REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

Communication Policy

Table of Contents

1. Introduction

The Communication Policy constitutes an essential component of the national strategy to address the growing challenges of cybersecurity. It defines the framework for communication and coordination among public institutions, the private sector, and the public, with the aim of addressing cyber threats, managing incidents and raising awareness about cybersecurity.

Through the definition of communication protocols, crisis communication plans and cooperation mechanisms, the policy aims to strengthen the national response to cyber risks, protect national interests and maintain public trust in digital services and the environment.

Effective communication in the field of cybersecurity constitutes an essential component of protecting the national interest, maintaining public trust, and ensuring a coordinated response to cyber incidents. In an increasingly complex digital environment exposed to hybrid threats, the lack of structured communication can lead to misinformation, public panic, damage to institutional reputation and direct harm to national security.

This policy defines the national communication framework for cybersecurity issues by establishing guiding principles, clear roles, institutional responsibilities, and coordination mechanisms between public institutions, the private sector, academic actors, and the public.

2. Purpose

The purpose of this policy is to ensure that all stakeholders, from government agencies to the private sector and the public, are informed, coordinated, and prepared to deal with cyber threats. This will be achieved through the establishment of clear communication protocols, appropriate training, and the use of advanced technologies, with the aim of maintaining national security and public trust.

Furthermore, it also aims to create and consolidate a standardized, coordinated, and reliable communication system in the field of cybersecurity. It seeks to ensure that institutional communication supports the prevention and effective management of cyber incidents, enables accurately and timely information to the public, maintains trust in state institutions and contributes to strengthening national response capacities to cyber threats. At the same time, aims to ensure full compliance with the legal and regulatory framework in force.

3. Scope of application

This policy applies to the National Cyber Security Authority and all its constituent structures, to public institutions of central and local administration, to operators of Critical and Important Information Infrastructures, as well as to private entities involved in incidents with national impact. The policy also extends to communication relations with national and international partners in the field of cybersecurity.

4. Fundamental Principles of Communication

National communication on cybersecurity is guided by the principle of accuracy over speed, ensuring that any information published is verified and based on confirmed facts. Transparency is considered a key element of public trust, implemented in a controlled manner to avoid violating operational security and compromising investigations or safeguards.

The policy is based on the “need-to-know” principle, according to which information is shared only with parties who have a legitimate need to know. Communication about incidents with wide-ranging impact should be centrally coordinated and carried out solely through authorized authorities, avoiding uncoordinated statements that could create confusion or institutional damage.

5. Roles and Responsibilities

The National Cyber Security Authority holds the central role of coordinating national communication on high-impact cyber incidents. NCSA is responsible for issuing official announcements, ensuring the coherence of the institutional message, and acting as a point of contact with international counterpart authorities.

The National CERT plays a technical support role, preparing professional analyses that serve as the basis for public and institutional communication, as well as publishing technical notices and professional advice for the security community.

Public institutions are obliged to report any security incident to NCSA in a timely manner, and to refrain from undertaking uncoordinated public communication. They should designate dedicated contact points for communication issues in the field of cybersecurity.

6. Elements of Communication Policy

I. Internal Communication Protocols

Defining communication channels and rules within public institutions and between the public and private sectors, for the exchange of information on cyber threats, vulnerabilities, and incidents.

Institutions are required to use secure channels for communicating information related to cyber incidents, to respect classified information, and to document any important decision-making during crisis management. Communication traceability is an essential element for accountability and continuous institutional improvement.

II. Public Communication Strategies

Drafting protocols for public communication regarding cyber threats and incidents, as well as awareness issues. This framework defines the type of information to be published, its method, and the authorities authorized for official communication.

Communication with the public must be clear, professional, and based on verified facts. Information disseminated must neither create panic nor downplay real risks but maintain a balance that fosters trust and civic responsibility. All public communication must respect personal data protection principles and the public interest.

Crisis Communication Plans

Drafting communication plans during and after cybersecurity incidents or crises, ensuring the timely and accurate dissemination of information to the public, the media, and other stakeholders.

In the event of a high impact cyber incident, institutional communication should follow a clear, phased structure. Initially, a preliminary statement is issued to inform the public about the situation. Subsequently, periodic updates are provided on the development of the incident and the measures taken. After the management of the situation is completed, institutions are required to provide a summarized communication that includes lessons learned and remedial measures taken. The principle of a single point of communication should be respected throughout the process.

7. Managing Classified Information

The publication of information containing technical details that could be exploited for further attacks, sensitive operational data, personal data without a legal basis, as well as information that could undermine investigative processes or incident response procedures is not allowed. Any decision to publish information must consider the balance between transparency and security.

8. Inter-institutional and International Communication and Cooperation

NCSA encourages and promotes the exchange of information with international counterpart authorities, partner organizations, critical infrastructure operators and other strategic actors, with the aim of exchanging information, sharing best practices, and coordinating the response to cyber threats of an international nature.

Facilitating communication and cooperation with international organizations and foreign governments, for the exchange of information, best practices, and coordination of response to cyber threats of an international nature.

9. Training and awareness on Effective Communication

Developing training programs for relevant personnel on effective communication, including handling sensitive information and managing communication in crisis situations, organizing simulation exercises for incidents, and promoting an institutional culture that considers responsible communication as an integral part of cybersecurity.

10.Use of Communication Technology

Using appropriate tools and technologies to ensure fast, secure, and consistent communication across various channels.

11.Feedback Mechanisms

Establishing communication channels to receive feedback from the public and stakeholders on cybersecurity policies and incidents, enabling a continuous and effective two-way flow of communication.

12.Reference

All communication activities under this policy are carried out in full compliance with national legislation on cybersecurity, legislation on the protection of personal data, as well as with the international obligations of the Republic of Albania.

13.Review Frequency

This policy shall be reviewed at least once a year and after any major incident that highlights the need for improvement of communication mechanisms or institutional coordination.