**DECISION**

**No. 723, dated 3.12.2025**

**ON THE ESTABLISHMENT, ORGANIZATION, AND FUNCTIONING OF THE CYBERSECURITY EMERGENCY AND CRISIS RESPONSE TEAM**

Pursuant to article 100 of the Constitution and paragraph 4, article 29 of law no. 25/2024 "On Cybersecurity", upon the proposal of the Prime Minister**,** the Council of Ministers

DECIDES:

I. TO ESTABLISH THE CYBERSECURITY EMERGENCY AND CRISIS RESPONSE TEAM – CERT

1. Within the National Cybersecurity Authority (hereinafter, NCSA), the Cybersecurity Emergency and Crisis Response Team (hereinafter, CERT) is established and operates as an ad-hoc, case-by-case structure responsible for a timely and efficient handling of cybersecurity emergencies and crises in the Republic of Albania.
2. CERT is chaired by the National Cybersecurity Authority and is composed of:
a) representatives from public institutions, as follows:
   i. Ministry of Interior;
   ii. Ministry of Defence;
   iii. Ministry for Europe and Foreign Affairs;
   iv. Electronic and Postal Communications Authority;
   v. State Intelligence Service;
   vi. National Agency for Information Society;
   vii. Commissioner for the Right to Information and Protection of Personal Data;
   viii. State Police;

b) cybersecurity experts, information technology experts, and OT experts (*operational technology*), whose engagement shall be carried out in accordance with the provisions of points 7–12 of this Chapter.
3. The heads of the institutions referred to in letter "a", point 2, of this Chapter shall, within 5 (five) days from the entry into force of this decision, submit to the NCSA the names of their institutional representatives, and shall update the list in case of changes within 5 (five) days from the occurrence of such changes.
4.The NCSA, by order of the director general, based on the cybersecurity emergency or crisis situation, on a case-by-case basis, and taking into consideration the complexity of the situation, the nature of the attack, and the number of affected infrastructures, shall determine the number of experts to be included in the CERT team and their respective profiles.
5.The following criteria must be met by cybersecurity experts, information technology experts, and OT experts to be part of the CERT:
a) General criteria:

i) have full legal capacity to act;
ii) hold a Level six qualification of the Albanian Qualifications Framework, "Bachelor" degree or an equivalent qualification, according to the legislation on higher education, in the field of information and communication technologies (ICT) or in other fields related to the knowledge specified in letter "b" of this point;
iii) have not been convicted by a final court decision for the commission of a criminal offense;
iv) meet the criteria of integrity and trustworthiness regarding the protection of confidentiality and integrity of information, as well as personal background verification.
b) Professional criteria:
i) have at least 7 (seven) years of professional work experience;
ii) possess professional skills in the field of cybersecurity and information technology;
iii) possess in-depth knowledge in the field of cybersecurity and information technology, as follows:

- knowledge of computer systems, virtual systems, and operating systems such as Linux, Windows Server, virtual systems like VMware or KVM, HyperV, etc.;
- knowledge of computer network protocols;
- knowledge of applications and platforms used in information systems and networks;
- knowledge in the field of information security;
- knowledge of cyber-attack tactics, techniques, and procedures (TTPs), and applications used for this purpose;
- knowledge of cyber-forensics techniques;
- knowledge in incident management and personal data protection, such as Log Analysis, SIEM, etc.;
- knowledge of cybersecurity crisis management;
- knowledge of Python and object-oriented programming languages;
- knowledge of Artificial Intelligence/AI, Machine Learning, Blockchain, Cryptography, Autonomous Vehicles/Machines, etc.

c) To meet the criteria mentioned in letters "a" and "b", of point 5, of this Chapter, the applicant must submit the following documentation:
i) an identification document (ID card/biometric passport);
ii) criminal record certificate, court certificate confirming they are not under judicial proceedings, and prosecutor's office certificate confirming they are not under criminal investigation, as well as a self-declaration confirming their criminal status;
iii) a copy of the diploma;
iv) a copy of the employment booklet or a certificate from the tax authorities showing professional experience;
v) a curriculum vitae with professional experience (CV);
vi) a self-declaration regarding integrity and reliability in preserving the confidentiality and integrity of information;
vii) copies of certifications in the field of cybersecurity and information technology;
viii) the submission of the following certifications constitutes an advantage:

- certifications in network administration and systems management;
  ii. certification in information security systems administration;

- professional cybersecurity certifications such as Security+, CISA, CISSP, CISM, CEH, OSCP, CHFI, or equivalent;
- certifications in cybersecurity incident management;
- certifications in incident investigation and digital forensics;
- certifications in Artificial Intelligence/AI;
- certifications in Machine Learning;
- certifications in Blockchain;
- certifications in Cryptography;
- certifications in Autonomous Vehicles/Machines;
- certifications focused on the cybersecurity of industrial and critical systems (SA/IEC Cybersecurity Expert);
- certifications in the protection of OT and ICS systems (GIAC Global Industrial Cyber Security Professional);
- certification in SCADA systems architecture and security (Certified SCADA Security Architect);
- any other certification relevant for cybersecurity incident management.

ç) The documents required in letter "c" of point 5 of this Chapter must be submitted in original copies or certified true copies of the original.

6. NCSA, within 1 (one) week from the entry into force of this decision, shall publish on its official website the call for participation of cybersecurity experts, information technology experts, and OT experts, for the purpose of preparing the list of cybersecurity, IT, and OT experts who will be part of the CERT, whereas, with regard to international experts, the call will also be published on the official pages of international cybersecurity forums.

7. The announcement shall contain detailed information regarding the criteria that cybersecurity experts, IT experts, and OT experts must meet, the documents they must submit, and the manner and format of submission.

8. The announcement shall remain open for a period of 1 (one) month.

9. After the submission of the documentation to the NCSA, the latter, within 30-day time limit, shall evaluate it based on the fulfilment of the criteria set out in this decision, as well as through an interview process, and shall thereafter notify the selected experts.

10. NCSA shall prepare the list with the names and contact details of cybersecurity, IT, and OT experts, from which the experts who will be part of the CERT shall be selected.

11. Experts included in the CERT list who, in the performance of their duties under the provisions of this decision, will have access to accredited communication and information systems where classified information is processed, are required to follow the procedures for obtaining a "Personnel Security Clearance Certificate", in accordance with the provisions of the legislation on classified information.

12. NCSA shall issue the call for cybersecurity experts, IT experts, and OT experts within January of each year.

## II. THE METHOD OF ORGANIZATION AND FUNCTIONING OF THE CYBERSECURITY EMERGENCY AND CRISIS RESPONSE TEAM

1. CERT convenes, under the NCSA, in the event of a cybersecurity emergency or crisis to prepare an action plan, manage, and resolve the cybersecurity emergency or crisis.
2. CERT meetings are chaired by the Director General of the NCSA, or in their absence, by a Director with a technical profile from the NCSA.
3. A technical secretariat of the CERT is established and operates within the CERT, responsible for preparing meeting materials and notifying CERT members of meetings. The composition of the CERT technical secretariat is determined by order of the Director General of the National Cybersecurity Authority.
4. During cybersecurity emergencies and crises, inter-institutional communication is maintained using official communication channels, alternative channels, and backup channels. The technical secretariat keeps the minutes of the meetings, and preserves the content of communications, notifications, and the requests received or sent via information technology tools.
5. To respond to cybersecurity emergencies and crises, upon the request of the CERT, cybersecurity experts, IT experts, and OT experts from other state institutions may be engaged according to their field of responsibility, to respond to emergencies and crises within the relevant sectors.

## III. FUNCTIONS OF THE CYBERSECURITY EMERGENCY AND CRISIS RESPONSE TEAM (CERT)

The functions of the CERT are as follows:

a) Develops an emergency and cybersecurity crisis action plan;
b) Manages and resolves cybersecurity emergencies and crises while maintaining confidentiality at all times;
c) Provides support in drafting recommendations for restoring information systems and networks in information infrastructures to normal operation following a large-scale incident or during a cybersecurity emergency or crisis.

## IV. FINAL PROVISIONS

The National Cybersecurity Authority, as well as the institutions referred to point 2(a) of Chapter I, are tasked with implementing this decision.

This decision shall enter into force upon its publication in the Official Journal.

**PRIME MINISTER**
EDI RAMA