Cybersecurity Awareness 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. **Policy Description** 3
3. **Scope of application** 3
4. **Mission and Goals** 3
5. **Roles and responsibilities** 4
6. **Tools and Concrete Measures** 4
7. **Partners and Cooperation** 4
8. **Monitoring and Evaluation** 4
9. **Funding and Implementation Calendar** 5
10. **References** 5
11. **Review Frequency** 6

1. Introduction

The Cybersecurity Awareness Policy in Albania aims to strengthen the protection of individuals, organizations and society as a whole against the risks they encounter in cyberspace. Through increased awareness and education, this policy contributes to the creation of a safer and more informed digital environment, as well as to the reduction of successful cases of cyber incidents and threats in the country.

2. Policy Description

The number of users of information and communication technologies in Albania has been continuously increasing, influenced in particular by the digitalization of electronic public services.
At the same time, children, young people, and adults widely use the internet and social media for communication, education, access to information, as well as for conducting financial transactions and business activities.

In this context, cyberspace is not used solely for legitimate purposes, but also by malicious actors seeking unlawful gains, primarily of a financial nature, thereby compromising user security and rights.
Considering the high level of technology usage and the growing cyber threats affecting individuals, organizations, and public and private entities, there is a need to undertake structured education and awareness initiatives. These initiatives aim to ensure that technology users, regardless of age or level of education, are familiar with the basic principles of safe internet use and with methods of protection against cyber threats.

3. Scope of application

This policy is implemented at the national level and includes all social and institutional groups that use or provide digital services. It particularly addresses public institutions, the private sector, educational institutions, civil society organizations, and citizens.

The policy serves as a guiding document for the design and implementation of awareness campaigns, education programs, training and other activities aimed at improving society's knowledge and skills in the field of cybersecurity.

4. Mission and Goals

The mission of this policy is to build a cybersecurity-aware and informed society in Albania through the involvement of public and private actors across all sectors.

The goals are:

- Increasing citizen awareness of cybersecurity threats and ways to protect themselves, including all age groups.
- Raise awareness among public and private entities and organizations regarding cyber risks and cybersecurity.
- Expanding awareness campaigns across all developing sectors.
- Increasing cooperation with various stakeholders, at national and international level, with the aim of undertaking and implementing awareness campaigns.

- Reducing the possibility of cyber risks affecting citizens, through awareness and education as a preventive measure.

5. Roles and responsibilities

The role of NCSA

The National Cyber Security Authority has a leading role in the development, coordination and monitoring of cybersecurity awareness policies and activities. NCSA defines priority topics, develops awareness materials, coordinates national campaigns and collaborates with other institutions to ensure uniform implementation of this policy.

The role of public institutions

Public institutions have a responsibility to integrate cybersecurity awareness into their daily activities, particularly through employee training and ongoing communication with citizens. They should contribute to the implementation of this policy by organizing awareness-raising activities and reporting on their results.

The role of the private sector and civil society

The private sector and civil society organizations are important partners in the implementation of this policy. Through cooperation with NCSA and public institutions, these actors can contribute to the dissemination of awareness-raising messages, the development of educational programs, and the increase of the overall level of cybersecurity culture in society.

6. Tools and Concrete Measures

The implementation of this policy is supported by the following key measures:

- developing comprehensive awareness-raising and educational campaigns for citizens, organizations and public and private entities.
- organizing seminars, trainings and educational activities in the field of cybersecurity for all sectors of society;
- creation and operationalization of support mechanisms for addressing cyber incidents and providing technical assistance to victims;
- promoting cybersecurity as an integral part of school and university education.

The envisaged measures are in line with the objectives of the National Cyber Security Strategy and are detailed in the relevant Action Plan.

7. Partners and Cooperation

The implementation of this policy relies on cooperation with national actors from the public and private sectors, including educational institutions, civil society organizations and experts in the field. At the international level, cooperation is carried out with organizations and institutions where Albania is a member or partner, as well as with agencies and structures of allied countries, with the aim of exchanging experiences and best practices in cybersecurity.

8. Monitoring and Evaluation

NCSA monitors the implementation of the policy through the analysis of awareness campaigns and activities planned according to the annual calendar. It also reviews periodic reports on the

implementation of measures and annual reports on the implementation of the National Cyber Security Strategy.

To assess the level of awareness and effectiveness of measures, questionnaires and other assessment instruments are carried out that measure society's knowledge and skills in the field of cybersecurity.

9. Funding and Implementation Calendar

- Activities foreseen for the implementation of this policy will be financed with financial means foreseen in the state budget and various donors, which will enable the implementation of the measures and actions foreseen by the 2025-2027 Action Plan of the National Cyber Security Strategy, in accordance with the objectives of this policy.
- The work on the implementation of the measures envisaged by this policy will begin once it is approved. The organization and implementation of awareness campaigns, trainings and seminars in the field of cybersecurity for all sectors will be carried out in accordance with the Action Plan 2025-2027 of the National Strategy for Cybersecurity, which are in line with the objectives of this policy.

Awareness activities will be divided into clusters, with tailored materials prepared for each group.

These clusters will include:

- Awareness activities for children
- Awareness activities for parents and educators
- Awareness-raising activities for young people, including students
- Awareness activities for the elderly
- Awareness-raising activities for government institutions and employees
- Awareness-raising activities for law enforcement institutions
- Awareness-raising activities for citizens
-

All activities for the above groups will be carried out within one year according to an annual calendar that will be prepared by the institution.

In addition, awareness-raising activities will be carried out every month through social media on specific topics. Regarding the integration of cybersecurity as part of school and university education, inter-institutional meetings will be held and working groups will be created, within the framework of the implementation of this policy, and in the future.

10. 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 cybersecurity awareness.

11. Review Frequency

This document shall be reviewed at least once a year to ensure that it remains up to date with technological and societal developments. The review may be carried out earlier if new needs or challenges are identified that require adaptations regarding cybersecurity awareness.