International Cooperation Policy

Address: "Papa Gjon Pali II" Street, no. 3, Tirana
Website:www.aksk.gov.al Email:info@aksk.gov.al
Tel./Fax: 04 2221 039

Table of Contents

1. Purpose

The purpose of this policy is to emphasize international cooperation by effectively addressing international threats and cyber challenges.

The policy aims to establish a clear, structured, and implementable framework for how the Republic of Albania builds and develops international cooperation in the field of cybersecurity, to effectively address international threats and cyber challenges.

2. Scope of application

This policy is implemented within the framework of the national cybersecurity strategy 2025-2030 and regulates the principles of international cooperation between responsible national security and defense institutions and international partners, with the aim of building and maintaining a secure, stable and resilient cyberspace.

The policy aims to promote information exchange, coordination of actions and harmonization of practices to address increasingly complex and cross-border cyber threats.

3. Fundamental Principles

The implementation of this policy is based on several fundamental principles that underpin any form of international cooperation. First, the national sovereignty and strategic interests of the Republic of Albania are respected. Cooperation is developed on the basis of mutual trust, transparency and mutual benefit with international partners.

Particular importance is attached to maintaining the confidentiality of the information exchanged, especially when it comes to sensitive data or information related to national security. Any cooperation is carried out in full compliance with national legislation and Albania's international obligations, based on the principles of reciprocity, transparency and continuous improvement of institutional capacities.

4. Roles and Responsibilities

4.1 Role of the National Security Authority

The National Cyber Security Authority plays a central role in coordinating international cooperation in the field of cybersecurity. NCSA is the institution that identifies the country's strategic needs in this field, proposes cooperation initiatives with international partners and oversees the implementation of signed agreements. NCSA also represents Albania in international cybersecurity networks, forums and mechanisms and is responsible for monitoring the implementation of this policy and reporting on the progress achieved.

4.2 Role of the National CSIRT

The National CSIRT plays a primarily operational role in international cooperation by actively engaging in international CSIRT networks, exchanging technical information on incidents, vulnerabilities and threats. Through this cooperation, the CSIRT contributes to increasing national technical capacities and ensures that Albania benefits from the experiences and best

practices of partner countries. The CSIRT also participates in international exercises simulating cyber incidents, with the aim of improving response preparedness.

4.3 Role of the Ministry for Europe and Foreign Affairs

The Ministry for Europe and Foreign Affairs contributes to this policy through the dimension of cyber diplomacy. It supports Albania's representation in international organizations and structures, and assists in the coordination of diplomatic relations related to international agreements in the field of cybersecurity. In this way, it ensures that technical cooperation is harmonized with the country's foreign policy.

4.4 Role of other public institutions

Other public institutions, according to their respective mandates, participate in the implementation of this policy by contributing to international projects, initiatives, or mechanisms. They are required to report periodically on the activities they carry out within the framework of international cybersecurity cooperation.

5. Elements of International Cooperation Policy

Bilateral and Multilateral Agreements:

Promoting and developing bilateral and multilateral agreements with states, international organizations and structures, with the aim of cooperating in the field of cybersecurity, exchanging information on cyber threats, conducting joint exercises and coordinating the response to cyber incidents.

Participation in International Forums:

Active participation in international forums, organizations and conferences related to cybersecurity, such as the United Nations, INTERPOL, NATO Cyber Defense Cooperation Center (CCDCOE), and the Global Forum for Cyber Expertise (GFCE), Incident Management Forum, etc.

Global Cybersecurity Rules and Standards:

Harmonization of national policies, regulatory frameworks and practices with international cybersecurity rules and standards, including ISO/IEC standards and the NIST framework for risk management and information security.

Legislation and Enforcement of the Law on Cross-Border Cybercrimes:

International cooperation for the development and harmonization of legislation on cybercrimes, including international legal assistance mechanisms, with the aim of preventing, investigating and prosecuting cybercrimes of a cross-border nature.

In this context, initiatives for technical assistance and capacity building are supported, especially for developing countries, in order to increase global cybersecurity.

Cybersecurity Information Sharing, Threat Intel and Operational Coordination

Participation in international mechanisms and networks for sharing information on cyber threats, vulnerabilities, and incidents is carried out in accordance with the applicable legislation on information and data protection.

Operational coordination with international counterparts is promoted for a joint and coordinated response to cyber incidents, as well as the development of joint research and development projects in the field of cybersecurity.

Cyber diplomacy is an instrument for addressing issues related to cyber security and stability at the international level.

Trainings and Academic Exchanges:

Participation in international training, education and academic exchange programs, with the aim of strengthening professional and institutional capacities in the field of cybersecurity.

Support for International Cybersecurity Initiatives:

Support and encourage international initiatives that aim to strengthen cyber stability and protect critical information infrastructures at the global level.

6. References

This policy is based on national legislation on cybersecurity, the National Strategy for Cybersecurity, as well as recognized international practices and standards in the field of international cooperation on cybersecurity.

7. Review Frequency

This document should be reviewed at least once a year or when there are significant changes to the institution's information security management system.