**REPUBLIC OF ALBANIA**
**NATIONAL CYBER SECURITY AUTHORITY**

# Policy on Strengthening Institutional Capacities for Cybersecurity

# Table of Contents

## 1. Introduction

The Policy on Strengthening Institutional Capacities for Cybersecurity represents an important step toward enhancing cybersecurity in Albania. This policy aims to increase institutional capacities for the prevention, mitigation, and effective response to cyber risks and incidents, as well as the protection of critical and important information infrastructures, thereby contributing to the strengthening of national security.

## 2. Policy Description

The Policy for Strengthening the Capacities of Institutions for Cybersecurity aims to address challenges regarding the technical and human capacities of public and private institutions at the national level by providing for measures that should be taken to increase capacities in order to strengthen cybersecurity.

With the advancement of technology development and the digitalization of services in Albania, risks in cyberspace have also increased. Recently, an increasing trend of cyber incidents targeting critical and important information infrastructures, both public and private, has been observed. With the increase in cyber risks and incidents, an effective response to them is necessary, but for this, institutional technical and human capacities are needed. The lack of necessary capacities and resources constitutes a challenge that must be addressed. The consequences that incidents may have on information infrastructures can seriously affect national security and the economy, consequently, it is necessary to take action to increase the capacities of institutions at the national level to guarantee security and protection from various attacks by malicious actors in cyberspace.

In this context, the Policy for Strengthening the Capacities of Cybersecurity Institutions will address the lack of capacities by defining concrete measures to increase human capacities, technical capacities, as well as measures to create the necessary mechanisms and increase national and international cooperation, in order to build and strengthen capacities.

## 3. Mission and Goals

The mission of this policy is to enhance the capacities and effectiveness of institutions responsible for cybersecurity in Albania to prevent and counter cyber threats, with the aim of safeguarding national stability and security.

The policy goals are:

- Strengthening existing capacities and building new institutional capacities in the field of cybersecurity
- Increasing capacities, measures and technical means to protect and respond to cyberattacks
- Increasing capacity buildings specialized in cybersecurity
- Creating and strengthening national and international cooperation mechanisms with the aim of increasing capacities in the field of cybersecurity

## 4. Scope of Application

This policy applies to all public institutions, state agencies, and structures that provide digital public services or manage systems and data essential to the functioning of the state. The policy aims to address a comprehensive approach to capacity building for both public and private institutions.

The policy serves as a guiding document for the development of internal capacity-building plans and for the integration of cybersecurity into human resources management, technology policies, and institutional organization.

## 5. Fundamental Principles

The implementation of this policy is based on the principle that institutional capacities should be built in a sustainable and long-term manner. The policy emphasizes the importance of continuous professional development of staff and the continuous adaptation of institutions to technological developments.

Another fundamental principle is the integration of cybersecurity into existing institutional governance structures, so that it is not treated as a secondary function, but as an integral part of management and decision-making.

## 6. Concrete Tools and Measures

This policy is in line with the vision and objectives of the National Cyber Security Strategy 2025-2030 and reinforces measures to increase institutional, public and private capacities.

Concrete measures and actions will be detailed in the Action Plan of the National Cyber Security Strategy, according to needs and priorities. The measures that will be taken to implement this policy include:

- Measures to increase human resource capacities
- Measures to strengthen technical capacities
- Measures to establish the necessary mechanisms and increase national and international cooperation, in order to build and strengthen capacities.

Measures to increase human resource capacities include:

- Creating a sustainable education system for young people seeking to specialize in the field of cybersecurity, through the establishment and strengthening of the National Cyber Security Academy, and increasing the capacities and quality of educational institutions in the field of cybersecurity in the country.
- Designing study and training programs in the field of cybersecurity with the aim of creating a new generation of cybersecurity experts and continuously updating existing higher education curricula in the field of cybersecurity.
- Organizing and implementing national training programs and conducting joint cyber exercises on the prevention, management, response and investigation of cyber incidents with staff responsible for cyber security of public and private institutions in the country, including all sectors.
- Organizing training and exercises (Table Top Exercise) for high-level decision-making structures, related to cyber crisis communication and management.
- Training to increase the capacities in the field of cybersecurity and cyber diplomacy of the staff of responsible institutions.

Measures to increase technical capacities include:

- Increasing the budget for CSIRT[1]national and sectoral CSIRTs to ensure the necessary technical tools and security infrastructures for monitoring, protecting, managing, and responding to cyber incidents.
- Building the technical capacities of the National Security Operations Center (National SOC) for proactive and reactive monitoring, as well as handling cyber incidents.
- Optimization of security infrastructures and expansion of government sector coverage capacities.
- Equipping institutions with the necessary hardware and software tools and infrastructures in accordance with the latest standards, for the detection and prevention of potential cyber attacks.
- Developing technical monitoring, assessment, analysis and response capacities of CSIRTs and the Cybercrime Investigation Directorate at the State Police.
- Establishing laboratories for malware analysis, cyber forensics, and cyber incident simulation.
- Creating a dedicated platform for reporting illegal online content targeting children and young people, in cooperation with the State Police.
- Implementing advanced and improved techniques and procedures for cybersecurity and cyber protection;
- Conducting continuous risk, compliance, and technical capacity analyses to identify and address ongoing needs.

Measures to Establish Necessary Mechanisms and Enhance National and International Cooperation include:

- Drafting and signing cooperation agreements with states, agencies, as well as regional or international centers in the field of cybersecurity with the aim of increasing capacities.
- Drafting and signing cooperation agreements with universities regarding the updating of curricula and the development of scientific research in the field of cybersecurity.
- Cooperating with the Ministry of Education and Sports to enable a sustainable education system in cybersecurity (establishment and accreditation of the National Cybersecurity Academy, curriculum improvement, and enhancement of higher education quality related to cybersecurity study programs).
- Deepening cooperation with international organizations for the exchange of technical expertise and information regarding cyber threats and vulnerabilities, as well as for responding to cybersecurity incidents.
- Signing cooperation agreements in the field of security and cybercrime between relevant institutions at the national level, with the aim of increasing capacities and exchanging knowledge and information.
- Implementing joint projects and initiatives with international partners to strengthen cybersecurity capacities.

## 7.Collaboration and Partners

National partners for the implementation of this policy include public and private sector entities, civil society organizations, and experts who contribute knowledge and experience. At

[1] Computer Security Incident Response Team (CSIRT)

the international level, partners include international organizations of which Albania is a member or candidate country, as well as international agencies of allied and strategic partner governments, with the aim of strengthening defensive capacities and responses to cyber threats and enhancing national cybersecurity.

## 8. Monitoring and Evaluation

Monitoring of the policy will be conducted through analysis of the implementation of actions foreseen in this policy and in the Action Plan of the National Cybersecurity Strategy that align with its objectives, through meetings with responsible implementing institutions and monitoring reports. Monitoring is carried out based on semi-annual or annual reports and reporting from institutions responsible for implementing the measures. Upon completion, a monitoring report is prepared, and relevant conclusions are drawn, based on which improvements to measure are proposed when deemed necessary.

## 9. Financing and implementation calendar

The implementation of activities foreseen under this policy will be financed through the state budget and various donors. Well-planned financing will enable the achievement of results in line with the objectives of this policy and the National Cybersecurity Strategy.

This policy will be implemented in accordance with the timelines set out in the implementation calendars for each of the envisaged measures. The implementation calendar is prepared annually and therefore covers a one-year period.

## 10.References

This policy is based on national cybersecurity legislation, the National Cybersecurity Strategy, and internationally recognized practices and standards in the field of cybersecurity capacity development.

## 11.Review Frequency

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