# NATIONAL CYBER SECURITY STRATEGY

## - Version 2.0 -

# CONTENTS

SUMMARY ..... 3

1 INTRODUCTION ..... 4

2 GENERAL PRINCIPLES AND OBJECTIVES ..... 5

3 ACTION FRAMEWORK – STRATEGIC OBJECTIVES ..... 6

3.1 Determining the stakeholders participating in the National Cyber Security Strategy – stakeholders ..... 7

3.2 Defining critical infrastructure ..... 7

3.3 Risk assessment at national level ..... 8

3.4 Recording and improving the existing institutional framework ..... 8

3.5 National Cyberspace Contingency Plan ..... 9

3.6 Determining basic security requirements ..... 10

3.7 Handling security incidents ..... 10

3.8 National preparedness exercises ..... 11

3.9 User-citizen awareness ..... 12

3.10 Reliable information exchange mechanisms ..... 12

3.11 Support of research and development programmes and academic educational programmes ..... 13

3.12 Cooperation at international level ..... 13

3.13 Evaluation and revision of the National Strategy ..... 14

4 CONCLUSION ..... 14

# SUMMARY

This document describes the National Cyber Security Strategy, through which the Greek State's central planning with regard to cyberspace security is being developed.

Given that the use of the internet and information and communication technologies (ICTs) is continuing to grow in every aspect of public and private sector activity, special emphasis needs to be placed on the establishment of a safe online environment, infrastructure and services, which will boost citizens' trust, leading them to further use of new digital products and services. A safe environment together with the promotion of new services and products on the one hand, and the safeguarding of citizens' privacy and rights in the new digital world on the other, are considered essential conditions for boosting and promoting economic development in Greece.

The establishment of the National Cyber Security Strategy determines the main principles for the creation of a safe online environment in Greece and sets strategic objectives and the action framework through which they will be achieved. The objectives and the individual actions for their achievement are described in detail herein.

The implementation of the National Cyber Security Strategy is to be undertaken by the National Cyber Security Authority which is being created to bridge the organisational and coordinative gap among the stakeholders involved in cyberspace security in Greece, both in the public and private sector. Furthermore, the National Cyber Security Authority will evaluate, revise and update the National Cyber Security Strategy if required, and at the latest every three years.

# 1 INTRODUCTION

The increasing use of information and communication technologies (ICTs) allows for the exceptionally fast transmission, processing and storage of vast amounts of data which today's societies are using more and more to further advance their economic, social, technological, cultural and scientific development. At the same time, widespread internet availability allows direct access to such data and the exchange of information, thus radically altering social and economic life. The economy, commerce and businesses increasingly rely on digital infrastructure for their further development. Public administration expects digital technology to become a means of improving the services provided and to lead to rational use of its information resources. Open and free internet access, and the confidentiality, integrity, availability and resilience of ICT systems are the basis for prosperity, national security but also for the safeguarding of fundamental rights and freedoms.

As our society comes to rely more and more on information and communication systems, their security has become a matter of major national interest, whilst at the same time it is becoming increasingly necessary to protect users of digital services, especially young people. The term 'cyber security' refers to all the appropriate actions and measures that must be taken in order to ensure the protection of cyberspace from such threats that are directly linked to cyberspace itself and which can cause damage to inter-dependable information and communication technology (ICT) systems. The National Cyber Security Strategy is a tool for improving online security, by ensuring the integrity, availability and resilience of critical infrastructure and the confidentiality of transmitted digital information, whilst also upholding the principles of open society, constitutional freedoms and individual rights.

# 2 GENERAL PRINCIPLES AND OBJECTIVES

The growth and shielding of digital services and markets is a key pillar of support for the national economy and confers a competitive advantage both at national and European level. As Greece continues to experience growth and to invest in digital markets, networks and services, both in the public and private sector, the creation of a National Cyber Security Strategy is rendered a necessity. The main principles of the National Cyber Security Strategy are:

A. The development and establishment of a secure and resilient cyberspace which will be regulated in accordance with national, EU and international rules, standards and good practices and in which citizens, and public and private sector stakeholders can be active and interact securely, as per the values that govern the rule of law such as, indicatively, those of freedom, justice and transparency.

