REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

Cybersecurity Performance Monitoring and Evaluation Policy

Table of Contents

1. Introduction 3

2. Purpose 3

3. Fundamental Principles 3

4. Roles and Responsibilities 3

5. Elements of the Performance Monitoring and Evaluation Policy 3

6. References 5

7. **Review Frequency** 5

1. Introduction

The Cybersecurity Performance Monitoring and Evaluation Policy is fundamental to ensure the sustainability and protection of critical and important information infrastructures. This policy focuses on continuous monitoring, systematic risk assessment and continuous improvement of the level of cyber resilience, with the aim of protecting critical services and assets from current and potential cyber threats. The lack of a structured and coordinated approach to performance monitoring and evaluation would expose national security, economic stability and public welfare to risks with serious and long-term consequences.

2. Purpose

The purpose of this policy is to define the principles and main directions for the development and implementation of an effective system for monitoring and evaluating the cybersecurity performance of critical and important information infrastructures, with the aim of strengthening their protection against cyber threats and safeguarding national security, economic stability, and the public interest.

3. Fundamental Principles

The policy is based on the principles of measurability, objectivity and evidence-based, as well as continuous monitoring, ensuring accurate assessment of the performance of critical and important information infrastructures, transparency of reports, cooperation between public institutions, the private sector and civil society, as well as the use of advanced technologies for the continuous improvement of cybersecurity.

4. Roles and Responsibilities

- **The role of NCSA**

The National Cyber Security Authority (NCSA) coordinates performance monitoring and evaluation at the national level, defines the standards and methodologies to be applied by critical infrastructures, and oversees compliance with these standards.

- **The Role of Public Institutions**

Public institutions the measures of this policy within their organizations, ensure the collection and reporting of performance data, and collaborate with NCSA for continuous safety improvement.

- **The Role of the Private Sector and Civil Society**

The private sector and civil society support performance monitoring and evaluation by sharing information on performance indicators, as well as contributing to the continuous improvement of cybersecurity.

5. Elements of the Performance Monitoring and Evaluation Policy

- **Continuous Monitoring**

Implementation of systems, processes and mechanisms for continuous and real-time monitoring of cyber activities, anomalies and threats affecting critical and important infrastructures.

- **Performance Evaluation Indicators**

Defining clear indicators and criteria for evaluating cybersecurity performance, including threat detection capability, incident response time, and systems recovery capacity, in order to continuously measure the level of security and resilience.

- **Risk Assessment and Management**

Conducting periodic risk assessments to identify vulnerabilities and potential threats to infrastructures, analyzing the impact and probability of materialization of cyber risks.

- **Compliance Controls and Re-Controls**

The implementation of periodic controls and reassessments to verify the compliance of critical infrastructures with national cybersecurity policies, standards, and requirements.

- **Incident Reporting and Analysis**

Development and implementation of standardized protocols for reporting, analyzing and documenting cyber incidents, including the functionalization of a central reporting system for incidents affecting critical and important infrastructures.

- **Public-Private Partnerships**

Strengthening cooperation with public and private entities that own or operate critical infrastructure, with the aim of improving monitoring, reporting and evaluation practices of cybersecurity performance.

- **Capacity Building and Training**

Investing in ongoing training and professional development programs for personnel involved in cybersecurity monitoring, analysis and assessment, to ensure appropriate skills and competencies.

- **Use of Technological Advancements**

Utilizing advanced technological solutions, including artificial intelligence and machine learning, to increase the efficiency of monitoring, analyzing and predicting cyber threats.

- **Information Sharing Platforms**

The establishment and operationalization platforms for sharing information, best practices and experiences regarding cybersecurity threats, vulnerabilities, and incidents among stakeholders.

- **Emergency Preparedness and Response Plans**

Developing and maintaining effective cyber emergency preparedness and response plans, with the aim of timely addressing and mitigating the impact of identified incidents.

- **Stakeholder Engagement and Awareness**

Continued engagement of public institutions, the private sector and the public to raise awareness on the importance of monitoring and evaluating cybersecurity performance for critical infrastructures.

- **Review and Update Mechanisms**

Periodic review and update of this policy and its implementation mechanisms, in line with evolving cyber threats, technological advances and changes in the legal and regulatory framework.

6. References

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

7. 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.