REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 713 Prot. Tiranë më, 21 . 08 . 2024

U R DH Ë R
Nr. 299 , datë 21 / 08 / 2024

PËR
MIRATIMIN E RREGULLORES "PËR KATEGORIZIMIN E INCIDENTEVE TË SIGURISË KIBERNETIKE"

Në zbatim të pikës 8 të nenit 23, të ligjit nr. 25/2024 "Për sigurinë kibernetike",

U R DH Ë R O J:

1. Miratimin e rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike" sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et Sektoriale, CSIRT-et pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe subjektet e tjera të cilat bëjnë njoftimin vullnetar të incidentit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM

Igli TAFA

REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
KËSHILLI I MINISTRAVE

REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

No. 713 Prot. Tirana on, 21 .08. 2024

ORDER
No. 299, dated 21/08/2024
“ON THE APPROVAL OF THE REGULATION "ON THE CATEGORIZATION OF CYBER SECURITY INCIDENTS"

Pursuant to point 8 of article 23 of the law no. 25/2024 "On Cyber Security",

I ORDER:

1. The approval of the regulation "On the categorization of cyber security incidents" according to the text that is attached to this order and is an integral part thereof.
2. The National Cyber Security Authority, Sectoral CSIRTs, CSIRTs of operators of critical and important information infrastructures, and other entities that make voluntary notification of the incident are charged with the implementation of this order.
3. This order shall enter into force immediately.

DIRECTOR GENERAL

Igli TAFA

Signature

REPUBLIKA E SHQIPËRISË

NATIONAL CYBER SECURITY AUTHORITY

REGULATION

ON THE CATEGORISATION OF CYBER SECURITY INCIDENTS

CONTENTS **page**

Introduction

Effective cyber security management involves a combination of capabilities for the prevention, detection, and response to incidents in cyberspace. In order to achieve a high level of security, a critical or important information infrastructure must be capable to respond to incidents and must have in place appropriate procedures in case an incident occurs that compromises information security.

For an effective resolution of potential cyber security incidents, it is necessary to categorize cyber security incidents, as well as to define the procedure and elements for reporting a cyber security incident.

CHAPTER I

GENERAL PROVISIONS

Article 1
Purpose

The purpose of drafting this regulation is to define the types and categories of cyber security incidents affecting information systems and networks, the format, reporting elements, reporting deadlines, the method of documenting and recording the cyber incidents.

Article 2
Legal basis

This regulation is drafted pursuant to Article 9 letter “g”, Article 17, point 3 letters “b”, “c” and “d”, Article 23, points 3, 4, 5, 6, 8, Article 25 of Law no. 25/2024 “On Cyber Security”.

Article 3
Scope of application and responsible entities

The provisions of this regulation shall be applied by the National CSIRT and the CSIRT of the operator, for classifying, prioritizing, reporting, documenting, and recording the cyber incident. This regulation shall also be applied by other entities which make a voluntary notification of the incident.

Article 4
Definitions

For the purposes of this regulation, the following concepts shall have the following meanings:

1. **“Cyber security incident”**, is any event that compromises the availability, authenticity, integrity, confidentiality of data stored, transmitted, or processed, or of services provided or accessible through networks and information systems.
2. **“Significant cyber incident”**, is an incident which:
a) has caused or is capable of causing severe operational disruption of services or financial loss to the affected operator;
b) has affected or is capable of affecting other natural or legal persons by causing significant material or non-material damage.
3. **“Critical information infrastructure”**, is the entirety of information networks and systems, owned by a public or private authority, that provide services, the compromise or destruction of which would have a serious impact on the health, security, economic well-being of citizens, and the effective functioning of the economy in the Republic of Albania.
4. **“Important information infrastructure”**, is the entirety of information networks and systems owned by a public or private authority, which is not part of the critical information infrastructure, but which may endanger or restrict the provision of the service and the continuity of work, in the event of a breach of information security.
5. **“Cyber threat**”, is a possible event or act that may harm, disrupt, or negatively affect information networks and systems, their users, and other persons.
6. “Operator of critical information infrastructure”, is any natural or legal person who manages critical information infrastructure and meets the requirements set forth in this law.
7. **“Operator of important information infrastructure”**, is any natural or legal person who manages the important information infrastructure and meets the requirements set forth in this law
8. **“Cyber security risk”**, is an event, identifiable with a potential negative effect on the security of information networks and systems.
9. **“Cyber security incident handling”**, are all necessary procedures for the prevention, identification, analysis, response, and recovery from a cyber security incident.
10. “Vulnerability” is a weakness, susceptibility or flaw in ICT products or services that can be exploited by a cyber threat.

