REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 2066 Prot

Tiranë më 27.06.2025

URDHËR

Nr. 181 datë. 27.06 2025

PËR

MIRATIMIN E RREGULLORES PËR FUNKSIONIMIN TEKNIK TË CSIRT-EVE SEKTORIALE DHE CSIRT-EVE PRANË OPERATORËVE TË INFRASTRUKTURAVE TË INFORMACIONIT

Në zbatim të pikës 4, të nenit 15 të ligjit nr.25/2024 "Për sigurinë kibernetike",

URDHËROJ

1. Miratimin e rregullores "Për funksionimin teknik të CSIRT-eve sektoriale dhe CSIRT-eve pranë operatorëve të infrastrukturave të informacionit" sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

REPUBLIKA E SHQIPËRISË - KËSHILLI I MINISTRAVE - AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

No. 2066 Prot   Tirana, on 27.06.2025

ORDER

No. 181 date. 27.06.2025

ON
“THE APPROVAL OF THE REGULATION ON THE TECHNICAL FUNCTIONING OF SECTORAL CSIRTs AND CSIRTs WITHIN INFORMATION INFRASTRUCTURE OPERATORS”

Pursuant to point 4, article 15 of law no. 25/2024 “On Cybersecurity”,

I HEREBY ORDER:

1. The approval of the Regulation “On the technical functioning of sectoral CSIRTs and CSIRTs within information infrastructure operators”, according to the text attached to this Order and forming an integral part thereof.
2. For the implementation of this Order, the sectoral CSIRTs and the CSIRTs within information infrastructure operators are charged.
3. This Order shall enter into force immediately.

GENERAL DIRECTOR

IGLI TAFA

Signature

REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

Regulation on the Technical Operation of Sectoral CSIRTs and CSIRTs within Information Infrastructure Operators

Content

1. Introduction

The exponential increase in the number, complexity, and impact of cyberattacks over the past decade has called into question the traditional capacities of institutions to manage risks in the digital space. Ransomware-based attacks, attacks on critical and important information infrastructures, data manipulation, and disinformation campaigns demand a far more organized, standardized, and interoperable approach to cybersecurity incident management.

In this context, the need for a sustainable, independent, and integrated structure,equipped with trained personnel and advanced tools becomes critical for safeguarding institutional integrity and ensuring the continuity of digital services for citizens and businesses.

For this purpose, law no. 25/2024 “On Cybersecurity” has established the creation and functioning of computer security incident response teams (CSIRTs), as important structures for coping with cybersecurity challenges at the national, sectoral, and operator level. This framework aims to strengthen institutional capacities to address cybersecurity challenges and to build a reliable mechanism for the real-time detection, analysis, and handling of cyber incidents.

This regulation sets forth the technical rules governing the operation of sectoral CSIRTs and CSIRTs within information infrastructure operators, based on the internationally recognized SIM3 (Security Incident Management Maturity Model). SIM3 enables the assessment and development of CSIRT functional maturity across four core parameters: Organization, Human Resources, Tools and Technologies, and Operational Processes.

The implementation of the SIM3 model also supports the harmonization of CSIRT operations with the requirements of the European Union[1] NIS2 Directive and ENISA standards, positioning Albania in alignment with regional and European efforts to build a unified and resilient cybersecurity architecture.

The technical functioning of CSIRTs is founded on the principles of professionalism, operational maturity, and continuous improvement of technical and organizational capacities. These principles ensure a structured, reliable, and sustainable resilient into fulfilling their functions in addressing cybersecurity threats and incidents.

2. Purpose

This regulation defines the technical rules for the functioning of sectoral CSIRTs and those established within information infrastructure operators, with the aim of strengthening resilience against cyber risks and threats and creating a unified approach among responsible bodies/entities for cybersecurity at both sectoral and operator levels.

The regulation aims to:

- Standardise the organizational structure and technical operations of sectoral CSIRTs and those within operators, in accordance with international best practices.

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the European Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

- Establish a clear and measurable framework for operational maturity, enabling the assessment and gradual enhancement of CSIRT capabilities;
- Ensure sustainable development and continuous improvement of technological, procedural, and human capacities within CSIRTs, to guarantee effective and coordinated responses to cybersecurity incidents;
- Alignment with international best practices and ensure compliance with the EU Directive NIS2;

3. Scope of application

This regulation applies to entities responsible for cybersecurity and operators of critical and important information infrastructures, within which CSIRT structures are established and operate, in accordance with the provisions of law no. 25/2024 "On Cyber Security."