B. The continuous improvement of our capabilities for protection against cyber-attacks, with emphasis on critical infrastructure and the safeguarding of operational continuity.

C. The institutional shielding of the national cyber security framework, for effective handling of cyber-attack incidents and the minimisation of impact by cyberspace threats.

D. The development of a strong culture of security in citizens and the public and private sectors, by utilising the relevant capabilities of the academic community and of other public and private sector stakeholders.

The individual objectives of the National Cyber security Strategy can be summarised as follows:

1. To upgrade the level of prevention, evaluation, analysis and deterrence of threats against the security of ICT systems and infrastructure.
2. To enhance the ability of public and private sector stakeholders to prevent and handle cyber security incidents and to improve the resilience and recoverability of ICT systems following a cyber-attack.

3. To create an effective coordination and cooperation framework by determining the individual competences and roles of the various public and private sector stakeholders involved in the implementation of the National Cyber Security Strategy.
4. To ensure the active participation of Greece in international cyber security initiatives and actions by international organisations, for the enhancement of national security.
5. To make all social institutions aware and to inform users regarding the secure use of cyberspace.
6. To continuously adapt the national institutional framework to new technological requirements and to EU directions for effective handling of illegal acts linked to cyberspace activity.
7. To promote innovation, research and development in security issues and cooperation between the stakeholders involved.
8. To make use of best international practices.

The adoption, implementation and supervision of the National Cyber Security Strategy will contribute to the creation of a powerful rule of law, with a high level of security and resilience against cyber threats, with respect towards privacy, individual and social rights, and which will provide quality electronic services to citizens and businesses, whilst at the same time acting as a lever for the growth of the economy and businesses by setting common rules for all stakeholders involved.

# 3 ACTION FRAMEWORK – STRATEGIC OBJECTIVES

The National Cyber Security Strategy consists of two individual phases. The development and implementation of the Strategy in the initial phase and its assessment and review in the second phase. These phases determine a continuous life cycle, in the sense that the National Strategy is first developed and implemented, then assessed, according to predetermined assessment indicators and, if deemed necessary, revised and updated.

The stakeholders involved are divided into two levels: strategic and operational. The National Cyber Security Authority is a stakeholder at a high political and governmental level, with extended competences, which monitors, implements and bears overall responsibility for the National Cyber Security Strategy. The National Cyber Security Authority will exercise its competences (probably) with the contribution of a National Advisory Body/ Forum, in which all the public and private sector stakeholders involved will participate in close cooperation with the national Computer Emergency Response Team (CERT). Within the framework of its competences, it will monitor, coordinate and evaluate the work by the stakeholders involved, for the achievement of the strategic actions and objectives. The operational level includes, among others, the Computer Security Incident Response Teams – CSIRTs, also known as Computer Emergency Response Teams – CERTs, of the public and private sector, who bear the responsibility of dealing with cyber incidents (cyber defence) as per their competences.

The framework of actions required for the implementation of the National Cyber Security Strategy is defined below:

## 3.1 Determining the stakeholders participating in the National Cyber Security Strategy – stakeholders

The National Strategy mainly concerns stakeholders that are crucial for the smooth functioning of society.

It is therefore important to clearly determine the public and private stakeholders involved which will contribute to the development and implementation of the national strategy.

## 3.2 Defining critical infrastructure

Definition and registration of Critical Infrastructures (both in the public and in the private sector) and of their interdependencies.

## 3.3 Risk assessment at national level

The preparation of a risk assessment study at national level following a scientific and technological procedure which, in summary, is based on the identification, analysis and evaluation of the impact of risk and leads to the determination of a plan for the protection of critical infrastructure per sector and/or per stakeholder. The study, which will be revised every three years, will take into account all potential threats, especially those related to malicious actions (e.g. cyber crime, cyber-attacks) but also the risks related to natural phenomena, technical failures or malfunctions, and human error. Threats stemming from the interdependency of the information and communication systems of stakeholders participating in the National Strategy will also be taken into account, whilst the extent and severity of the impacts at national level will be further investigated.

