REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

Protection of Critical and Important Information Infrastructures 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. **Introduction** 3
2. **Purpose** 3
3. **Scope of Application** 3
4. **Fundamenteal Principles** 3
5. **Key Elements of the Policy** 4
6. **References** 5
7. **Review Frequency** 5

1. Introduction

The Critical Infrastructure Protection Policy is based on the applicable legislation on cybersecurity, as well as on the objectives and priorities of the National Cybersecurity Strategy and aims to guarantee the protection, sustainability and uninterrupted operation of systems and assets that are essential for national security, public order and economic stability of the country. This policy constitutes an important component of the national cybersecurity framework, addressing the risks and threats that compromise critical and important information infrastructures.

By promoting cooperation between the public and private sectors, the policy aims to support the development and implementation of technologies, mechanisms and best practices in the field of cybersecurity, with the aim of strengthening the protection and increasing the resilience of critical infrastructure.

2. Purpose

The policy aims to:

- Ensure the effective protection of critical infrastructure sectors, through the identification, assessment and management of risks and threats that may affect their functioning;
- Develop and implement strategies for preventing, detecting and responding to cyber attacks and incidents that threaten the integrity, availability and confidentiality of critical infrastructures;
- Establish strong and sustainable defense for these systems by ensuring that they are prepared to cope with and recover from any potential threat.

3. Scope of Application

This policy applies to all critical and important information infrastructures, including the energy, transport, health, public administration, banking/finance, digital infrastructure, water supply, space, education and any other sector that, in the event of disruption or violation, would cause serious consequences at the national level.

4. Fundamenteal Principles

- The implementation of this policy is based on several basic principles in accordance with the objectives set out in the National Cyber Security Strategy. The protection of critical and important infrastructures is based on a proactive approach, where security measures are determined in accordance with the level of threat and potential impact. The principle of resilience is also emphasized, according to which the infrastructure must not only be protected, but also be able to function and recover after incidents.
- Another essential principle is inter-institutional public-private cooperation, as part of the list of critical and important infrastructures are also operated by private entities.

5. Key Elements of the Policy

i. Identification of Critical Infrastructure:
Clear definition of infrastructures that are considered critical, including, but not limited to, the energy, transportation, health, telecommunications, finance, water supply, and government services sectors.

ii. Risk Assessment and Management:
Conducting periodic risk assessments to identify cyber threats and vulnerabilities affecting critical infrastructure, as well as developing measures to manage, treat, and mitigate them.

iii. Cybersecurity Standards:
Implementation of cybersecurity standards and regulatory requirements for critical infrastructure sectors, including requirements for information systems, incident reporting, and compliance monitoring.

iv. Public-Private Partnership:
Promoting cooperation between public institutions and private entities that own or operate critical infrastructure, through information sharing, the development of joint exercises and coordinated planning of response to cyber incidents.

v. Incident Response and Recovery Plans:
Developing, implementing and updating comprehensive plans for response to and recovery from cyber incidents, clearly defining roles, responsibilities and communication protocols during emergency situations.

vi. Investing in Cybersecurity Technologies:
Implementing advanced cybersecurity technologies to protect critical infrastructures and increase capabilities for detecting and preventing attacks.

vii. Human capacity development:
Focusing on training and human capacity development in cybersecurity with the aim of increasing skills for managing and protecting critical infrastructures.

viii. Information Sharing Mechanisms:
Establishing platforms and protocols for sharing information about cyber threats, vulnerabilities, and incidents among critical infrastructure stakeholders.

ix. International Cooperation:
Engaging in international collaborations to share best practices, intelligence information, and strategies for protecting global critical infrastructure.

x. Periodic compliance checks:
Implementing regular checks and assessments to ensure compliance of critical infrastructure entities with cybersecurity policies, standards, and requirements.

xi. Awareness and Training Programs:
Developing regular awareness training and training exercises for stakeholders in critical infrastructure sectors on cyber threats.

xii. Support for research and development:
Encouraging and supporting research and development for new cybersecurity technologies and best practices, focused particularly on the protection of critical infrastructure.

6. References

This policy is based on national cybersecurity legislation, the National Cybersecurity Strategy, and internationally recognized practices and standards in the field of protection of critical and important information infrastructures.

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.