CHAPTER II

CATEGORISATION AND TYPES OF CYBER SECURITY INCIDENTS

Article 5
Types of cyber security incidents

1. This regulation defines 3 (three) types of cyber security incidents, as detailed in the table *1* of this regulation.

2. The types of cyber security incidents are as follows:

a) High-impact cyber incidents;
b) Medium-impact cyber incidents;
c) Low-impact cyber incidents;

3. High-impact cyber incidents are severe cyber incidents with a high impact on critical operations or sensitive data. These incidents require the rapid mobilization of incident response teams and may involve notifying stakeholders and regulatory authorities.

4. Medium-impact cyber incidents are cyber incidents with a medium impact that may have limited consequences on the integrity, availability, or confidentiality of systems or data. These incidents require a coordinated response to address vulnerabilities and restore normal services.

5. Low-impact incidents are minor incidents that mainly have minimal and manageable consequences. These incidents can be handled by standard operating procedures without special intervention.

Table 1 Types of cyber security incidents

Types of cyber incidents	Description
HIGH IMPACT CYBER INCIDENTS	Represents a critical situation affecting key operations or sensitive data, causing significant disruption or a major risk to information security. This type of situation requires an immediate and coordinated response from specialized teams, and may also require the immediate notification of the stakeholders and the relevant authorities to minimize further consequences.
MEDIUM IMPACT CYBER INCIDENTS	Represents incidents with a medium impact that may have limited consequences on the integrity, availability, or confidentiality of systems or data. Requires a coordinated response to address vulnerabilities and to restore normal services.
LOW IMPACT CYBER INCIDENTS	Indicates low-impact incidents that generally have minimal and manageable consequences. These incidents can be handled through standard operating procedures without special intervention.

🟨 CYBER INCIDENTS WITH MINIMAL IMPACT

🟧 CYBER INCIDENTS WITH MEDIUM IMPACT

🟥 CYBER INCIDENTS WITH HIGH IMPACT

Legend: Explanation of the table referring to colors

Article 6
Categories of cyber security incidents

1. The categorization of cyber security incidents supports the planning of actions for handling and resolving the cyber security incident, as well as determines the reporting formats depending on the impact of the cyber security incident.

2. This regulation sets out 12 (twelve) categories of cyber incidents as detailed in Table 2 of this regulation. The categories of cyber security incidents are as follows:

a) abusive content;

b) malicious code;

c) gathering of information;

c) attempted intrusion;

d) intrusions;

e) availability;

ë) information content security;

f) fraud;

g) vulnerability;

gj) cryptomining;

h) exfiltration;

i) incident in the testing environment.

3. The definition of cyber security incident categories has been made based on the incident classification published by the European Union Agency for Cybersecurity (ENISA).

Table 2: Categorization of incidents

No.	CATEGORIES OF INCIDENTS	INCIDENT SUBCATEGORIES	DESCRIPTION
1	**Abusive content**	🟨 Spam	The mass distribution of emails without the recipient's consent, which may contain malware or fraudulent schemes aimed at compromising the information security of users
		🟨 Harmful speech	Discrediting or discriminating against an individual (e.g. cyberstalking, racism and threats against one or more

