Public-Private Partnership 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. Purpose

The purpose of this policy is to provide a strategic approach to facilitate and strengthen cooperation between government entities and private sector organizations, with the aim of increasing the level of national cybersecurity and protecting critical infrastructures and services.

2. Scope of application

This policy strengthens public-private cooperation and contributes to increasing capacities for prevention, protection, and response to cyber incidents. In this context, the policy aims to:

1. Minimize cyber risks and guarantee the integrity, availability, and resilience of critical infrastructure services.
2. To support the development and implementation of high cybersecurity standards.
3. Promote a coordinated, sustainable, and comprehensive approach to cybersecurity.

3. Fundamental Principles

The Public-Private Partnership Policy is based on the principle of protecting the public interest and national security, the shared responsibility of the public and private sectors, as well as building trust and transparency between the parties. Cooperation is developed in accordance with the legislation in force, ensuring proportionality, efficiency, and protection of confidentiality of information. The policy encourages the involvement of relevant stakeholders, long-term sustainability, and the continuous improvement of cooperation mechanisms, with the aim of creating added value and strengthening national capacities.

4. Roles and responsibilities

The role of NCSA

The National Cyber Security Authority has a coordinating role in the implementation of this Public-Private Partnership policy. NCSA determines national cooperation priorities, facilitates the establishment and operation of partnership mechanisms between public institutions and private sector actors, oversees the implementation of cybersecurity measures, promotes secure information sharing, and supports joint initiatives at the national level.

The role of public institutions

Public institutions are responsible for actively participating in the implementation of this Public–Private Partnership policy, in accordance with legal requirements and while consistently respecting clearly defined security requirements. Public institutions cooperate with NCSA and private sector actors to strengthen capacities, manage risks, and improve capabilities for the prevention, detection, and response to cyber threats at the national level.

The role of the private sector and civil society

The private sector and civil society organizations are key partners in the implementation of this policy, contributing with technical expertise and innovation. In cooperation with NCSA and public institutions, these actors participate in joint initiatives, share good practices, and support the development of national capacities for the prevention, detection and response to cyber threats.

5. Elements of Public-Private Partnership Policy

i. Cooperation Structure

The establishment of a formal structure or platform for continuous communication and cooperation between the public and private sectors in the field of cybersecurity. This could include joint committees, working groups, or task forces.

ii. Information Sharing Mechanisms

The creation and implementation of protocols for sharing information on cyber threats, vulnerabilities, and best practices between public and private entities, ensuring compliance with privacy, confidentiality, and information protection requirements.

iii. Joint Cybersecurity Initiatives

The development of collaborative projects and programs that leverage the capacities and expertise of the public and private sectors, with a focus on critical infrastructure protection, research and development, and cybersecurity awareness.

iv. Human Capacity Building and Development

The implementation of joint training programs and exercises for cybersecurity experts, with the aim of strengthening professional skills and addressing the lack of capacity and talent in this field.

v. Legal and Regulatory Support

Providing legal support and developing a regulatory framework that encourages private sector participation in cybersecurity initiatives and provides legal protection for information sharing in accordance with applicable legislation.

vi. Cybersecurity Standards and Best Practices

Encouraging the adoption and implementation of national and international cybersecurity standards and best practices, especially within the private sector.

vii. Incident Response and Recovery Planning

Cooperation in the development and implementation of joint strategies for cyber incident response and recovery planning, with the aim of managing and mitigating the impact of incidents.

viii. Funding and Resources

Allocating government resources and providing incentives to support cybersecurity initiatives in the private sector, including grants, fiscal incentives, and funding for joint research and development projects.

ix. Cooperation in Risk Management

Collaboration to identify, assess and mitigate cybersecurity risks, especially those that affect both the public and private sectors.

x. Policy Development and Strategic Planning

The inclusion of private sector expertise and perspectives in the development of national cybersecurity policies and strategic plans, with the aim of building a coordinated and comprehensive approach to cyber threats.

6. References

This policy is based on national legislation on cybersecurity, the National Strategy for Cybersecurity, as well as recognized international practices and standards in the field of public-private partnership in cybersecurity.

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.