REPUBLIC OF ALBANIA

NATIONAL CYBER SECURITY AUTHORITY

No. 2459 Prot . Tirana, on 27.08.2025

ORDER

No.229, date 27.08.2025

ON THE APPROVAL OF THE PROCEDURE ON COMMUNICATION WITH THE PUBLIC ON CYBER INCIDENTS THAT AFFECTS THE PUBLIC INTEREST

Pursuant to letter a, point 1, article 2 and article 99 of law no. 44/2015 “Code of Administrative Procedures of the Republic of Albania” and point 2, article 26 of law no. 25/2024 “On cyber security”,

I ORDER:

1. The approval of the procedure " On communication with the public about cyber incidents that affect the public interest", according to the text attached to this order, an integral part thereof.

2. The Directorate of Cyber Security Analysis, Directorate of Incident Monitoring and Response, the Operational Center SOC C-SIRT, and the Directorate for Coordination of International Projects and Strategic Development of Cybersecurity, of the National Cyber Security Authority, shall be charged with the implementation of this order.

3. This order shall enter into force immediately.

DIRECTOR GENERAL

Igli Tafa

PROCEDURE ON COMMUNICATION WITH THE PUBLIC ON CYBER INCIDENTS THAT AFFECTS THE PUBLIC INTEREST

This procedure aims to determine the manner of communication with the public in cases of cyber incidents that have or may have an impact on the public interest. It aims to ensure institutional transparency, accurate and timely information to the public, maintaining the trust of citizens and stakeholders, and minimizing the negative impacts that may be caused by disinformation or panic created in the public.

The procedure applies to all cyber incidents that affect or risk affecting critical and important information infrastructures, critical services, personal or sensitive data, as well as the normal functioning of services provided, with importance for the public.

A 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, referred to in Law No. 25/2024 "On cyber security". A cyber incident that affects the public interest is considered any incident that affects citizens, users, clients or critical services with a wide impact on the public and that requires official communication in order to prevent its escalation and minimize the consequences of the incident.

Communication with the public in the event of cyber incidents must be accurate, clear, transparent and responsible. The information published must be verified, understandable to the general public and proportionate to the level of risk and impact of the incident. This communication must be in accordance with the legislation in force on cybersecurity, the legislation in force on the right to information and the protection of personal data and the legislation in force on classified information.

In accordance with points 1 and 2 of article 26 of law no. 25/2024 "On cyber security", the National CSIRT at the National Cyber Security Authority, after consulting with the information infrastructure operator, informs the public about incidents occurring in critical and important information infrastructures when the information is necessary for public awareness, to prevent a significant incident, to handle the incident or when it affects the public interest, while always maintaining the confidentiality of the incident data. The procedure for carrying out the communication is followed according to the steps set out in this document.

COMMUNICATION PROCEDURE

Step 1: Cyber incident confirmation

The National CSIRT, as the structure responsible for monitoring, analyzing and managing cyber threats, vulnerabilities and incidents at the national level, confirms the cyber incident and implements the procedure for its management. If, after analyzing the cybersecurity incident, it results that there are significant impacts on the public such as service interruption, compromise of personal data, financial impact and other impacts affecting the public interest, the Authority continues to inform the public through official communication channels, after consulting with the information infrastructure operator.

Step 2: Preparing the initial public notification

The Authority prepares the initial notification which contains a general description of the incident, the services or categories of users and citizens affected, the measures taken to manage the situation and, if necessary, information on further steps. This notification aims to inform the public about the incident and the emergency measures to be taken to minimize the risk, without revealing details that could jeopardize safety or the analysis of the incident, as well as to prevent the creation of panic among citizens.

Step 3: Continuous update on the situation

When deemed necessary, during incident management, the Authority updates information to the public, depending on the development of the situation and the level of public interest. These updates include information on the progress of the resolution of the incident, additional security measures taken and, when necessary, practical recommendations for citizens or affected entities.

Step 4: Publication of the incident report and final announcement

After finalizing the report of the cyber incident analysis, the Authority publishes the report on its official website. In cases where this report contains sensitive data, the process of anonymizing the data is carried out before its publication. A final notification is also published, which presents a summary of the incident, the impact assessment and recommendations to avoid similar incidents in the future.

Communication with the public is carried out through the institution's official channels, which include the following:

- official *website;*
- the institution's social networks;
- press release, as appropriate.

The Authority identifies inaccurate information or disinformation in the media and social networks regarding the incident and takes measures to correct them through official and coordinated communications.