				many individuals).
		Violent/sexual/bullying online content towards children		Child pornography, distribution of violent materials, etc.
		Deliberate misinformation		Distortion of information, which is intended to cause panic.
2	**Malicious code**	Virus towards critical services	Virus towards other services	Software that is intentionally installed on a system for malicious purposes.
		Worm towards critical services	*Worm* towards other services	
		Trojan targeting critical services	Trojan towards other services	
		Spyware towards critical services	*Spyware* towards other services	
		Dialler towards critical services	*Dialler* towards other services	
		Rootkit towards critical services	*Rootkit* towards other services	
		Ransomware targeting critical systems	Ransomware towards other systems	Malicious code, which encrypts data on the computer systems of an end user and/or servers.
		Erasure of data *(wiper)* in critical systems	Erasure of data *(wiper)* in other systems	Malicious code, which aims to destroy or delete the data from the affected system, causing the data to become unusable or the system to no longer function.
3	**The gathering of information**	Scanning		Attempts to identify vulnerabilities within a system. This incident category also includes the testing process, aiming the gathering of the information regarding hosts, services, and accounts. Examples: *fingered*, *DNS Query, RCE, ICMP, SMTP (EXPN, RCPT, etc.),*scanning of ports.
		Sniffing towards critical services	*Sniffing* towards other services	Monitoring and recording of network traffic (interception).
		Social engineering		Collection of information from end users, in a non-technical manner (e.g. fraud, "shoulder surfing", "*tailgating*", "*piggybacking*", Espionage or threats).
4	**Attempted intrusion**	Exploitation of known vulnerabilities to access services critical	Exploitation of known vulnerabilities to access other services.	Attempts to compromise a system or to disrupt services by exploiting vulnerabilities, e.g., backdoor, fragmentation, etc.
		Efforts for *login*		Multiple login attempts, e.g., *Guessing / cracking of passwords, dictionary attack, brute force, RCE.*
		0-day attack towards critical services	0-day attack against other services	Attempted intrusion using an unknown *exploit*.
		Compromise of privileged accounts		Successful compromise of a system or

5	**Interventions**	Compromise of non-privileged accounts		the application (service). This incident may be caused by a known or new vulnerability, but also by unauthorized local access.
		Compromise of an application providing a critical service	Compromise of an application that provides other services	E.g. the execution of techniques *injection* as: *SQL Injection, Command Injection, File Injection, XSS, CSRF, RCE, API attack* etc.
6	**Availability**	DoS/DDoS that has disrupted critical services		DoS is a cyberattack tactic in which a computer system is used to flood a server, service, or network with excessive traffic causing overload and preventing normal use of the service by legitimate users. When more than one infected computer system is involved in this attack, it is categorized as DDoS. DDoS often relies on DoS attacks originating from botnets, although other scenarios also exist, such as DNS Amplification attacks. Some examples are ICMP flood, SYN, Teardrop attacks, and mail-bombing. Availability may also be affected by local actions (destruction, interruption of electricity supply, etc.) - or by natural catastrophic events, spontaneous failures, or human errors, without including malice or negligence.
		DoS/DDoS that has significantly affected critical services and/or disrupted other services		
		DoS/DDoS that has no impact on critical services but has significantly affected other services.		
		Sabotage that has affected the critical system	Sabotage that has affected other systems.	
		Service interruption as a result of an incident during the maintenance process and/or technical incident, such as: Power/Fire/Flooding that has affected critical infrastructure	Services interuption as a result of maintenance and/or technical processes such as: Energy/Fire/Flood that has affected other services	
		Interruption due to natural disasters that have affected critical infrastructure	Interruption due to natural disasters for other services	
7	**Information Content Security**	Unauthorized access to critical services	Unauthorized access to other services	The security of information content can be compromised through the successful breach of accounts, applications, data, and systems. Additionally, attacks can intercept and access the information during transmission (*wiretapping*, *spoofing* or *hijacking*). These attacks may be caused by human errors, configuration errors, or software errors.
		Unauthorized modification in critical services	Unauthorized modification in other services	
8	**Fraud**	Unauthorized use of resources		Unauthorized use of resources for purposes of personal gain unrelated to work activity, such as: chain-letters, use of work emails for registering on platforms not related to work activity, etc.

