REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

# Cyber Risk Assessment Policies

# Table of Contents

## 1. Introduction

The Cyber Risk Assessment Policy is essential for ensuring security in an increasingly complex cyber environment exposed to evolving risks. Cybersecurity risk assessment, carried out by responsible structures, constitutes a key process for identifying, analyzing and assessing threats and vulnerabilities affecting critical and important information infrastructures, as well as national interests.

This process provides the foundation for the development and implementation of cybersecurity policies and measures, supporting the development of strategies for managing and mitigating risks, as well as contributing to strengthening resilience and the effective protection of national interests.

## 2. Purpose

The purpose of the Cybersecurity Risk Assessment policy is to identify, analyze, assess, and prioritize threats and vulnerabilities that could impact critical infrastructure, essential services, and national interests. This process aims to support strategic decision-making for managing and mitigating cyber risks, improving existing security measures, efficiently allocating resources, and strengthening the common defense of national security.

## 3. Scope of application

This policy is implemented by the National Cyber Security Authority and is mandatory for implementation by operators of Critical and Important Information Infrastructures according to the legal provisions in force.

## 4. Principles of cyber risk assessment

Cyber risk assessment is based on fundamental principles as a structured, systematic and continuous process, taking into account the probability of occurrence and the potential impact of threats on assets, critical services and national interests.

The assessment is conducted in a proportional and context-appropriate manner considering the importance of the infrastructure, information sensitivity, and the level of exposure to threats, integrating technical, organisational and human aspects, providing a comprehensive view of the risk.

The process is transparent and documented, ensuring traceability of analysis, decision-making and results, and enabling subsequent review and audit. Risk assessment is considered a dynamic process, which is periodically reviewed and updated to reflect changes in the threat environment, technology and capabilities.

## 5. Evaluation elements include:

i. Threat Identification

Identifying cyber threats affecting the national space, including, but not limited to, malware, ransomware attacks, phishing, state-sponsored cyber activities, and insider threats.

ii. Vulnerability Assessment

Analyzing vulnerabilities in government networks and systems, critical infrastructure sectors, and private enterprises, in order to assess the level of risk and exposure to identified threats

iii. Risk Analysis

Assessing the likelihood of occurrence and severity of the impact of threats that could exploit identified vulnerabilities, assessing their potential impact on national security, the economy and public safety.

iv. Review of the Current Security Posture

The assessment of existing cybersecurity measures and their effectiveness includes policies, procedures and technical controls in addressing and handling identified risks.

v. Incident History Review

Review and analysis of previous cyber incidents, with the aim of identifying systemic vulnerabilities and assessing existing response capacities.

vi. Stakeholder Consultation

Engaging public institutions, private entities and international partners to collect information, intelligence and best practices in the field of cybersecurity.

vii. Risk Mitigation Recommendations

Drafting recommendations to address identified risks, including technical and organizational measures based on policies and regulatory requirements as well as capacity building and awareness-raising initiatives.

viii. Resource Allocation

Supporting the process of allocating the necessary financial, technological and human resources to serve the management and reduction of cyber risks at the national level.

ix. Regular Updates and Continuous Monitoring

Providing regular updates to reflect changes in the cyber threat landscape and ensuring ongoing oversight.

x. Reporting and Communication

Reporting findings, analyses and recommendations to relevant authorities and stakeholders, as well as clear and effective communication of risks and actions needed to address them.

## 6. References

This policy is based on national cybersecurity legislation, the National Cybersecurity Strategy, as well as recognized international practices and standards for cybersecurity risk assessment and analysis.

## 7. Review Frequency

This document should be reviewed at least once a year or whenever significant changes occur in the institution's information security management system.