## 3.4 Recording and improving the existing institutional framework

The primary phase of developing and implementing a National Strategy involves recording and evaluating the current institutional framework and the structures in place for meeting the objectives of the National Strategy:

- Legislation, roles and competences of the stakeholders linked to Cyber Security (e.g. processing of personal data, electronic communications, waving of confidentiality of communications, network integrity and availability, etc.).
- Regulatory acts, specialised per sector (e.g. banking) and their impact to date on the improvement of Cyber Security (e.g. regulations and auditory role of the Bank of Greece).
- Structures, stakeholders and services of the public or private sector, with an operational role in safeguarding Cyber Security (e.g. Computer Security Incident Response Teams – CSIRTs).
- Existing emergency plans such as Egnatia, Xenokrates, etc.
- EU and other international directives and regulations regarding network and information security and the security of critical infrastructure.

The detailed recording and evaluation of the efficiency of the existing institutional framework and the relevant structures will lead to the detection of those points that are not adequately covered or demonstrate overlaps but also of those points that require improvement and more effective coordination. The result of this action will be the adoption of the required legislation, with respect towards constitutional freedoms and individual rights and towards International Law, in accordance with the overall social and political situation but also with the requirements of the National Cyber Security Strategy, so as to achieve its objectives.

The National Strategy reflects it relativeness not only to the existing institutional framework, but also to other Strategies at national or international level (e.g. National Regulation of Security, National Military Strategy, e-Governance Strategy, etc.). It is also harmonised with the requirements of relevant EU regulations and directives (in particular with Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July, 2016, concerning measures for a common high level of security of network and information systems across the Union – NIS Directive).

## 3.5 National Cyberspace Contingency Plan

Development of a National Cyberspace Contingency Plan which will determine the structures and measures for dealing with significant incidents taking place within the critical information and communication systems of the stakeholders participating in the National Cyber Security Strategy and the reinstatement of the services such stakeholders offer to society.

The main objectives of the National Cyber Security Plan include the determination and description of the criteria used so that an incident may be deemed critical, the determination of important procedures and actions for dealing with such incidents and of the roles and competences of the various stakeholders managing the specific incident.

## 3.6 Determining basic security requirements

All the stakeholders participating in the National Cyber Security Strategy are obliged to take all technical and organisational measures that ensure the secure and seamless operation of their information and communication systems and minimise the impact of a security incident. Such measures include prevention measures but also ones for handling security incidents.

The National Cyber Security Authority will determine (e.g. through regulatory acts) the minimum security requirements and the corresponding technical and organisational measures, based on risk assessment at national level, which the stakeholders must implement so as to achieve a fundamental and common level of security.

The establishment of a minimum, common and harmonised level of requirements and measures among the stakeholders, which will be applied during implementation, evaluation and proper application auditing, is especially significant.

Moreover, it will enhance the stakeholders' ability to exchange information, since there will be a 'common language', whilst also facilitating the reporting of security incidents and the implementation of common security practices.

## 3.7 Handling security incidents

In the event of a cyber security incident, the stakeholders participating in the National Strategy must be prepared to react effectively. Knowledge of the technical details of the incidents the stakeholders are required to handle, their analysis, and the dissemination of the knowledge required help all participants to better prepare themselves for dealing with the incident but also to proceed with corrective actions with regard to the security measures taken, so as to minimise the risk of a repetition of the incident. In this way, preparedness and the ability to handle security incidents and to subsequently recover are enhanced at national level. Management of emergency incidents is realised in accordance with the National Cyberspace Contingency Plan.