		Copyright	The provision or installation of copies of unlicensed commercial software or other materials protected by copyright.
		Masquerade	Attack technique in which an individual or process attempts to gain unauthorized access to resources or data by representing themselves as a legitimate entity. This is done by falsifying their identity, such as through the use of stolen data for authentication or manipulation of network protocols to deceive security systems into believing that the traffic or the requests are from an authorized source.
		Phishing/Spear Phishing/Whaling/Smishing/Vishing	Phishing is a fraudulent technique aimed at obtaining sensitive information through emails, messages, or phone calls. These may be targeted (*spear phishing*), directed at high-level executives (*whaling*), or untargeted, with the sender falsely claiming to be a legitimate entity.
9	**Vulnerability**	Visible vulnerabilities to abuse in critical services Visible vulnerabilities for abuse in essential services Visible vulnerabilities for abuse in other services	Vulnerabilities that are disclosed publicly by unauthorized parties and pertain to the services of an information infrastructure.
10	**Cryptomining**	Cryptomining in critical systems or in other systems	The use of resources for profit purposes from the generation of virtual currencies, such as: Bitcoin.
11	**Exfiltration**	Extraction of data from critical infrastructure systems to a C2 server Extraction of data from other infrastructure systems to a server C2	The unauthorized process of data exfiltration from infrastructure systems to a C2 server for malicious purposes.
12	**Incident in the testing environment**	Incident occurring in the testing environment for critical systems or other systems	The misuse of sensitive data in a testing environment such as: In the financial system, when implementing a new system and using real client data, the PCI DSS standard must be applied -> Obtaining permission for data, and ultimately their destruction in a permanent manner.

Article 7

Incident prioritization

1. Based on the types and categories of the cyber incident that occurred and its impact, the incident response teams at the operator and at the National Cyber Security Authority prioritize the cyber incident.
2. Incident prioritization foresees three (3) classifications and depending on the prioritization, a task force is assigned, which will take the necessary measures to respond to the incident and to analyze the incident as shown in the table below:

Table 1: Prioritization of Incidents and the response task force according to the impact of the incident

Classification of incidents	Description	Task Force for Analysis and Response
INCIDENTS WITH HIGH IMPACT	Indicates a serious incident with a high impact on critical operations or sensitive data. Requires rapid mobilization of incident response teams and may involve notifying stakeholders and regulatory authorities.	A minimum of **6 experts**, including at least one expert in monitoring and responding to cyber incidents, one expert in protection and incident management, one expert in cyber incident simulations, one expert in cyber incident investigation, as well as representatives from the affected infrastructure departments and representatives from the affected infrastructure departments. This team is coordinated with the State Police and the relevant law enforcement institutions. National or international partner organizations may be involved in this operation. The National CERT may also become part of the communication and coordination of work, upon the proposal of the Director General.
INCIDENTS WITH MEDIUM IMPACT	Represents incidents with a medium impact that may have limited consequences on integrity, availability or confidentiality of systems or data. It requires a coordinated response to address vulnerabilities and to restore normal services.	At least **4 experts** on standby, including specialists in system recovery, network security, and data protection. This team is coordinated with the State Police and the relevant law enforcement institutions.
INCIDENTS WITH MINIMAL IMPACT	Indicates incidents with low impact that mainly have minimal and manageable consequences. These incidents may be handled	At least **2 experts** on standby to assess and mitigate the incident. This team coordinates with the State Police and the relevant law enforcement institutions.

	by standard operating procedures without any special intervention.	

CHAPTER III

REPORTING OF CYBER SECURITY INCIDENTS

Article 8
Reporting of cyber security incident

1. Operators of critical and important information infrastructures are obliged to report to the national CSIRT and sectoral CSIRT all categories of cyber security incidents as defined in Article 6, point 2 detailed in table no.2, within 4 hours from the moment the incident is identified, and to provide copies of the logs upon request.

2. In the case of significant incidents, operators of critical and important information infrastructures are obliged, within 72 hours from the moment of identification, to update the information and conduct an initial assessment of the significant incident, including its severity, impact, and where applicable, indicators of compromise. With reference to the categories and subcategories of incidents specified in Article 6, point 2, and detailed in Table 2 of this regulation, the following are considered significant incidents: categories 1 to 11 as well as all subcategories of incidents with high and medium impact, specifically as follows:

a. Online content that is violent, sexual, or bullying towards children;
b. Deliberate misinformation;
c. Virus towards critical services / Virus towards other services;
d. *Worm* towards critical services/ *Worm* towards other services;
e. Trojan towards critical services/ Trojan towards other services;
f. *Spyware* towards critical services/ *Spyware* towards other services;
g. *Dialler* towards critical services/ *Dialler* towards other services;
h. *Rootkit* towards critical services/ *Rootkit* towards other services;
i. Ransomware against critical systems/ Ransomware against other systems;
j. Erasure of data *(wiper)* in critical systems/ Erasure of data *(wiper)* in other systems;
k. *Sniffing* towards critical services;
l. Exploitation of known vulnerabilities to access critical services / Exploitation of known vulnerabilities to access other services;
m. Attempts for *login;*
n. *0-day attack* towards critical services/*0-day attack* towards other services;
o. Compromise of privileged accounts/ Compromise of non-privileged accounts;

p. Compromise of an application providing a critical service / Compromise of an application providing other services;

q. DoS/DDoS causing interruption critical services/DoS/DDoS that has significantly affected critical services and/or has interrupted other services;

r. Sabotage that has affected the critical system;

s. Service interruptions as a result of an incident during the maintenance and/or technical process such as: Power/Fire/Flood that has affected critical infrastructure;

t. Interruption due to natural disasters that have affected critical infrastructure;

u. Unauthorized access to critical services/ Unauthorized access to other services;

v. Unauthorized modification in critical services/ Unauthorized modification in other services;

w. Unauthorized use of resources;

x. Visible vulnerabilities to abuse in critical services / visible vulnerabilities to abuse in important services;

y. Cryptomining in critical systems or in other systems;

z. Extraction of data from critical infrastructure systems to a C2 server / Extraction of data from other infrastructure systems to a C2 server;

3. Reporting according to points 1 and 2 of this article shall be carried out in accordance with the format in annexes 1 and 2 attached to this regulation.

4. To determine the significance of the impact of a cyber incident, the following parameters are evaluated:

a) the number of users affected by the service disruption;

b) duration of the incident;

c) geographical scope in relation to the area affected by the incident;

ç) the degree of disruption of service operation;

d) the extension of influence in economic and social activities;

dh) the dependency of the sectors on the services provided by the information infrastructure operator;

e) the importance of maintaining an adequate level of service, taking into account the availability of alternative means for providing this service.

5. Operators of critical and important information infrastructures, within one month from the notification of the incident according to points 1 and 2 of this Article, must submit to the national CSIRT a final report, which includes:

i. a detailed description of the incident, including its significance and impact;

ii. the type of threat or the main cause that may have caused the incident;

iii. the measures applied and the ongoing measures for reducing the consequences;

iv. where applicable, the cross-border impact of the incident.

6. In cases of an ongoing cyber incident, the operator of the information infrastructure affected by this incident, in addition to the obligation to submit the final report at the time of closure of the cyber incident pursuant to point 5 of this article, is also obliged to submit a progress report to the National CSIRT.

Article 9
Cyber incident reporting procedure

In the event of a cyber security incident, the contact point of the information infrastructure where the incident occurred reports the cyber security incident to the National CSIRT through:
a) the reporting platform,
b) official letter,
c) the email
d) telephone, the dedicated number at the National CSIRT.

Article 10
Voluntary incident notification

1. In addition to operators of critical and important information infrastructures, other entities may voluntarily report cyber incidents to the national CSIRT.
2. Voluntary reporting does not create consequences or obligations for the reporting entity, had the report not been made.
3. Other entities report the cyber incident according to the provisions of Article 8 of this regulation, as well as according to the reporting formats specified in Annex 1, Annex 2 of this regulation, and the Report according to point 5 of Article 8 of this regulation.
4. The procedure for reporting a cyber incident by other entities is carried out through:
   a) official letter,
   b) the email.
   c) telephone, the dedicated number at the National CSIRT.

Article 11
Incidents that shall not be reported

The following cyber incidents shall not be necessary to be reported:

a. A malware or virus on an employee’s device that can be easily remediated, e.g.: (a single case of a user device with a virus that is automatically detected and easily cleaned)
b. Short-term interruptions in non-critical services, e.g.: (equipment that experienced an unplanned interruption which was easily restored in a short period of time)
c. Employees violating specific institutional specific policies or guidelines for internet use, e.g.: (individual users who browse inappropriate but not illegal or malicious websites during working hours)
d. Unexploited vulnerabilities in non-critical information systems, services or networks, e.g.: (a vulnerability in a user's desktop that has not been exploited)

CHAPTER IV

DOCUMENTATION OF CYBER SECURITY INCIDENTS

Article 12
Documentation and registration of the incident by critical infrastructure operators

1. Operators of critical and important infrastructure shall document all significant information and the chronology of the incident.
2. Incident documentation shall be considered as documenting all relevant information regarding the incident, including the time of occurrence, the nature of the incident, the systems, services, data, or processes that are affected, and the actions taken up to that point.
3. The registration of incident documentation by the operators shall be kept in accordance with the register format defined in Annex 3, which is part of this regulation.

Article 13
The incident register by AKSK

The data on reported incidents shall be collected and documented in the electronic register administered by the National Cyber Security Authority, according to Annex 4 of this regulation, for the purpose of:

a) Taking measures to prevent similar incidents in the future through analysis of the incident.

b) The identification of occurred incidents for the maintenance of statistics, which provide an overall picture of the type, size, and frequency of cyber incidents.

ANNEX 1

Cyber incident reporting form within 4 hours from identification			
Section 1: Organization data			
Name of the Organization:		Sector:	
Type of information infrastructure:	□ Critical □ Important		
Public IP of the infrastructure:			
Number of Employees: □ 0-50 □ 51-100 □ 101-500 □ 500+			
Have you contracted third parties for the security of your company:	□ Yes □ No	If yes, what is the name of the company	
Does your organization apply cyber security?	□ Yes □ No	If yes, what is the name of the company where you are insured?	
Reporter's data			
First Name Last Name:		Job position:	
E-mail:		Cel:	
The incident is being handled by the Sectoral CSIRT	□ Yes □ No	Sectoral CSIRT contact point	
The type of assistance you are requesting from AKSK			
□ Reporting only	□ Handling	□ Recommendations	
Section 2 : Incident Details			
Date and time of the incident detection		Date and time of incident reporting	
Identification of the incident			
□ Notifications from devices	□ SIEM / SOC	□ Log analysis	
□ Notification from third parties	□ Notification from the user	□ Help Desk	
□ Other: ________________________________			
Current status of the incident			
□ It is occurring	□ It is occurring and is under	□ It has occurred and is under	□ It has occurred

	control	control	
Do you have a backup?	□ Yes	□ No	

Incident category			
□ Abusive content	□ Malicious code	□ Collection of information	□ Intrusion attempts
□ Intrusions	□ Availability	□ Information Content Security	
□ Fraud	□ Vulnerability	□ Cryptomining	
□ Exfiltration	□ Incident in the testing environment		
Incident subcategory			
Description of the incident			
The affected systems or assets			
Please include 5-10 lines of "time-stamped logs" in plain ASCII			

ANNEX 2

The form for reporting a cyber incident within 72 hours from identification

Section 1: Impact of the incident

Number of affected users:	□ 0-50 □ 51-100 □ 101-500 □ 500+
Duration of the incident:	
Geographical scope in relation to the area affected by the incident:	
Degree of service disruption:	
Impact on economic and social activities:	□ Yes □ No
Dependency of other sectors on the services provided by the operator of the information infrastructure:	□ Yes □ No
A sufficient level of service has been maintained:	□ Yes □ No
Financial impact of the incident:	
Legal impact:	
Reputational impact:	□ Low □ Intermediate □ High □ Critical

Section 2: Classification of the incident

What was the initial access vector of the attack (Initial Access Vector)?	
Do you have evidence for *priviledge escalation* or *lateral movement* ?	

Section 3: Information on the attack actor

Do you know the group / attacker?	□ Yes □ No	If yes, what is the name	
Have you communicated with the attack group?	□ Yes □ No		

Technical details

Malware variant		IoC	
Exploited CVEs		Encryption method (in the case of ransomware):	
Exfiltrated data	□ Yes □ No	Website where the data have been exfiltrated	

Response and recovery

Backup has been used	□ Yes □ Partially □ No
Has the Initial Access vector been closed?	□ Yes □ No
Describe the steps taken for incident response	

ANNEX 3

The incident register administered by the operator		
No.	Format elements	Explanation
Up to 30 minutes from the detection of the incident		
1	Incident ID	Unique identifier for incident tracing
2	Date and Time of Discovery	The date and time when the incident was first identified or detected.
3	Detection Method	How was the incident detected (e.g., intrusion detection system, employee reporting, automatic alert).
4	Reported by	Name and contact information of the person or system that reported the incident.
After 30minutes from the detection of the incident		
5	Category of Incident	Category of cyber incident.
6	Subcategory of the Incident	Subcategory of the cyber incident.
7	Description of the Incident	Detailed description of the incident, including what happened and which systems, services, data, or processes are affected.
8	Affected Assets	List of assets affected by the incident (e.g., systems, networks, devices, data).
9	Level of Severity	Severity of the incident based on predetermined criteria (e.g., Low, Medium, High, Critical).
10	Incident Coordinator	Name and role of the individual responsible for overseeing the incident response process.
11	Cyber Incident Response Team	Members of the incident response team and their roles.

12	Initial response	Immediate actions taken in response to the incident (e.g., isolation of affected systems, revocation of rights of access, etc.).

13	Communication	Recording of communications during the incident, including internal notifications and external communications with stakeholders, clients, or authorities.
14	Technical Analysis	Detailed analysis of the incident, including the attack vectors used, exploited vulnerabilities, and the compromised data.
15	Isolation, Deletion and Recovery	The specific steps taken to isolate the incident, eliminate threats and restore affected systems to normal operation.
16	Resolution and Closure	Details regarding the resolution of the incident, including when and how normal operations were restored.
17	Incident report	The incident report documents the incident, analyzes its causes and consequences, as well as identifies important lessons learned from it that can help in the prevention of future incidents, in linked format.
18	Post-Incident Activity	Actions taken such as post-incident analysis, lessons learned, and measures to prevent recurrence.
19	Review and Update	The date when the incident and the response process will be reviewed to update policies, procedures, and controls based on lessons learned.

ANNEX 4

The incident register administered by AKSK

No.	Format elements	Explanation
Up to the 30 minutes from the detection of the incident		
1	Incident ID	Unique identifier for incident tracking
2	Infrastructure	The infrastructure where the incident occurred
3	Date and Time of Detection	The date and time when the incident was first identified or detected.
4	Method of Detection	How was the incident detected (e.g., intrusion detection system, reporting by employee, automatic alert).
5	Reported By	Name and contact information of the person or system that reported the incident.
After 30 minutes from the detection of the incident		
6	Incident Category	Category of the cyber incident.
7	Incident Subcategory	Subcategory of the cyber incident.
8	Description of the Incident	Detailed description of the incident, including what happened and which systems, services, data, or processes are affected.
9	Affected Assets	List of assets affected by the incident (e.g., systems, networks, equipment, data).
10	Level of Severity	The severity of the incident based on predefined criteria (e.g., Low, Medium, High, Critical).

11	Incident Coordinator	Name and role of the individual responsible for overseeing the incident response process.
12	Cyber Incident Response Team	Members of the incident response team and their roles.
13	Initial response	Immediate actions taken in response to the incident (e.g., isolation of affected systems, revocation of access rights, etc.).
14	Communication	Recording of communications during the incident, including internal notifications and external communications with stakeholders, clients, or authorities.
15	Technical Analysis	Detailed analysis of the incident, including the attack vectors used, exploited vulnerabilities, and compromised data.
16	Isolation, Deletion, and Recovery	The specific steps taken to isolate the incident, eliminate threats, and restore the affected systems to normal operation.
17	Resolution and Closure	Details on the resolution of the incident, including when and how normal operation was restored.
18	Incident report	The incident report documents the incident, analyzes its causes and consequences, as well as identifies important lessons that may help in its prevention of future incidents, in linked format.
19	Post-Incident Activity	Actions taken such as post-incident analysis, lessons learned, and measures to prevent recurrence.
20	Review and Update	The date when the incident and the response process will be reviewed to update policies, procedures, and controls based on lessons learned.