4. Definitions

The terms defined in this regulation hold the same significance as those outlined in law no. 25/2024 "On Cyber Security". The following terms are defined as follows:

1. **Personal Data** – according to this regulation has the same meaning as the definition given in the legislation in force on the protection of personal data.
2. **PIR (Post-Incident Review)** – An analytical process conducted after a cybersecurity incident to assess its cause, impact, response effectiveness, and derive lessons to prevent similar future incidents
3. **MTTR (Mean Time to Repair)** – The average time required to repair a device or system and restore it to operational status following a technical failure
4. **MTTR-R (Mean Time to Repair – Recovery)** – The average time needed to fully restore a system after an outage
5. **SOAR (Security Orchestration, Automation and Response)** – is the platform for automation of response and operational security analysis.
6. **SIM3 (Security Incident Management Maturity Model)** it is the international maturity model for CSIRTs, which assesses and improves four functional parameters: Organisation (O), Human Resources (H), Technical Tools (T), and Operational Processes (P).
7. **Operational Maturity** – The level of development and formalization of a CSIRT's capacity to respond to cybersecurity incidents, measured according to the SIM3 model
8. **RFC 2350** – is an international standard document used for the official description of a CSIRT (structure, services, contacts, jurisdiction).
9. **SIEM (Security Information and Event Management)** – Systems that collect, analyze, and correlate security events for monitoring and early alerting
10. **STIX (Structured Threat Information Expression)** is a standard format for describing and sharing data on cyber threats.
11. **TAXII (Trusted Automated Exchange of Indicator Information)** – is a protocol for automated exchange of cyber threat intelligence
12. **Traffic Light Protocol (TLP)** – is a classification scheme for the separation of sensitive information, based on the levels: TLP: RED, TLP: AMBER, TLP: GREEN, TLP: CLEAR.

13. **KPI (Key Performance Indicators)** – Metrics used to measure the performance and responsiveness of a CSIRT
14. **BCM (Business Continuity Management)** – it is a systematic approach to ensure that the CSIRT can continue to provide its critical services even during and after an unexpected disruption, whether as a result of a cyber incident, natural disaster, infrastructure failure, or human factors.
15. **IPS/IDS (Intrusion Prevention/Detection System)** – are systems that detect and/or prevent unauthorized intrusions into a network or systems.
16. **EDR/XDR (Endpoint/Extended Detection and Response)** – are advanced solutions for monitoring, detecting, and responding to cyber threats on endpoint devices (EDR) and in broader network and cloud environments (XDR).
17. **MISP (Malware Information Sharing Platform)** – is an open-source platform for sharing, storing, and correlating indicators of compromise and cyber threat intelligence.
18. **IDS (Intrusion Detection System)** – it is a network security technology that monitors traffic and devices for suspicious activity or policy violations.
19. **NetFlow** – it is a protocol that collects metadata on IP traffic passing through network devices, aiding in traffic pattern and performance analysis
20. **OTRS (Open-source Ticket Request System)** – is an open-source service management system that can be used by any department in an information infrastructure to reduce operational costs and improve service performance.
21. **TheHive** – it is an open and scalable platform for managing security cases, designed to assist SOC, CSIRT, and CERT teams in handling cybersecurity incidents.
22. **OT (Operational Technology)-** refers to the hardware and software that monitor and control devices and physical processes in various industries, such as manufacturing, energy, and transportation.
23. **IT (Information Technology)** – it encompasses the use of computers, software, and networks to create, process, store, and transmit data and information.
24. **DDoS (Distributed Denial of Service)** – it is a type of cyberattack in which multiple distributed devices (often infected with malware) are used to overwhelm a server, network, or online service, rendering it inaccessible to legitimate users.

5. Structure of the CSIRT network in the Republic of Albania

The network of Cyber Security Incident Response Teams (CSIRTs) in the Republic of Albania constitutes a functional architecture built upon the principles of collaboration, interoperability, and real-time information sharing. This organizational structure is defined by law No. 25/2024 “On Cybersecurity” and comprises multiple operational levels that span the entire institutional spectrum and the sectors of critical and important information infrastructures.

5.1. National CSIRT

Established within the National Cyber Security Authority (NCSA), the National CSIRT serves as the leading and coordinating entity at the national level for all cybersecurity incident response activities. It is responsible for managing incidents with national impact, facilitating international cooperation, and standardizing practices for responding to cybersecurity incidents.

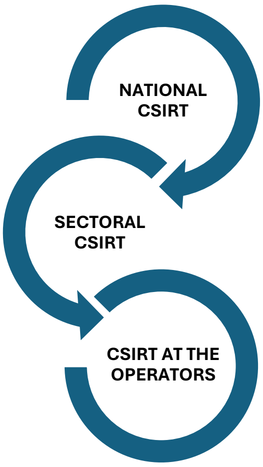
5.2 Sectoral CSIRT

The Sectoral CSIRT is the cybersecurity incident response team established by designated cybersecurity entities to provide services within specific sectors, as defined in the annexes of the cybersecurity law.

5.3 CSIRT at the Operators

CSIRTs within information infrastructure operators are internal teams established by operators of critical or important information infrastructure, who are responsible for handling cyber incidents at the organizational level and for reporting them to the sectoral and national CSIRT.

5.4 The CSIRT Scheme



6. Technical Rules for the Operation of the Sectoral CSIRT and the Operator's CSIRT

The technical functioning of CSIRTs is based on four core parameters: Organization (O), Human Resources (H), Technical Tools (T), and Operational Processes (P).

6.1 Parameters

Organisation (O)

This parameter defines how a CSIRT is structured and operates, including its scope of activity, the services it provides, and the organizational and policy framework that supports it.

Human resources (H)

Human capacities constitute one of the most important assets for the functioning of the CSIRT. In this regard, CSIRTs must have qualified staff, trained continuously and equipped with the necessary technical and interpersonal competencies for the effective management of cybersecurity incidents. For this purpose, it is essential to establish clear mechanisms for professional development and the continuous improvement of the technical and managerial capacities of the staff, through regular training programs, adherence to best standards, and support for skills development in line with the evolution of cyber threats.

Operational Processes (P)

An essential component of CSIRT's functioning is the clear and comprehensive description of the main operational processes such as: management and monitoring for the prevention of cyber incidents, assessment and analysis of cyber risk, and other supporting processes related to the effective operation of structures for cyber security.

In particular, the cybersecurity incident management process must be thoroughly detailed and encompass all phases as defined in the applicable regulation on incident management procedures. This includes countermeasures, playbooks, and general protective actions from the receipt and verification of incident reports, classification and technical intervention, coordination with involved parties, alerting affected sectors, to incident resolution and retrospective analysis for continuous improvement.

All these processes must be documented in a detailed manner, measurable through performance indicators, repeatable according to standard procedures, and constructed flexibly to adapt to technological, regulatory, and organizational changes in order to ensure consistency, maturity, and improvement of capacities.

Technical Tools(T)

The use of modern technological tools is another important component for the functioning of CSIRTs in order to strengthen the response to cyber security threats/risks. This includes the use of technological tools such as:

- SIEM systems for monitoring and managing security events
- Systems for interaction and threat information sharing via protocols such as STIX, TAXII, and TLP
- Ticketing systems for case tracking and management
- Forensic analysis and threat intelligence sharing platforms

The deployment of these technological tools significantly enhances the cybersecurity incident management process by increasing operational efficiency, reducing response time, and enabling deep and structured analysis of each incident.

6.2. Communication and information sharing

Effective communication and secure information sharing constitute a crosscutting component that supports all functional parameters of both the CSIRT within the information infrastructu re operator and the sectoral CSIRT. These elements are important for a coordinated response to cybersecurity incidents.

In this context, the CSIRT at the operator and the sectoral CSIRT must create and use secure communication channels, ensuring the confidentiality, integrity, and traceability of the information shared with other entities, and take into consideration the application of standards and protocols for the secure exchange of information such as STIX, TAXII, TLP, etc.

7. The maturity assessment level of CSIRTs

This regulation provides a clear and simplified framework for measuring the level of development and functionality of each CSIRT parameter, based on the four core dimensions: Organization, Human Resources, Operational Processes, and Technical Tools.

This maturity assessment enables CSIRTs to identify strengths and gaps, to plan strategic and operational improvements, to increase effectiveness and resilience, as well as to align with international standards and the requirements of the applicable legislation on cybersecurity. The assessment is structured across a five-level scale, allowing for objective identification of the current maturity stage for each parameter, as outlined in the following table:

Level	**Description**
Level 0 – (*Not Applicable / Undefined / Unaware***)**	This level indicates a complete lack of awareness or practice regarding the specific parameter, typically referring to initial response teams that have not undertaken any measures to operate in accordance with defined parameters.
Level 1 – (*Implicit)*	This level reflects that the parameter is recognized within the team. The team understands the process, but it is undocumented and lacks standardized dissemination among team members.
Level 2 – (*Documented but Not Formalized***)**	This level represents a situation where information and practices exist within informal internal systems. These include documented processes, tools, and policies, but without formal approval from the responsible CSIRT structures. Even if there is internal consensus on the content, the absence of formal endorsement limits the maturity to this level.
Level 3 – (*Formalized and Approved by Responsible Structures)*	This level requires that the content of the parameters be documented and officially approved by the responsible CSIRT structures. These documents must be integrated into the team's daily operations and reviewed regularly.
Level 4 – (*Controlled and Supervised by Oversight Structures***)**	In addition to being documented and approved (as in Level 3), this level requires the parameter to be subject to a regular and active control process by oversight structures. This process must include clear evidence, periodic monitoring, and feedback mechanisms between the team and its supervisory entities.

8. Mechanisms for the development of parameters

These mechanisms represent important practices that must be implemented by every CSIRT, with the aim of strengthening its institutional role, improving response to cybersecurity incidents, and enhancing its ability to operate in a coordinated, documented, and adaptive manner in the face of technological and regulatory changes.

Development Mechanisms for Parameter O – Organization, includes:

- Drafting and approval of clear internal and external communication policies

- Drafting and adoption of policies for the classification and management of cyber incidents in accordance with the current legal framework on cybersecurity;

- Continuous use of the RFC 2350 reference document as a standard for describing CSIRT services;
- Establishment of mechanisms for managing relationships with institutional partners and peer CSIRTs;
- Development of a three-year CSIRT growth plan with measurable objectives and monitoring indicators;
- Annual audits by NCSA to verify compliance with organizational structure requirements;

Development Mechanisms for Parameter H – Human Resources, includes:

- Drafting of a functional manual defining roles and responsibilities of CSIRT staff;
- Development of sustainable practices for continuous knowledge exchange among team members;
- Documentation of recruitment processes, initial training, and ongoing professional development;
- Implementation of a regular performance evaluation cycle and updating of staff competencies;
- Use of online training platforms and virtual labs to enhance technical skills.

Development Mechanisms for Parameter T – Technical Tools, includes:

- The minimal use of open source tools *(open-source tools)* për analizën dhe reagimin ndaj incidenteve kibernetike *(e.g. MISP, TheHive)*;
- Implementation of threat detection tools such as IPS/IDS, EDR/XDR;
- Automation of threat detection and alerting processes via SIEM systems, which collect, analyze, and correlate security data in real time to identify potential cybersecurity incidents;
- Centralized and immutable storage of event logs, in accordance with the regulation on log retention methods and timeframes;
- Use of secure information-sharing protocols such as STIX 2.1 and TAXII 2.1;
- Integration of continuous monitoring and automated response platforms (SOAR) for high operational efficiency.

Development Mechanisms for Parameter P – Operational Processes, includes:

- Drafting and updating an Operational Manual of the CSIRT that covers all processes and guidelines for the management of cyber incidents;
- Documentation of the standard formats for the registration and handling of cyber incidents, according to the classifications of type, urgency, and impact of cyber incidents based on the regulation approved by order of the general director of the Authority "Categorisation of cybersecurity incidents";
- Provision of regular training and development of simulations to test operational practices;
- Monitoring of key performance indicators such as response time, classification accuracy, and recovery time from cybersecurity incidents;
- Conducting retrospective analyses after each cybersecurity incident to document lessons learned and continuously improve existing security practices.

8.1 Parameters

8.1.1 Parameter O – Organization

Organisation is one of the main parameters and represents the institutional, legal, and functional foundation of a CSIRT. This parameter defines the organisational structure, mandate, roles and responsibilities, as well as the framework for internal and external cooperation, ensuring that the CSIRT operates with full efficiency.

Key Elements of the Parameter Organization:

Parameter	**Description**	**Minimum Requirement for CSIRT**
O-1 Mandate	The CSIRT's mandate defines its existence and function according to applicable legal provisions.	The CSIRT must have a clearly documented mandate issued by a high-level governing or executive authority, based on law.
O-2 Entities (*Covered Group / Service Beneficiaries*)	The group of entities or users for whom the CSIRT provides services.	The CSIRT must precisely define the users it covers.
O-3 Authority	The authority granted to the CSIRT to act on behalf of its clients in fulfilling its mandate.	The CSIRT's authority must be clearly described and originate from high levels of governance.
O-4 Responsibilities	The obligations and responsibilities the CSIRT is expected to fulfil toward the entities it serves.	The CSIRT must have clearly defined responsibilities derived from its mandate and authority.
O-5 Service Description	Description of the services provided by the CSIRT and how to contact it.	Must include contact information, service hours, service descriptions, and information handling policy.
O-6 Public Media Policy	Policies for interaction with public media and social networks.	The CSIRT must have a media relations policy for handling cybersecurity incidents, awareness campaigns, or crisis situations.
O-7 Service Level Description	Description of service levels that can be expected from the CSIRT.	Authorized personnel must respond to any request or communication from peer teams within no more than two (2) working days from receipt.

Parameter	**Description**	**Minimum Requirement for CSIRT**
O-8 Cyber Incident Classification	Use of a classification scheme for cyber incidents that includes type, severity, and priority.	The CSIRT must have a classification scheme for cyber incidents, including their type and severity.
O-9 Participation in National and International CSIRT Networks	Participation of the CSIRT in national and international cooperation networks.	The CSIRT must participate in cooperation networks, either directly or through a higher-level CSIRT.
O-10 Organizational Framework	A document that integrates all parameters O-1 through O-9 into a unified framework.	There must be a framework document that consolidates the mission and all parameters O-1 through O-9 of the CSIRT.
O-11 Security Policy	Security and operational resilience policies of the CSIRT, including Business Continuity Management (BCM).	A security policy must exist that addresses the specific needs of the CSIRT and BCM, aligned with the CSIRT's overall policy.

8.1.2 Parameter H – Human Resources

Human Resources is a critical parameter for the sustainability and professionalism of a CSIRT. This parameter focuses on the quality, training, composition, and continuous development of both technical and managerial staff.

Key Elements of the Human Resources Parameter

Parameter	**Description**	**Minimum Requirement for CSIRT**
H-1 Code of Conduct / Practice / Ethics	Rules or guidelines for professional and ethical behaviour of CSIRT members, which may extend beyond the workplace.	The CSIRT must have a specific code of conduct or ethics tailored to its operational structure and handling of sensitive data, beyond general CSIRT rules.
H-2 Staff Continuity	Ensuring operational continuity in cases of staff absence due to leave, illness, or resignation.	Sectoral CSIRTs must have at least 4 members; CSIRTs within critical infrastructure operators must have no fewer than 2 members to ensure

Parameter	Description	Minimum Requirement for CSIRT
		staffing resilience and the ability to manage unforeseen situations.
H-3 Skills and Task Descriptions	Definition of required skills for each position within the CSIRT.	All CSIRT roles must have clearly defined technical and interpersonal skills, along with corresponding responsibilities for each team member.
H-4 Staff Development	Policy for professional development through ongoing training.	The CSIRT must have a staff development policy covering training for both new and existing members.
H-5 Technical Training	Training programs to enhance the technical skills of CSIRT staff.	The CSIRT must provide technical training aligned with staff roles to develop technological competencies.
H-6 Soft Skills Training	Training programs to develop personal skills such as communication, time management, and performance under pressure.	The CSIRT must ensure soft skills training for all team members, including communication and presentation.
H-7 Building and Maintaining Collaborative Relationships with External Actors	Staff participation in meetings and activities with other CSIRTs and security organizations.	The CSIRT must have a policy that encourages staff participation in national and international CSIRT cooperation networks.

8.1.3 Staff Roles and Professional Profiles

The effective functioning of a CSIRT requires a clearly defined role structure and qualified personnel with documented competencies, distributed across technical, managerial, and communication domains. The table below outlines the core staff roles within a functional CSIRT, along with their key responsibilities and recommended qualifications.

CSIRT Role	Key Responsibilities	Recommended Qualifications
CSIRT Manager	- Leads the CSIRT at strategic and operational levels. -Represents and reports to NCSA and other regulatory institutions by sector, as	- Master’s degree in ICT, Information Security, or Cybersecurity. ~5+ years of experience in cybersecurity

CSIRT Role	Key Responsibilities	Recommended Qualifications
	well as to higher-level management within the organization. -Oversees business continuity plans (BCM) and self-assessment processes	management. -Certifications such as SIM3, CISM, CISSP or equivalent are advantageous
Technical Analyst	- Analyses cybersecurity incidents and applies the CIA triad. -Monitors traffic and alerts in real time. -Conducts digital forensic examinations and log analysis	- Bachelor's degree in ICT, Computer Science, or related fields. - Experience with security analysis tools such as SIEM, IDS/IPS. -Certifications like CEH, CompTIA Security+, ECIH are advantageous
Security Engineer (SOC/Infrastructure)	- Configures and maintains technical tools (SIEM, SOAR, IDS/IPS). - Performs technical controls for incident prevention and detection. -Understands network topologies and defence architectures.	- Degree in ICT, Engineering, or related disciplines- Practical experience with security tools and automation systems. - Certifications such as CompTIA CyberOps, GIAC, CCNA Security are advantageous
Communication Coordinator / Point of Contact	- Reports cybersecurity incidents according to their TLP classification. - Shares information with institutional partners. - Communicates with the public and media during cybersecurity incidents	- Degree in ICT, Technical Communication, Public Relations, or related fields. - Strong writing and communication skills. – Knowledge of basic information security protocols and standards is advantageous.

8.1.4 Parameter T – Technical Tools

Technical Tools refer to the technological infrastructure that supports the operational functioning of a CSIRT. These tools include systems, applications, platforms, and communication protocols that assist in the detection, analysis, handling, and reporting of cybersecurity incidents.

Key Elements of the Technical Tools Parameter are as below:

Parameter	Description	Minimum Requirement for CSIRT
T-1 IT Asset and Configuration Inventory	Description of IT/OT devices and configurations used by CSIRT users.	The CSIRT must have access to an up-to-date and detailed inventory of critical IT/OT assets, including their technical configurations.
T-2 Information Source List	List of sources for threat intelligence, vulnerabilities, security monitoring, and scanning.	The CSIRT must maintain an organized list of information sources to track developments in cybersecurity.
T-3 Consolidated Communication Systems	Consolidated communication systems (email, messaging apps) accessible to all CSIRT members.	The CSIRT must use a reliable messaging system that enables secure information sharing among team members.
T-4 Cyber Incident Tracking System	System for logging and tracking cybersecurity incidents (e.g., RT(IR), OTRS, TheHive).	The CSIRT must use a specialized system for incident tracking, except in very minor cases where a spreadsheet may suffice.
T-5 Resilient Telephony Systems (Emergency Use)	Voice communication systems with high availability and reliability.	The CSIRT must have a backup mechanism for voice communication in case of system failure.
T-6 Resilient Messaging Systems (Emergency Communication)	Messaging systems must be highly available and meet service level requirements.	The CSIRT must ensure messaging systems are functional and backed up for data retention.
T-7 Reliable Internet Access	High-availability internet access aligned with CSIRT service needs.	The CSIRT must have a backup internet line or robust redundant configuration.
T-8 Toolset for Incident Prevention	Set of tools for preventing cybersecurity incidents (IPS, antivirus, vulnerability scanners, etc.).	The CSIRT must use or have access to a clearly defined set of tools for incident prevention.
T-9 Toolset for Incident Detection	Set of tools for detecting cybersecurity incidents (IDS, NetFlow, MISP, etc.).	The CSIRT must use or have access to detection tools and define its role for each.

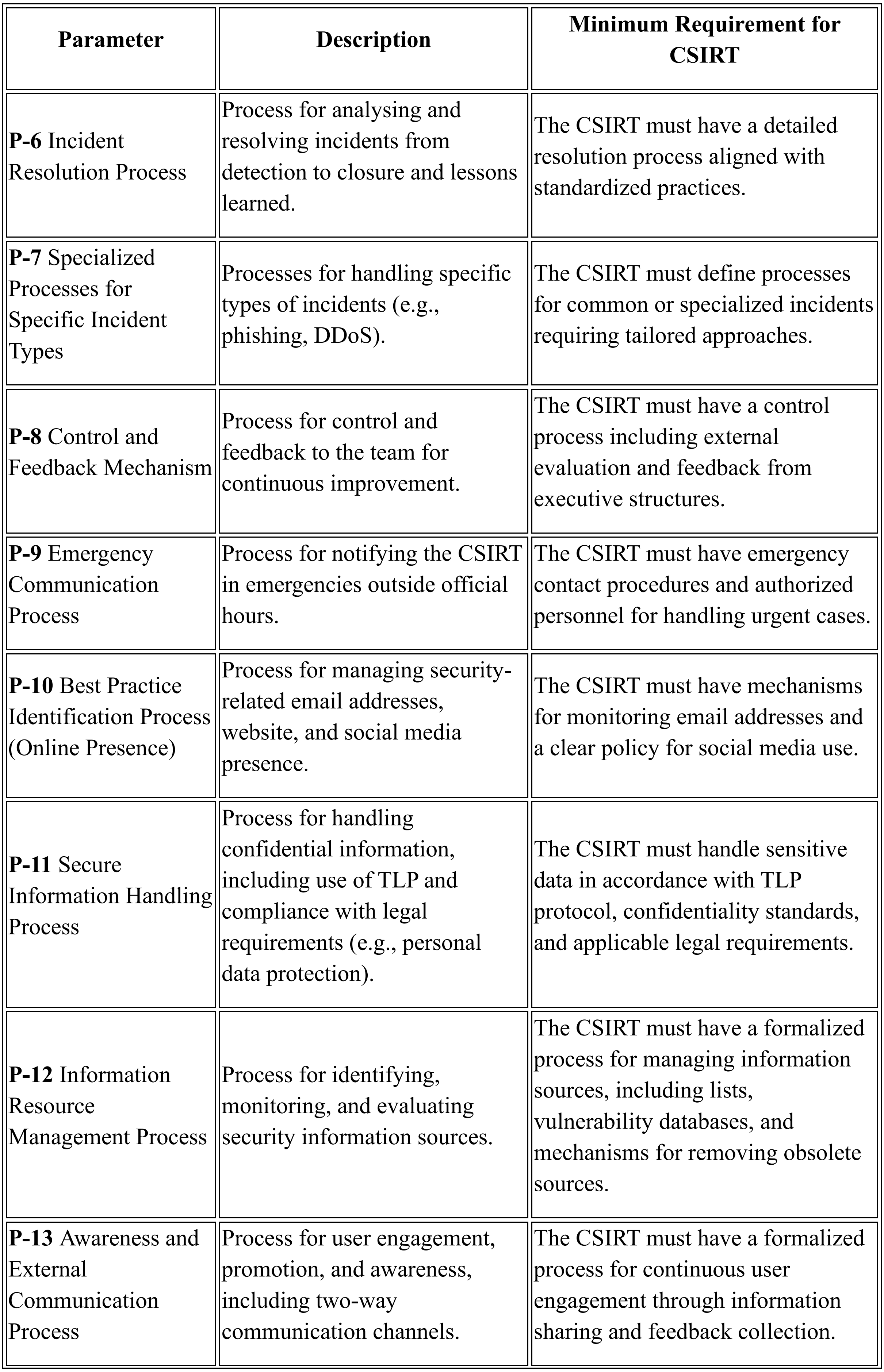
Parameter	Description	Minimum Requirement for CSIRT
T-10 Toolset for Incident Resolution	Set of tools for resolving cybersecurity incidents post-occurrence (forensic kits, malware analysers, etc.).	The CSIRT must have a clearly defined set of tools for incident resolution and be involved in their selection and use.

8.1.5 Parameter P – Operational Processes

Operational Processes focus on the real-world functioning of a CSIRT in managing cybersecurity incidents and daily operations. This parameter encompasses all procedures, rules, and workflows that enable the identification, handling, and effective closure of cybersecurity incidents, including activities for prevention, reporting, and continuous improvement.

Key Elements of the Operational Processes Parameter are as below:

Parameter	Description	Minimum Requirement for CSIRT
P-1 Reporting Cyber Incidents to Executive Levels	Process of reporting critical incidents within the structure and to external authorities.	The CSIRT must be able to report critical incidents to appropriate executive levels at any time, based on an approved policy or procedure.
P-2 Media Communication	Process for communicating with the media office of the CSIRT's supporting structure.	The CSIRT must have a mechanism to inform the press office promptly and outside official hours in case of public-interest incidents.
P-3 Reporting to Legal Experts	Process for notifying the legal office to handle legal requests.	The CSIRT must be able to contact legal experts in real time, especially in urgent cases.
P-4 Incident Prevention Process	Structured process to prevent incidents using technical tools and proactive services (e.g., threat alerts, vulnerability updates).	The CSIRT must have a structured prevention process including threat notifications, proactive monitoring, and communication of preventive measures.
P-5 Incident Detection Process	Process for detecting incidents, including alert generation and use of detection tools.	The CSIRT must have a clear process for detecting and categorizing incidents, including alert generation.



Parameter	Description	Minimum Requirement for CSIRT
P-6 Incident Resolution Process	Process for analysing and resolving incidents from detection to closure and lessons learned.	The CSIRT must have a detailed resolution process aligned with standardized practices.
P-7 Specialized Processes for Specific Incident Types	Processes for handling specific types of incidents (e.g., phishing, DDoS).	The CSIRT must define processes for common or specialized incidents requiring tailored approaches.
P-8 Control and Feedback Mechanism	Process for control and feedback to the team for continuous improvement.	The CSIRT must have a control process including external evaluation and feedback from executive structures.
P-9 Emergency Communication Process	Process for notifying the CSIRT in emergencies outside official hours.	The CSIRT must have emergency contact procedures and authorized personnel for handling urgent cases.
P-10 Best Practice Identification Process (Online Presence)	Process for managing security-related email addresses, website, and social media presence.	The CSIRT must have mechanisms for monitoring email addresses and a clear policy for social media use.
P-11 Secure Information Handling Process	Process for handling confidential information, including use of TLP and compliance with legal requirements (e.g., personal data protection).	The CSIRT must handle sensitive data in accordance with TLP protocol, confidentiality standards, and applicable legal requirements.
P-12 Information Resource Management Process	Process for identifying, monitoring, and evaluating security information sources.	The CSIRT must have a formalized process for managing information sources, including lists, vulnerability databases, and mechanisms for removing obsolete sources.
P-13 Awareness and External Communication Process	Process for user engagement, promotion, and awareness, including two-way communication channels.	The CSIRT must have a formalized process for continuous user engagement through information sharing and feedback collection.

Parameter	Description	Minimum Requirement for CSIRT
P-14 Hierarchical Reporting Process within Infrastructure	Process for reporting to senior management, including statistics and incident analysis.	The CSIRT must have a formalized process for regular and structured reporting to senior leadership.
P-15 Reporting Process	Process for reporting to competent authorities or the public when necessary (e.g., monthly/annual reports).	The CSIRT must have a clear process for reporting incidents to responsible authorities, including statistics and actionable security insights based on incident classification.
P-16 Internal Meeting Process	Process for organizing internal team meetings, physical or online.	The CSIRT must ensure regular meetings, documentation of action points, task allocation, and discussion of lessons learned.
P-17 Collaboration Process with Partner CSIRTs	Process for collaboration with peer teams (CSIRTs, SOCs, etc.).	Partner entities and mutual collaboration methods must be clearly defined.

9. Continuous monitoring and improvement of CSIRTs

To strengthen the performance and operational resilience of CSIRTs, this regulation establishes a structured process for ongoing monitoring and improvement.
This process focuses on the following mechanisms:

- Self-assessment of parameters (O – Organization, H – Human Resources, P – Operational Processes, T – Technical Tools)
- External evaluation through interviews, on-site visits, and analysis of official documentation
- Technical simulations and scenario-based testing to assess incident response capabilities
- Performance measurement based on key indicators (KPIs), such as response time, recovery time, number of resolved incidents, post-incident reports, and training participation

9.1. Key Performance Indicators (KPIs) for CSIRTs

To enable objective and comparable evaluation of CSIRT effectiveness, the regulation prescribes the use of a set of key performance indicators (KPIs). These indicators serve to measure the team's operational capacity, analyze performance trends, and guide strategic improvements.

KPI	**Description**
Mean Time to Respond (MTTR)	Time from incident notification to intervention
Mean Time to Recovery (MTTR-R)	Time until infrastructure is restored to functional status
Number of Incidents Handled	Monthly reporting of closed incidents
Post-Incident Reports (PIR)	Documented reports for analysis and lessons learned
Training Engagement	Number of sessions and participants per year

9.2 Role of NCSA in Supporting CSIRTs

The National Cyber Security Authority (NCSA) will provide continuous support to CSIRTs in developing capacities and implementing evaluation recommendations through:

- Provision of standardized templates for improvement plans
- Training and technical assistance for CSIRTs requiring targeted support
- Organization of annual workshops for experience sharing and dissemination of best practices

10. Self-Assessment and Oversight

In the framework of ensuring quality and the continuous improvement of CSIRTs' operations, and in accordance with the provisions of this regulation, each CSIRT is obliged to carry out a self-assessment once a year, with the aim of an objective evaluation of its capacities and functions, as well as the identification of areas in need of improvement. This self-assessment shall be conducted for each parameter (O- Organization, H- Human Resources, P- Operational Processes, T - Technical Tools);

The self-assessment must cover all parameters (O – Organization, H – Human Resources, P – Operational Processes, T – Technical Tools). Its aim is to identify gaps, assess progress, and establish the foundation for a concrete improvement plan.

The results of the self-assessment must be documented, and all findings submitted to the National CSIRT to support transparency, data analysis, and the continuous enhancement of sectoral and operator-level CSIRT capabilities.