During the handling of security incidents, an important role is that of the Computer Security Incident Response Teams – CSIRTs, whose main function is to coordinate actions during management of the incident by the stakeholders involved, based on predetermined roles, competences and procedures and on operational and communicational capabilities. at national level there are other response teams already operating, or ones that may be created, with regard to computer security per sector. In addition, the National CERT aims to optimise the level of prevention, assessment and analysis of the threats among the stakeholders participating in the National Strategy. The National CERT, in collaboration with the other CSIRTs/CERTs operating within Greece and with other national CSIRTs/CERTs with which a cooperation network has been established, constantly monitors at both a national and international level the threats and vulnerabilities of information and communication systems, analyses and evaluates them, based on the particularities of each country, and informs the stakeholders so as to enhance their preparedness for dealing with security incidents.

## 3.8 National preparedness exercises

National Preparedness Exercises are a significant tool for evaluating participating stakeholders' preparedness and for detecting system weaknesses and vulnerabilities. The simulation of security incidents offers the opportunity for handling these under conditions similar to actual incidents, through implementation of the relevant security measures taken, and of drafted pertinent contingency plans, so that the stakeholders may proceed with relevant improvements and updates. Furthermore, such exercises enhance the exchange of information and knowledge, and the cooperation between participating stakeholders, whilst they strengthen the culture of collaboration towards increasing the level of cyber security in Greece.

Preparedness exercises are conducted at regular intervals. The exercises are supervised by the National Cyber Security Authority and are planned based on explicitly determined timetables, roles, scenarios and objectives. The results of the exercises and in particular the acquired knowledge must be made available to the

stakeholders involved in the exercises but also to other competent stakeholders. The participation of Greece in other EU and international preparedness exercises is also being sought.

## 3.9 User-citizen awareness

Awareness with regard to the threats and vulnerabilities related to cyber security and their social impact is of vital importance. Appropriate and targeted awareness – educational campaigns both for the users of stakeholders participating in the National Cyber Security Strategy and for citizens in general, help to enhance knowledge with regard to the dangers of the online environment so as to increase protection from common threats, something which is expected to eventually boost the level of cyber security in Greece.

The actions, mechanisms and methods related to user-citizen awareness, depend on the audience to which they are directed. The design, organisation and implementation of the user-citizen awareness programme is supervised by the National Cyber Security Authority and indicatively includes citizen information campaigns (e.g. via the Ministry of Education in primary and secondary education), educational activities (e.g. in collaboration with university institutions) for administrators and users of the stakeholders' information and communication systems, promotion through websites, etc.

## 3.10 Reliable information exchange mechanisms

The exchange of information, other than the compulsory exchange mentioned in paragraph 3.6., between the private stakeholders participating in the national Cyber Security Strategy and their supervisory bodies in the public sector and with the national Cyber Security Authority, is particularly important for the implementation of the National Strategy. Private stakeholders are encouraged to exchange information pertaining to the information and communication systems they operate, to the security policies they have implemented, and to the threats and security incidents they face. Similarly, public sector stakeholders are encouraged to exchange information collected, which may potentially endanger the desired level of cyber

security. By correlating this information it is possible to analyse the development of threats related to the country's cyber security.

It is necessary to develop such mechanisms for the reliable exchange of information within a framework of mutual trust and respect towards the roles and competences of all stakeholders participating in the National Cyber Security Strategy.

At this stage, probably, though, also at a later phase, there will be a possibility of examining the development of public and private sector partnerships which will be established based on a common scope of implementation while using well-defined roles in order to achieve common objectives.

### 3.11 Support of research and development programmes and academic educational programmes

The substantial support by the state of the academic community's endeavour to participate in national, EU or other international research and development programs and the adaptation of their curriculum to issues concerning the National Cyber Security Strategy, is a substantial parameter for strengthening the level of cyber security in Greece, especially when taking into account that this is a field of constantly evolving cutting edge technologies and specialised knowledge.

### 3.12 Cooperation at international level

Given that cyberspace and the internet are a global information environment, dealing with threats and vulnerabilities of information and communication systems becomes a global endeavour that requires cooperation at national level. