate technical, operational and organisational measures, proportionate to the risks posed to the security and integrity of such networks and services

The measures taken, taking into account the latest developments in technology, shall ensure a level of security appropriate to the identified risks and, in particular, shall prevent or minimise the impact of security incidents on end-users and on interconnected networks and services.

Article 2
Object

1. The Regulation aims to determine:

   a. Objectives and measures for guaranteeing the secure operation of the network infrastructure and/or electronic communications services, by undertakingss providing access to public electronic communications networks and/or services, ensuring the confidentiality, integrity and continuous availability of these networks/services.
   b. Obligations and basic measures that undertakings must take to prevent to prevent the occurrence of cybersecurity incidents in electronic communications networks and/or services, or to minimize their consequences, as well as to report them regularly when they occur.
   c. The conditions under which a security breach or incident is considered significant, in order to give rise to the obligation of the undertakings to inform AKEP and other competent authorities about this security breach or incident.
   d. Standardization of the assessments and reporting of security incidents, and security measures undertaken by undertakings, ensuring the use of a unique reporting methodology and format, according to the models adopted by AKEP (Annex 1 and Annex 2).
   e. The manner and content of the periodic reporting of security measures and security incidents, to be submitted by undertakings to AKEP.
   f. Administrative measures and sanctions applied in case undertakings do not fulfill the obligations provided in this Regulation, based on Article 184 of Law no. 54/2024.

Article 3
Scope of application

This regulation applies to all undertakings/operators that provide public electronic communications networks, or electronic communications services available to the public, within the territory of the Republic of Albania. The obligations of this regulation apply regardless of the technology or platform used, including providers of traditional telephony and internet services, to the extent determined by law, as well as providers of 5G networks.

Article 4
Legal basis

1. This Regulation has been drafted pursuant to Article 56 of Law No. 54/2024 "On Electronic Communications in the Republic of Albania"[1] and takes into account the obligations set out in Chapter VII, Articles 54, 148 and 157 of Law No. 54/2024, regarding the security of networks and services, the availability of services, the taking of technical and organizational protective measures.
2. The Regulation takes into account the standards of the EU Directive 2022/2555 (NIS2) which represents the European best practice in the field of cybersecurity as well as the provisions related to the protection of subscribers' personal data, based on the applicable legislation on personal data.

Article 5
Definitions

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

Article 6
Criteria for assessing the impact of security incidents

1. **Initial Impact Assessment:** Undertakings are obliged to conduct a preliminary/initial impact assessment of any security incident on their public electronic communications networks and/or services as soon as possible. This initial assessment is based on the criteria of Annex 2 of this Regulation, which provides an impact assessment matrix according to the parameters

[1] Law no. 54/2024 is aligned with Directive (EU) 2018/1972 of the European Parliament and of the Council, dated 11 December 2018 "On the establishment of the European Electronic Communications Code".

key ones such as: impact on critical services, duration of outage, number of affected users, geographical scope of impact, socio-economic impact of the incident, etc.

The classification of the incident as "low", "medium" or "high" impact, is done by referring to the thresholds set out in Annex 2.

2. **Classification of incidents:** At the end of the initial assessment, if according to Annex 2, the incident is classified with "medium" or "high" impact, then undertakings have the obligation to notify AKEP.
3. **Re-evaluation and final assessment:** Undertakings should update the impact assessment whenever new data or analysis on the incident emerges. Within 30 (thirty) calendar days from the occurrence of the security incident, the undertakings shall submit to AKEP, a final impact assessment, which includes the verified data, the full analysis of the cause(s) and the measures taken to reduce the consequences. This final report will be prepared according to the format of Annexes 1 and 2 and will serve as a basis for possible improvements of security measures by the operator.

Article 7

Measures to increase the security of networks and services

1. **Organizational measures and operational plans:** In order to prevent security incidents and minimize their impact, undertakings of networks and public electronic communications services are obliged to undertake the following organizational measures:

    a. **Adoption of an internal information security policy** by the management staff of the enterprise. The procedure should be written, published by the undertakings and communicated to all personnel, and reviewed and updated regularly (no less than 1 (one) time per year or after any significant security incident or major change in infrastructure). This policy includes the main security objectives, the scope (for the systems, devices, and data it covers), as well as the basic principles that must be adhered to (e.g. the principle of layered security, the principle of privacy by design, etc.).

    b. **Cyber Risk Management:** Establish and implement a documented cybersecurity risk management framework, aimed at identifying, assessing, and systematically addressing risks to networks and information systems. This includes: risk management methodology (e.g. standards followed, assessment criteria), drawing up a risk register with the main risks identified (including internal and external threats, as well as risks from third parties/suppliers), prioritizing risks according to their levels, and dealing with them (through avoidance, repulsion, risk transfer or acceptance).
    This process should be continuous: reviewed at least 1 (one) time per year and immediately after any significant incident or major change in systems.

    c. **Security organizational structure and responsibilities:** Clearly define the roles and responsibilities for information security management within the undertakings. This

means:

i. the appointment of at least one authorized person, at the appropriate managerial level, responsible for cyber security issues, who will also act as a contact point with AKEP, for security incidents and reports;

ii. the definition of other key roles (e.g. system administrators, physical security officers, personal data protection officers/officers (DPOs), etc.) and the security-related duties of each;

iii. formalizing these responsibilities in the undertakings's organizational chart and job descriptions.

d. **Staff training and awareness:** Undertake regular cyber training programs and awareness campaigns for all employees, especially those who have roles in information security or who operate critical systems. The training program should include basic security topics (such as the company's security policy, knowledge of phishing/uniformity, password management, incident reporting procedures) and be expanded by role (e.g. advanced technical training for network administrators). At least 1 (one) time per year a mandatory training session should be conducted for all staff, as well as additional training after incidents or when weaknesses in staff knowledge are identified.

e. **Policies on the monitoring of logs and protection of personal data:** To develop clear policies for monitoring systems and the use of logs, in a transparent manner towards employees and subscribers, insofar as these logs may constitute personal data. Users/subscribers and employees should be clearly and easily informed about what personal data may be processed within the framework of network security measures (e.g. traffic logs, communications monitoring, intrusion detection systems, etc.). Also, the undertakings must have a policy of storage of personal data obtained from these security measures, where the terms of storage of logs and other data are defined and documented, in accordance with the principle of limitation of the storage period.

f. **Service continuity and recovery planning:** Prepare and implement a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), which is activated immediately in the event of a major security incident. The continuity plan should identify critical services and processes, define strategies for their continued operation even under degradation conditions (e.g. use of backup systems, diverting traffic to alternative networks) and assign teams/roles responsible for each emergency scenario. The recovery plan should detail the procedures for restoring systems to normal after a crash or attack (e.g. backup restoration, server reconstruction, **disaster recovery site**, etc.). These plans should be tested periodically (e.g. with exercises or annual simulations) to ensure their effectiveness. *(approved BCP/DRP document; continuity/recovery test results and reports; list of critical systems and RTO/RPO for each.)*

g. **Supply chain security:** Operators need to develop policies and take concrete measures to ensure that suppliers and their technical partners meet cybersecurity requirements. This includes:

i. **risk assessment of key suppliers** of equipment and services (e.g. 5G network

equipment suppliers, cloud service providers used by the operator, etc.) taking into account elements such as: their security practices, country of origin, cybersecurity certifications (e.g. ISO 27001, certifications within European schemes), the history of known incidents and national/European risk assessments for them;

ii. **Contractual safety requirements**: safety must be included in contracts with third parties (e.g. their obligation to notify the operator of incidents affecting the service provided, their implementation of minimum standards, as well as allowing audits by the operator or authorities);

iii. **Supply chain controls**: The operator must apply technical controls to protect its systems from supplier vulnerabilities (e.g. special monitoring of supplied equipment/applications, network segmentation for third-party devices, verification of the integrity of updates coming from the supplier, etc.) In the case of 5G networks, the operator must comply with the measures adopted by the national authorities within the EU 5G Toolbox, not to use equipment from suppliers considered to be at high risk in critical parts of the network, according to the list approved by decision of the Council of Ministers, for this purpose.

iv. **Access control and identity management:** (Combines technical and organizational elements). The operator must establish strict policies for managing accounts and access to their systems. This includes the principle of minimal access (each user or process has only the access necessary for their task), credential management (strong passwords, periodic rotation, prohibition of the use of anonymous shared accounts), the use of multi-factor authentication, wherever possible, especially for privileged access and administration tools, and continuous monitoring of access logs, to detect unauthorized uses).

2. **Technical and operational measures:** In addition to the above organizational measures, undertakings are obliged to implement the detailed technical and operational measures set out in Annex 3, which is attached to this regulation. Annex 3 includes specific cybersecurity objectives and minimum measures to be implemented in areas such as: physical infrastructure security, logical access control, use of cryptographic devices and encryption, incident detection and response, event monitoring and log storage, system integrity (malware protection), continuous management of updates/vulnerabilities, etc. Operators should implement the measures of Annex 3 as the mandatory minimum, and aim for the highest levels of safety when their technical capacities and resources allow it (principle of continuous improvement).
3. **Protection of users' personal data:** In application of the principle of "security of processing" of personal data, undertakings are obliged to take measures

   protection of users' personal data by applying the principle of minimum access, in order to:

   a. Be accessible only by authorized personnel, for specific and clearly defined legal purposes (need-to-know principle). This is related to access control, confidential handling of information and signing confidentiality agreements by personnel.
   b. To be protected from destruction, loss, alteration, disclosure, or unauthorized,

accidental, or unlawful access (integrity and confidentiality). This means using encryption when storing and transmitting sensitive data, using pseudonymization or anonymization where possible, as well as secured backups.

c. To be processed according to the principle of "privacy by design and by default" – e.g. In the development or adoption of new systems, security and privacy protection should be integrated from the design phase. The requirements of this point come in accordance with the legislation on the protection of personal data, specifically Article 23 (Privacy by design/default) and Article 28 (security of processing) of this Law.

Article 8

Notification obligations of undertakings

1. Notification of AKEP on security incidents: undertakings have the obligation to immediately notify AKEP and the National Authority responsible for Cyber Security (NSA) of any security incident that occurs, which is classified as "medium" or "high" impact, according to Annex 2. The notification to AKEP shall be made without unnecessary delays, in accordance with the provisions of Article 11 of this Regulation.
2. Security incidents that are the subject of notification under point 1 of this article may manifest themselves in various forms, including but not limited to:

    a. Denial of service (DoS/DDoS): attacks or events that cause network or system overload and prevent the normal provision of service to the user.
    b. Compromise of information systems: unauthorized or compromise (hacking) access of the operator's servers, networks or databases, which violates their integrity, confidentiality or availability.
    c. Unauthorized interference with electronic data: altering, deleting or entering data into the operator's systems without authorization, causing damage to the service (e.g. manipulation of network configurations, injection of harmful codes, etc.).
    d. Malicious software (malware), on devices that are under the direct control of the undertakings – infection with viruses, spyware, ransomware or other forms of malware of the operator's systems, despite the fact that it may have occurred as a result of the actions of third parties.
    e. Serious technical failure, which causes an impact on services according to the criterion of point 1 of this article.

3. The undertakings has the obligation to notify affected and/or endangered subscribers, when:

    a. **There is an imminent cyber threat to users**, which may affect the service they receive (e.g. a major malware attack that spreads quickly and can affect users' devices). In these cases, the operator must communicate to users the measures or actions they can take to reduce the risk, e.g. instructions for updating software, changing passwords, not opening suspicious messages, etc. If addressing these measures requires costs (e.g. installing a particular antivirus), the operator must inform users who should cover these costs (if the risk comes out of the operator's control, the cost

may fall to the users themselves).

b. **A personal data breach has occurred**. In these cases, the undertakings, in addition to the notification made to the Office of the Commissioner for the Right to Information and Protection of Personal Data, within 72 hours, must notify the affected subscribers himself, when the violation may cause them harm (e.g. theft of credentials, financial data or sensitive information). The notification to subscribers must clearly describe the nature of the personal data breach, the possible consequences, the measures taken by the operator and advice to the subscriber for further protection (password change, contacting the bank, blocking the card, etc.). Also, the operator must inform the subscribers about the contact point (e-mail address) of the officer responsible for the protection of personal data, so that the subscriber has as detailed information as possible.

4. Notifying subscribers/users about the risks: AKEP, if after a comprehensive assessment of the high-impact security incident reported by the undertakings of electronic communications networks and services, comes to the conclusion that there is a particular risk, asks the undertakings to immediately notify the subscribers.
5. Content of the notice to subscribers: The notification to subscribers must be drafted in clear and plain language and include at least:
    i. a description of the nature of the personal data breach;
    ii. the e-mail address covering the position of the personal data protection officer at the undertakings;
    iii. a description of the measures taken or proposed by the undertakings to address the infringement;
    iv. Practical advice for the subscriber in order to reduce risks (e.g. changing passwords, beware of suspicious emails – depending on the type of breach). This information is intended to provide the subscriber with the most complete picture possible, so that he can take appropriate actions to protect against risk.
6. **Obligation to notify pursuant to an order of AKEP:** In case the undertakings fails (or decides) to notify subscribers about a serious breach of personal data, AKEP, based on the assessment of the impact of the breach, officially asks the undertakings to fulfill the obligation to notify subscribers. This provision ensures that subscribers are not left uninformed in cases of serious violations, even if the undertakings hesitates or assesses otherwise. AKEP's request will specify the deadline within which the operator must make the notification.
7. **Personal data breach log:** Undertakings must maintain an internal record of any data security breaches. This register must document the facts about the violation, its effects and the corrective measures taken. Its purpose is for the competent authorities (AKEP or the Commissioner's Office) to be able to verify the compliance of the undertakings with the notification obligations and the measures taken.
8. **Notification of service interruptions/restrictions:**

    a. Undertakings must inform AKEP about the limitation or interruption of the service:
        i. at least 48 hours in advance, in the case of works planned for the improvement,

modernization or maintenance of the network, which will last more than 30 minutes;

i. as soon as possible, but in no case later than 48 hours after the occurrence of the limitation or interruption caused by network faults or damages, when the interruption or limitation simultaneously impacts a significant number of users that is assessed as medium or high impact, according to Annex 2 of this Regulation.

b. Undertakings must notify affected subscribers of the limitation or interruptions of the service:

ii. at least 48 hours in advance, in the case of works planned for the improvement, modernization or maintenance of the network, which will last more than 30 minutes;

iii. as soon as possible, but in no case later than 48 hours after the occurrence of the limitation or interruption caused by defects or damages to the fixed network, when the interruption or limitation simultaneously impacts a significant number of users that is assessed as having a high impact, according to Annex 2 of this Regulation.

iv. Due to the nature of the service in the mobile network and the objective difficulties in the individual identification of the affected subscribers, the notification of subscribers according to point 7/b/, of this article, will be carried out in fulfillment of the principle of "best effort".

9. **Provision of information and audits at the request of AKEP:** At the request of AKEP, undertakings are obliged to:
   a. provide the necessary information required by AKEP to assess the security and integrity of their services and networks. This includes sending documented security policies, the results of risk assessments, the list of measures implemented, key security configurations, etc., according to the nature of the information being requested.
   b. make available the results of security audits carried out by an independent and certified body, or by the competent state body for cybersecurity, for their systems and networks. If an operator has carried out external audits, the relevant reports must be submitted to AKEP. In addition, the operator should facilitate the conduct of external audits initiated by AKEP itself or the national cyber authority, giving auditors access to documentation and systems, within legal limits. The cost of safety audits is covered by the undertakings himself, according to Article 56 of Law no. 54/2024.
10. **Measures ordered by AKEP** after incidents/audits: In case a serious security breach occurs, or when the results of an audit (according to point 9/b) show that the operator has not taken sufficient security measures, AKEP, by decision, determines the additional measures and the time limits within which the undertakings must implement those measures. These measures will be based on the minimum security requirements provided in Annex 3 of this Regulation and may include: technical improvements (e.g. further segmentation of the network, installation of additional intrusion detection systems), increase of human resources (e.g. hiring of security experts), specific trainings, or even operational limitations until the breaches are fixed. AKEP's decision will be reasoned and will set realistic deadlines for the fulfillment of new obligations by the undertakings.

Article 9

AKEP's liabilities

1. In the framework of protecting the interests of national security and guaranteeing the integrity and security of public electronic communications networks, AKEP fulfills the following obligations:
   a. **Coordination with the national cyber authority:** AKEP informs without delay the authority responsible for cyber security in the Republic of Albania, of all cybersecurity incidents that are reported to it and that may have a significant impact (according to the criteria of Article 6). This enables a unified national approach to the management of major incidents. On a case-by-case basis (e.g. incidents with cross-border impact or affecting other countries), AKEP also informs the European Commission and ENISA, in accordance with the legal provisions on data protection during international transfers.
   b. **Public Information:** When AKEP finds that public disclosure of a security incident is in the public interest (e.g. to raise awareness or prevent further spread of the effect), AKEP informs the public itself or asks undertakings to do so. In practice, this can be accomplished by issuing public announcements through the media, the official portal, social networks, etc., or by instructing operators to send notifications to their subscribers or the public. Before publishing the information, AKEP will consult with the affected operator to ensure that the notification does not reveal data that would violate further security or trade secrets.
   c. **International exchange of information:** AKEP exchanges information regarding security breaches with the European Commission, ENISA, as well as with counterpart authorities of other countries (especially European ones), when necessary. This is done in accordance with the requirements of the NIS Cooperation Group and other international mechanisms in which Albania participates. AKEP takes care that during this exchange the legal restrictions on the confidentiality of information and the protection of personal data are respected. The information shared may include the nature of the incident, the measures taken, but not details identifying individuals or trade secrets, except

      cases where otherwise required by law and by taking protective measures (e.g. confidentiality agreement between the authorities).
   d. **Notification of the Office of the Commissioner for Personal Data:** AKEP immediately notifies the Office of the Commissioner for the Right to Information and Protection of Personal Data, in cases where a network security incident is accompanied by a personal data breach. AKEP cooperates closely with this authority to ensure that undertakings have implemented security policies regarding the processing of personal data and have fulfilled the obligations of notifying the subjects of these data. This coordination ensures that the technical and privacy aspects of the incident are handled in a synchronized manner.

2. Points (a) to (d) of this article are in line with the supervisory role of AKEP, according to Article 56 of the Law on Electronic Communications and with the European best practices for regulatory authorities in the electronic communications sector.

Article 10

Reporting of security and audit measures

1. **Annual reporting of security measures:** Electronic communications undertakings are obliged to submit to AKEP, 1 (one) time per year, a comprehensive report on the security measures implemented and the security status of their networks and services. This annual report must be submitted no later than February of each year (covering the preceding calendar year) and drawn up in the format set out in Annex 3 of this Regulation.
2. **Independent Audit Report Requirement:** Electronic communications undertakings who meet one of the following conditions:

    a. They have realized annual income from electronic communications over 50,000,000 (fifty million) ALL;
    b. Have service contracts with one or several central or local government institutions or organizations;
    c. Have more than 2000 (two thousand) subscribers
    d. They have internet interconnection lines, so they bring wholesale internet to Albania

have the obligation to deposit with AKEP, one of the following documents:

    i. ISO 27001 Certificate, accompanied by the Certification Audit Report, carried out by an independent certified body;
    ii. Security Audit Report conducted by the competent state authority for cyber security.

Coverage of audit costs: The cost of security audit is borne by the undertakings himself in any case. The undertakings must contract at his own expense a qualified auditor (e.g. an audit firm with experience in the field of cyber security), or allow the competent state authority (e.g. audit team to

AKSK) to carry out an audit at a cost that can be billed to the undertakings according to the legislation.

3. **Post-audit corrective measures:** In case the audit results that the security incident has occurred due to structural weaknesses in the operator's systems, and/or the audit report highlights insufficient security measures, AKEP, after consulting with the national cyber authority, by decision obliges the undertakings to implement additional security measures, determining the minimum requirements to be fulfilled with reference to Annex 3 as well as the concrete deadlines for their implementation. AKEP will closely monitor the fulfillment of these measures and may request periodic evidence of

progress from the operator.

4. **Privacy during the audit**: During the security audit process (whether internal or external), undertakings are obliged to guarantee the pseudonymization or anonymization of personal data, to avoid unnecessary exposure of identifiable information, in accordance with the principles of personal data protection, in Article 23 "Privacy *by design and by default*") and Article 28 "Measures to ensure the security of processing" of the Law on Personal Data Protection). This means that auditors should, as far as possible, work with logs or datasets cleaned of sensitive data, unless their full analysis is necessary for the security assessment. Even in cases where personal data is to be reviewed, auditors are bound by the obligation of confidentiality and the undertakings must ensure that any audit report does not expose them in an unauthorized manner.

Article 11

Security incident reporting

1. Initial notification of the incident to AKEP: Undertakings are obliged to notify electronically, to AKEP, within 24 hours from the identification of the incident with the data available at the time of notification. This notification is mandatory only in case the incident is classified as "medium" or "high" impact. This notification should include:
   a. The date and time of the incident
   b. Affected Service
   c. The nature of the incident
   d. Preliminary impact of the incident
   e. Duration
2. Filing of Annex 1 and Annex 2, within 72 hours from the identification of the incident.
3. Updated notifications, of Annex 1 and 2, at any time, only if there is a significant change in the reported data;
4. Final reporting of the incident: Within 30 (thirty) calendar days from the identification of the security incident, undertakings are obliged to file Annex 1 and Annex 2 with the updated data.
5. When AKEP evaluate it reasonable for some of the high-impact incidents, undertakings should submit a report which should include, as follows:
   a. Executive summary: what happened and when, what impact it had (final statistics), what caused it and the measures taken;
   b. Root causes: detailed analysis of the technical/organizational cause of the incident (e.g. "an error in the configuration of BGP routers allowed a route hijacking attack" or "an employee sent a spear-phishing email that installed malware");
   c. Corrective and preventive measures: description of the measures taken for recovery (correction of the problem) and what measures will be taken to prevent a

similar incident from happening in the future (e.g. "we will implement two-factor authentication for remote access", "we will add 24/7 traffic monitoring", etc);

d. Detailed impact: the exact number of subscribers affected, the total duration of the service interruption, the volume of traffic lost, and any other consequences (e.g. estimated economic damage, equipment damage, etc.).
e. Public communications: if the operator has informed the subscribers or the public, describe the form and time when it was made (attaching copies of the announcements, if possible);
f. Institutional cooperation: mention whether other institutions have been involved or notified (e.g. The State Police for any criminal aspect, the authority responsible for cyber security, the Office of the Commissioner for Personal Data Protection, etc.).

6. **Method of submission of notifications:** Notifications according to this article are sent to AKEP, electronically to the dedicated official address: incidente.raportimi@akep.al. For submissions according to point 5 of this article, the notification, in addition to electronically, must also be filed officially with AKEP.
7. **Additional information**: AKEP may request additional information on a security incident at any time, beyond the data specified in the form. Undertakings are obliged to respond to these requests without delay, making available all relevant data. In this context, operators must store all data related to the incident (logs, investigative evidence, internal communications, etc.) for a period of not less than 12 months from the date of submission of the final notification. This is to enable AKEP (or other authorized authorities) to have the opportunity to carry out further analyses or ex-post inspections on the incident.
8. **Incidents involving personal data:** When a technical security incident has also involved the breach of personal data of users/subscribers, the undertakings is obliged to make a special notification to the Office of the Commissioner for the Right to Information and Protection of Personal Data, within 72 hours from the discovery of the data breach. This notification will contain the elements required in Article 29 of the Law "On Personal Data Protection". In his report to AKEP, the undertakings must confirm that he has made the notification to the Commissioner (by providing a ref. of the letter or email sent).
9. **Lack of additional responsibility from notification:** The act of reporting the incident to the authorities, according to the above obligations, does not automatically make the undertakings legally responsible for the content or consequences of the incident. The announcement is considered

   an act of good faith within compliance and will not be used to impose additional responsibilities on the undertakings beyond those provided for in the law. However, if subsequent investigations show breach of obligations or negligence on the part of the undertakings, the competent authorities may take punitive measures according to the legislation in force. This provision is intended to encourage swift and complete reporting of incidents, without fear that the reporting itself will be used against the reporter.

Article 12

Administrative infringements

Violations of this Regulation, when they do not constitute a criminal offense, are considered administrative infringements and are punishable by a fine according to the provisions of Article 184 of Law no. 54/2024 "On electronic communications in the Republic of Albania".

Article 13

Repeals

With the entry into force of this Regulation, Regulation no. 37, dated 29.10.2015 "On technical and organizational measures to guarantee the security and integrity of electronic communications networks and/or services", is repealed.

Article 14

Entry into force

This Regulation and the Annexes attached thereto, shall enter into force on the date of its approval by the Steering Council (DSC/VKD) of AKEP.

ANNEX 1 – Security Incident Form

Section	Field	Contents / Description
I. Contact Information	Undertakings Details	
	First and last name of the person responsible for handling security incidents and/or integrity breaches	
	Job Position	
	Address	
	Phone/e-mail	
II. Description of the security incident and/or breach of integrity	Type of incident	Describe the nature of the incident (e.g. DDoS, infrastructure outages, 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	○ Low ○ Average ○ High
	Immediate measures taken	Actions taken for recovery and impact minimization
	Planned preventive measures	
	Impact assessment	To be completed according to Annex 2
III. Additional Data	Attached technical evidence	(logs, audit report, screenshot, etc.)
IV. Representative for contact	Name, position, date and signature	

ANNEX 2 – Security Incident Impact Assessment

An incident is classified as High Impact if at least one of the following occurs:

1. **Critical services provided by institutions are affected as follows:**

- Hospitals and emergency services,
- Public institutions that provide critical services to the public
- Banking Sector
- Infrastructure such as energy and water, etc.

2. **Central system failure / domino effect risk:**

- Backbone/core failure,
- DNS/DHCP/AAA,
- Key international interconnection/peering,
- A defect that risks national spread.

If none of the above conditions are met, point scoring is used as in Table 1 below:

Criteria		Impact			
		Insensitive (=0)	Low (=1)	Average (=2)	High (=3)
1. Duration		30 min	30-120 min	2-6 h	> 6 h
2. Number of Users	Relatively in %	<1%	1-5%	5-20%	> 20%
	Absolutely	<1,000	1,000-10,000	10,000-100,000	> 100,000
3. Geographical Reach		Nje site/node	Municipality/City	Some counties/regions	National Team
4. Service Degradation Rate		Lightweight	Notable	Heavy	Total
5. Social/economic impact		No Impact	Restricted	Significant	Major

Table 1. Impact Assessment Criteria

The value for each Criterion in Table 1 will be as follows:

- Insensitive = 0
- Low = 1
- Average = 2
- High = 3

For the criterion of Number of Users, the highest value will be taken between the relative and absolute criterion.

The definition of the level of impact will be made according to the multiplication of the five criteria:

- Low Impact 0–5 points
- Medium Impact 6–10 points
- High Impact ≥11 points

ANNEX 3 – Cybersecurity Measures

Organizational Measures

Cybersecurity organizational measures are administrative and procedural actions, undertaken by operators of critical and important information infrastructures, including, among others, the allocation of roles and responsibilities for security, the design and adoption of security policies and procedures, cyber risk management, awareness raising and training of human resources, as well as the construction of a dedicated organizational structure for cybersecurity.

The fulfillment of the requirements of Annex A3 is done by formal self-declaration by the electronic communications undertakings, provided that the undertakings possess complete internal records and the documentation is available for inspection/audit by AKEP.

A1: Security Policy

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

Security measure	Implementation
A. Establish a high-level policy, approved by the management staff of the infrastructure, that addresses the security of communication networks and critical and important information systems and its periodic review. The review shall be done at least once a year or after any cybersecurity incident or after any major change in the Infrastructure.	A1. Information Security Policy Document approved by the management staff and containing the objectives, scope and principles of security in networks and information systems Version, date of approval, etc. A2. Periodic review reports Evidence showing the date of the revision and details of the changes made to the security policy.

A2: Cyber Risk Management

Establish and implement an appropriate risk management framework to identify and address risks to communication networks and information systems.

Security measure	Implementation
A. Creating a methodology for cyber risk management. Its revision should be done at least once a year and/or after any major changes in the infrastructure.	A1. Cyber risk management methodology document including version, date, and approval by management staff. A2. Periodic review reports and evidence showing the date of the review and details of the changes made to the risk management methodology.

B. Drawing up a list of risks to the security of communication networks and information systems, taking into account the main threats to critical assets. Its review should be done at least once a year and/or after any cybersecurity incident or after any major change in the Infrastructure.	B1. An assessment list of risks arising from various sources, including risks arising from third parties. B2. Notification of the management staff on the list of risks, as well as the decision taken for their treatment. B3. Revision of the list of risks and evidence showing the dates of the review, details of the changes made.
C. Establishing a plan for dealing with the identified risks.	C1. Risk management plan document. C2. Reflecting changes to the risk treatment plan.

A3: Organizational Security

Establish and implement an appropriate structure of security roles and responsibilities for information security management.

Security measure	Implementation
A. Assigning roles and responsibilities for information security management.	A1. List of security roles and detailed description of responsibilities for each role e.g CISO, ISO, DPO, DBA, SYSADM etc. A2. Organizational chart showing hierarchy and connections between security roles. A3. Contact list for persons responsible for information security (name, position, contact)
B. Clear policies for transparency of use and retention periods of personal data of logs and metadata	B1. "The Undertakings shall ensure that users and subscribers are informed in a clear, understandable and accessible manner about the extent to which the processing of personal data can be considered within the framework of network security measures (logs, traffic monitoring, systems, etc.). B2. "The undertakings determines and documents the terms of storage of personal data for the processing processes he develops in implementation of this regulation.

A4: Cybersecurity Requirements for Third Parties

Establish and implement a security policy for contracts with third parties to ensure that relations with third parties do not negatively affect the security of communication networks and information systems.

Any delegation of the processing of personal data to third parties is made on the basis of a special contract, in accordance with the legislation in force on the protection of personal data, where the objective, nature and purpose of the processing, the type of data, the categories of subjects, the technical and organizational security measures, as well as the obligations and responsibilities of the third party towards the undertakings are determined.

Security measure	Documentation / Verification of implementation
A. Establishing a security policy for supplies/contracts with third parties and reviewing it periodically. Minimum once a year and/or after any cybersecurity incident or after any major changes in infrastructure.	A1. Security policy for supplies/contracts with third parties (version, date of publication, approval). A2. Reports of the periodic review of the security policy and the changes made.
B. Incorporating security requirements into contracts with third parties, including confidentiality and secure transfer of information.	B1. Clear security requirements in contracts with third parties. B2. Confidentiality agreement for the storage of information with third parties.
C. Keeping tracks/records of cybersecurity incidents, related to or caused by the parties to the third	C1. Register of cyber incidents related to third parties (date, cause, impact, actions)

A5: Human resources security and access of persons

Establish and implement a policy on security and protection of personal data for human resources awareness, as well as access of persons, based on security objectives related to personnel.

Security measure	Implementation
A. Establishing a policy on security and protection of personal data for human resources.	A1. Security and personal data protection policy, for human resources (including all stages: before recruitment, during employment, disciplinary processes, at the end of the employment relationship). A2. Document of verification of the integrity of key personnel (proof of judicial status, references of previous jobs, certifications, CVs, etc.) A3. Procedure for the protection of personal data.
B. Implementation of a training program on cyber security and personal data protection (Minimum review once a year)	B1. Detailed training program, tailored to the roles and responsibilities of employees. B2. List of participants and training dates B3. Document on the implementation of awareness/training campaigns for employees regarding cyber security and the most frequent attacks such as "Phishing", "Malware" and for the protection of personal data, etc.
C. Informing and training new employees on the applicable cybersecurity policies and procedures	Q1. Evidence for training for new employees. Q2. Employee signed forms for recognizing policies and procedures. Q3. Non-Disclosure Agreement forms signed by employees.

A6: Asset Management

Establish and implement asset management procedures and configuration controls to ensure the availability of critical assets and configurations of communication networks and information systems.

Security measure	Implementation
A. Taking measures for the effective identification and management of assets. (Minimum 1 (one) time per year and/or after any major changes in the infrastructure	A1. The complete inventory of information technology assets including the asset category, no. series, internet protocol, location, seniority, status. A2. Inventory of impact, according to confidentiality, integrity, and availability.
B. Establishing and implementing policies/procedures for asset management.	A1. Detailed asset management policies/procedures, including roles and responsibilities, assets that are subject to this policy/procedure, asset management objectives, as well as asset destruction. (Review at least 1 (one) time per year and/or after any major changes to the infrastructure) A2. Detailed network and information systems topology
C. Taking measures to replace or isolate end-of-life systems ("EOL").	Q1. Document or evidence of identification of end-of-life systems (EOL) and planning for their replacement/isolation. Q2. Evidence of replacement/isolation of the asset, which has reached life cycle time (EOL). Q3. Verification of systems and evidence.
D. Perform automatic/manual updates ("patches") to the terminal systems and to the entire information technology (IT) and operational technology (OT) infrastructure.	Q1. Procedure for managing the implementation of updates (patches) for information technology (IT) and operational technology (OT) equipment and systems, including frequency, responsible, records. D2. Verification of systems/tools and evidence.
E. Define and implement security policies and controls for personal devices used to access infrastructure systems and data ("BYOD"), ensuring the protection of information and compliance with safety standards.	E1. Policy/procedure for the use of personal devices (phones, laptops, tablets, etc.), as well as an inventory of personal devices authorized for use in internal infrastructure networks and systems E2. Evidence of minimum security configurations of personal devices according to the policy.

A7: Cybersecurity Incident Management

Develop and implement plans and procedures for the management of cyber incidents, including their detection, response, reporting and communication.

Security Measure	Implementation
A. Drafting detailed plans and procedures for managing cybersecurity incidents. (Review at least 1 (one) time per year and/or after any cybersecurity incident or after any major change in infrastructure)	A1. Cyber incident management plan document (version, date, approval). A2. Procedure for identifying, classifying and handling incidents (action manual - "Playbooks"), list of persons of the cyber incident response team.
B. Storing data for all cybersecurity incidents.	B1. Incident log including: date, cause, impact, and corrective actions. B2. Individual incident training reports and analyses of lessons learned.
C. Defining and implementing cyber incident communications and reporting with authorities and notifying third parties and customers.	Q1. Incident reporting forms for the authorities defined in the applicable legislation on infrastructure cybersecurity. Q2. Communications and reporting inventory.

A8: Change Management

Define and implement policies and processes for change management through planning, assessment, approval, communication, implementation and monitoring of changes in infrastructure.

Security measure	Implementation
A. Ensuring that any changes in information technology (IT) infrastructure systems and processes within the critical/critical infrastructure are managed in a controlled and documented manner.	A1. Change management policy (including description, date, anticipated responsibilities and impact, implementation plan, etc.). (Review minimum 1 (one) time per year.) A2. Change Management Procedure (Steps from Proposal to Approval and Implementation) A3. Request for Change Form ("RFC")

A9: Work Continuity Management

Establish and implement contingency plans and a clear strategy to ensure the continuity of communication networks and information systems

Security measure	Documentation / Verification of implementation

A. Establish and implement a Business Continuity Plan ("BCP") to ensure the continuous operation of critical infrastructure processes in the event of cyber incidents, natural disasters, or operational disruptions. (Review minimum 1 (one) time per year and/or after any cybersecurity incident or after any major change in infrastructure.	A1. . Continuity of services strategy policy, including conditions for plan activation, recovery time, communication in times of crisis, incident scenarios, action plan, testing rules, etc. A2. Business Impact Analysis ("BIA"), identification of critical processes and determination of the time/recovery point objective ("RTO" – Recovery Time Objective / "RPO" – Recovery Time Objective). A3. Emergency contact list – information on crisis contact points.
B. Implementation of a policy/procedure for performing backups. (Review minimum 1 (one) time per year and/or after any cybersecurity incident or after any major change in infrastructure.	B1. Document of the policy/procedure for performing backups, including frequencies, types, data and services. B2. List of backups performed and data recovery and integrity test reports.
C. Avoiding Single Points of Failure in Critical and Important Infrastructure Services	C1. Technical verification of single points of failure. C2. Evidence of redundancy of services
D. Implementation of infrastructure according to High Availability (HA) service schemes	D1. Document of infrastructure schemes by high availability service (HA) at the levels of technical support of the first, second and second level third (L1, L2, L3) and the circumference with fire.
E. Implementation of a second environment for the recovery and continuity of operation of information technology (IT) systems after a cyber incident ("DRS" – Disaster Recovery Site).	E1. Strategy for DRS and detailed configurations. (Review at least 1 (one) time per year and/or after any cybersecurity incident or after any major change in the infrastructure of the OIKI/OIRI). E2. Disaster Recovery Plan (DRS), information technology (IT) and infrastructure recovery procedures (tasks and responsibilities, list of key systems and assets), (minimum review 1 (one) time per year and/or after any cybersecurity incident or after any major change in infrastructure. E3. Second environment test reports for recovery and continuity of operation of information technology systems for post-incident/disaster recovery (DRS). (Minimum 1 time per year and/or after any cybersecurity incident or after any major change in infrastructure. E4. Verification and evidence.

A10: Legal Compliance Management

Establish and implement a policy for monitoring the compliance of standards with legal requirements.

Security measure	Implementation
A. Monitoring the compliance of standards with legal requirements.	A1. Policy/procedure for monitoring compliance with legal standards and requirements. A2. List of applicable legal standards and requirements for infrastructure. A3. Review of Information Security Management System ("ISMS") policies and procedures, minimum 1 (one) time per year and/or after any cybersecurity incident or after any major change in infrastructure.

The Undertakings shall adopt and implement documented procedures for the receipt and handling of requests for access, rectification, deletion, restriction, objection to the processing of personal data, as well as coordination between the Personal Data Protection Officer and the network security structure for any case related to the rights of data subjects.

A11: Control and audit

internal and external, in order to monitor compliance and continuously improve the security of information in the infrastructure.

Security Measure	Implementation
A. Policy/procedure for internal control and audit for information security and periodic review. (Minimum 1 time per year and/or after any cybersecurity incident or after any major change in infrastructure).	A1. Document of the policy/procedure for controls and audits (version, date, approval of the policy/procedure by the management staff).
B. Conducting internal or third-party controls/audits for the security of information and critical infrastructure systems. (Minimum 1 (one) time per year and/or after any cybersecurity incident or after any major change in the infrastructure).	B1. Internal audit reports and deficiencies treatment plan (date, methodology, results). B2. Reports of audits conducted by third parties on information security. B3. List of corrective actions taken after audits and evidence of their implementation.

B. Technical and operational measures

Technical cybersecurity measures are technological solutions and mechanisms, which guarantee the protection and integrity of communication networks and information systems of information

infrastructure operators, including the implementation of access control, authentication and authorization, data encryption, monitoring and recording of security events, protection against cyber attacks, as well as the implementation of technologies for incident detection and prevention cybersecurity. Whereas, operational cybersecurity measures are the processes, practices and daily activities of operators of information infrastructures to ensure information security and the sustainable functioning of critical and important systems, including cybersecurity incident management, ensuring continuity of services and disaster recovery, infrastructure change management, as well as the application of procedures for reporting and communicating security events with the responsible authorities.

B1: Physical Security

To establish and implement appropriate physical and environmental security of networks/information systems and equipment.

Security Measure	Documentation / Verification of implementation
A. Implementation of physical security measures and environmental controls.	A1. Evidence of the implementation of physical security measures (locks, cabinets, electronic access control). A2. Traces of audit activities (logs) for access to authorized spaces and alerts for unauthorized entrances. A3. Reports on the operation and maintenance of alarm systems and fire extinguishers. A4. Ensure the division of physical spaces into segmented areas based on authorization levels, including the design of a detailed topology and a clear evacuation plan to ensure physical security and access management.
B. Implementation of a policy on physical security measures and environmental controls.	B1. Policy document on physical security and environmental controls (version, date, approval, revision).

B2: Management for Access Authorization

To establish and maintain appropriate controls and authorizations for access to communication networks and information systems.

Security Measure	Implementation

A. Implementation of policies for controlling and protecting access to networks and information systems. (Review at least 1 (one) time per year and/or after any major changes to the infrastructure	A1. Access policy document (roles, groups, rights, procedures for granting and revoking access). A2. Access Rights Granting Form A3. Form for revocation of access rights and delivery of assets. A4. Evidence of deletion of generic accounts and periodic access control reports.
B. Applying Traffic Filters in Case e Access in Distance of	B1. Technical verification and evidence for filtering and traffic encryption.
systems, as well as encrypting traffic with secure protocols	
C. Checking whether there are authorized lists/blocked lists ("Whitelists") configured in the firebook. Internet Protocol (IP) addresses allowed or blocked	Q1. Verification and evidence for configurations in the digital firewall (firewall).
D. Use of Random Password Management Policies for Local Users and Administrators.	Q1. Policy document for managing passwords and verifying the implementation of solutions for managing random passwords for users and local administrators ("LAPS") or similar technologies.
E. Creating and implementing a technological solution for user identity and access management ("IAM") to ensure security, authorization and auditing of activities of users on critical systems.	E1. Technical verification and evidence.
F. Implementation of a technological solution for privileged access management ("PAM")	F1. Technical verification and evidence.
G. Implementation of the network access security service, according to the principle of zero trust ("ZTNA" – Zero Trust Network)	G1. Technical verification and evidence.

B3: Cryptographic Devices

Ensure sufficient use of encryption to prevent and/or minimize the impact of user cybersecurity incidents on communication networks and information systems.

Security measure	Implementation

A. Implementation of encryption policies, including details about cryptographic algorithms and keys.	A1. Encryption policy document as e.g. algorithms: "AES", "RSA", "ECC", "TLS", "IPSec", "SSH" etc. A2. List of cryptographic keys (e.g., type, expiration date, generation and storage method).
B. Data encryption (in transit and in stable state)	B1. List of encryption configurations for data and applications ("on-prem", "hybrid", "cloud"). B3. Technical verification and evidence

B4: Cybersecurity Incident Detection

To create and maintain capacities for the detection of cyber security incidents.

Security measure	Implementation
A. Implementation of the automated system for the detection and management of security information and incidents/events ("SIEM" - Security Information and Event Management).	A1. Technical verification and evidence of the configuration of the automated system for the detection and management of information and security incidents/events (SIEM), including alerting and trace filtering rules, and incident detection activities (logs).

B5: Collection and processing of information on cyber threats

Establish and maintain a mechanism for monitoring, collecting and analyzing information regarding security threats in communication networks and information systems.

Security measure	Implementation
A. Continuous monitoring of external intelligence sources for cyber threat intelligence.	A1. Periodic reports from intelligence monitoring tools on cyber threats "threat intelligence". A2. List of resources used to gather threat intelligence
B. Implementation of the threat intelligence program, which includes roles, responsibilities and procedures.	B1. Threat intelligence program document (including the structure of roles and responsibilities). B2. Procedure for collecting, processing, analysing and disseminating information on cyber threats.

B6: Monitoring and Logging of Cybersecurity Events

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

Security measure	Implementation

A. Implementation of policies for monitoring and recording cybersecurity events	A1. Policy document for monitoring and recording traces and activities (logs), which includes minimum requirements, retention period, objectives, approval, update.
B. Putting in place the means for the collection of traces and activities (logs) of critical systems.	B1. List of Implemented Collection Tools of traces and activities/logs of log servers, etc. B2. Technical verification and evidence.

B7: Protecting the integrity of communication networks

To establish and maintain the integrity of networks and information systems, as well as to protect them from viruses, code injections and other malware, which can change the functionality of the systems.

Security measure	Implementation
A. Installation of equipment to monitor, control and limit the incoming and outgoing traffic of computer networks with the new generation digital firewall ("Next Generation Fireëall")	A1. Technical verification for the configuration of the new generation digital firewall. A2. Technical verification and evidence.
B. Monitoring, detecting and analysing suspicious behaviour on endpoints, such as computers, laptops and servers. This system collects and analyzes data from end-devices to detect sophisticated threats.	B1. Technical verification and evidence of traffic analysis.
C. Division of the network into subnets at the microsegmentation level	Q1. Technical verification and evidence of network topology with documented subnet partitioning.
D. Placement in different zones/subdivisions of the network/virtual local area network (zone/ subnet/ VLAN) of computers and servers with the Access Control List according to the principle of minimum rights ("last privilege")	Q1. List of virtual local networks (VLANs) and network subdivisions implemented, including access control lists. D2. Technical verification and evidence.
E. Isolation of the wireless network from the rest of the network.	E1. Technical verification and evidence of wireless network isolation configuration
F. Use of "Gateway Security Techniques" to limit the number of unique Network Connected Device Identification Addresses (MAC Addresses) to "1" for ordinary users and to a limited number for network technology experts information or cybersecurity.	F1. Technical verification of the configuration of the sites, applying the port security technique "Port Security" for the unique identification number of the networked device (MAC Address) allowed.

G. Implementation of techniques and standards for hardening of all equipment in the network.	G1. Manual for fortifying devices (PC, server, router, firewall). G2. Technical verification and evidence.
H. Logical isolation of the database and Web services (e.g. in different virtual local network/VLANs).	H1. VLAN virtual local network list and technical configuration verification for logical isolation of database and Web services.
I. Implementation of "DNS_SEC" to avoid "DNS Amplification" and "DNS Poisonning".	I1. Technical verification and evidence.
J. Implementing DoS/DDoS Attack Protection	J1. Technical verification of the configuration of DoS/DDoS(e.g protection mechanisms. "rate limiting","ËAF" – Web Application FireWall, tools for "anti-DDoS")
K. Implementation of a solution/system for controlling the security parameters of end devices ("NAC" – Network Access Control)	K1. Procedure for determining the minimum safety parameters (baseline). K2. Technical verification and evidence.

B8: User Access Management

Implement policies for password management and granting access according to the models of discretionary access control ("DAC"), mandatory access control ("MAC") and role-based access control (RBAC). Use the Active Directory (AD) service to manage privileges and restrict unauthorized access to the device.

Security Measure	Implementation
A. Implementing policies for managing user passwords	A1. Policy document for password management (complexity, expiration date, periodic changes).
B. Models for granting user access (discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC)	B1. Technical evidence of configurations and rules implemented in the system and verification.
C. Management of user access and privileges through the "AD" service	Q1. Technical verification and evidence of the implementation of "AD" (group structures, privileges, restrictions)
D. Securing and protecting data and restricting unauthorized access and information.	Q1. Verification of the implementation of the "Clean Desk" policy/procedure and the automatic screen locking policy/procedure after a passive time ("idle")
E. Implementation of Two-Factor Authentication (2FA) systems at the application level /web/mail/ device for all users of the critical system	E1. Verification and evidence.

B9: Activity and Authentication of Administrators

Ensure administrator access by implementing Multi-Factor Authentication (MFA) across apps, web, email, and devices. Use Data Loss Prevention (DLP) platforms to prevent unauthorized information leakage.

Security measure	Implementation
A. Implementation of multi-factor authentication (MFA) method, at the application/web/mail/device level for administrators	A1. Verification and evidence of implementation of the multi-factor authentication (MFA) method.
B. Using Data Loss Prevention (DLP) Method to Identify and prevention of Unauthorized Leakage of sensitive data outside the infrastructure.	B1. Verification of the implementation of the Data Loss Prevention Method (DLP) for sensitive data leakage.

B10: Application Security

Ensure the protection of applications by conducting security testing for vulnerability assessment ("VA") and penetration testing ("Penetration Test") and addressing identified problems.

Security measure	Implementation
A. Conducting tests for the security assessment of information technology applications and networks for vulnerability assessment (VA) and drafting of a plan for addressing the identified problems. (Minimum 1 (one) time per year and/or after each cybersecurity incident or after any major change in infrastructure.	A1. Vulnerability assessment report and treatment plan.
B. Checking whether web services operate by implementing the secure protocol "https".	B1. Technical verification and evidence (e.g. visual evidence of configurations through screenshots, logs and detailed documentation of technical parameters).
C. Anti-spoofing configuration: DMARC /SPF/DKIM in the e-mail system.	Q1. Technical verification and evidence (e.g. evidence of the implementation of anti-spoofing in the e-mail system)
D. Conducting software development testing ("staging/testing") in a dedicated environment separate from the production environment, if the infrastructure has a development department.	Q1. Verification of the evidence of the environment dedicated to software testing, separated from the production environment.

E. Implementation of a solution for filtering, monitoring and blocking malicious online traffic, with Web Application Security Firewall (WAF)	E1. Technical verification and evidence (e.g. visual evidence of configurations through screenshots, logs and detailed documentation of technical parameters).
F. Implementation of "Reverse Proxy" on a server that sits between clients and internal backend servers and acts as an intermediary for it process requests from clients and forward them to internal servers.	F1. Verification of the implementation of "Reverse Proxy" on web servers (e.g. visual evidence of configurations through screenshots, logs and detailed documentation of technical parameters).
G. Conducting tests to assess the security of applications and networks (Penetration Test – Black, Gray, White) and drafting a plan for addressing the identified problems.	G1. The test report of the types: "black", "grey", "white" for the security assessment of applications and networks (penetration test) and the treatment plan.
(Minimum 1 (one) time per year and/or after each cybersecurity incident or after any change major in infrastructure	

B11: Secure Software Development

Software production security for critical or critical infrastructures includes practices and measures that enable the design, development, testing, and implementation of high-security software to protect infrastructures from cyberattacks.

Security measure	Implementation
A. Implementation of a security procedure for the design and development of software. (Review once a year.)	A1. Documentation of the security procedure for the design and/or development of software. A2. The procedure should be approved by senior management staff and reviewed periodically.
B. Control and monitoring of access of software developers and users.	B1. Specific procedures, such as authentication, authorization, encryption for software developers, should be included in the procedure. B2. Clearly define the rights and accesses for software users
C. Maintaining the history of changes/configurations/development approval of the source code of the software.	Q1. Technical verification and evidence (e.g. visual evidence of configurations through "screenshot", log- and detailed documentation of technical parameters).
D. Risk and safety analysis of the software before it goes into production.	Q1. Risk and security analysis reports of the software before it goes into production, including dependence on third-party libraries.
E. Handling and documenting cybersecurity incidents for software development	E1. Software development audit reports and incident logs.

F. Monitoring the repository of the source code of the software.	F1. Reports Monitoring of countries of repository of the source code of the software
G. Realization of the encrypted connection of the application with the database.	G1. Technical verification and evidence (e.g. evidence of the encryption code of the data-based connection of the application.)
H. Backing up the source code and testing the integrity of the backup.	H1. Technical verification and records (e.g. evidence of the presence of a copy of the source code and tests for code recovery via saved copy)
I. Automation through pipeline ("CI/CD" – Continuous Integration / Continuous Delivery /Deployment) continuous integration/development/implementation of the software development, testing and publishing process.	I1. Technical verification and visual evidence of CI/CD configurations and operation through screenshots, logs and detailed documentation of technical parameters.

B12: Operational Technology (OT) Systems Security

Ensure the protection of operational technology systems, by implementing the principle of minimal access, network segmentation, and encryption of critical protocols. Implement measures for access control, real-time monitoring and protection of equipment from cyber and "malaria" attacks.

Security measure	Implementation
A. Implementation of the principle of minimum access privileges "Least privileges", by establishing role-based access control (RBAC) for users, Access Control List ("ACL") for traffic filtering, as well as closing unnecessary services in critical system systems. operational technology (OT)	A1. Technical verification and evidence.
B. Implementation of TLS/SSL, VPN for protocols (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	B1. Technical verification and evidence.
C. Implementation of "Hot" and "Cold" backups techniques, for data storage.	Q1. Technical verification and evidence
D. Implementation of a remote access management solution, according to the principle of zero trust (ZTNA).	Q1. Technical verification and evidence
E. Controlled management of patches and configurations, testing it beforehand in test facilities.	E1 Technical Verification and Evidence

F. Implementation of endpoint protection, including detection mechanisms, response or isolation of the attack at the "signature" level and "behaviour" behavior.	F1. Technical verification and evidence
G. Application of the "Hardening" technique of operational technology equipment, such as (PLC, RTU, HMI, SCADA, BMS etc.)	G1. Technical verification and evidence
H. Separation of information technology infrastructure from operational technology (by providing separate services for each infrastructure, such as "Active Directory", "Antivirus", next-generation firewall ("NextGen Firewall") and SIEM, that are dedicated to operational technology.	H1. Technical verification and evidence.
I. Implementation of real-time monitoring of operational actions in operational technology systems, as well as recording, analysis and notification of events based on in Functions and their importance for critical operations.	I1. Technical verification and evidence.

B13: Security of "IoT – Internet of Things" systems

To design and implement procedures for the security of "IoT" devices, including the use of mechanisms that guarantee the integrity and confidentiality of the systems. Implement secure updates and ensure the protection of authentication keys on "IoT" devices.

Security measure	Implementation
A. Design, approval, implementation and periodic review of procedures for the security of "IoT" devices and systems.	A1. Procedure for the security of "IoT" devices and systems

B. Security of "IoT" Devices: - Determination of minimum requirements for "hardware" equipment. - Use of mechanisms that guarantee integrity and confidentiality (Trusted Platform Module). - Application of secure updates/updates of operating systems and "firmware". - Guaranteeing the security of authentication keys. - Conducting traffic analyses at the behavioral level (when applicable).	B1. Technical verification and evidence (e.g. visual evidence of configurations through screenshots, logs and detailed documentation of technical parameters).
C. Guaranteeing the integrity and confidentiality of data transmitted between "IoT" devices. - Use of authentication certificates that provide security (devices with Hub or Central "IoT"). - Ensuring secure communication (TLS 1.2 and above). - Securing "IoT" data when it is transmitted and stored. - Clear definition of access controls ("IoT hub" and "IoT Central" application). - Realization of security monitoring of "IoT" solutions.	C1. Technical verification and evidence (e.g. visual evidence of configurations through screenshots, logs and detailed documentation of technical parameters).

B14: Security in Cloud Services

Security in Cloud services includes measures and policies that ensure the protection of data and infrastructure services, including strong authentication, data encryption and monitoring of activities. These measures are intended to guarantee integrity, the availability and confidentiality of the systems used in the "Cloud", as well as the compliance with the technical requirements and service level agreements ("SLA") agreed with the service providers.

Security measure	Implementation
A. Establishing a governance policy/procedure for Cloud services.	A1. Cloud Security Policy/Procedure.

B. Inclusion of technical, organizational and security requirements in service level agreements (SLAs) with Cloud service providers.	B1. Service level agreement (SLA) document, which includes key performance indicators, monitoring, safety, and recovery metrics.
C.Implementation of strong authentication, such as multi-factor authentication (MFA) for the access of the administration platform and services to the "Cloud".	C1. Verification and evidence for the implementation of authentication in the "Cloud".
D. Implementing an encryption mechanism for data in storage and in transit.	D1. Technical verification and evidence.
E. Making a regular backup of critical and important services in the "Cloud"	E1. Technical verification and evidence.
F. Implementation of log activation and monitoring activities of infrastructure in the "Cloud"	F2. Technical verification and evidence.
G. Implementation of a network security architecture that combines network and information technology security functions into a unified, Cloud-based platform. Using the Secure Access Service Edge ("SASE").	G1. Technical verification of the Secure Service Solution for Network Edge Access (SASE). ii. Verification and evidence of users' use of the Secure Network Edge Access (SASE) service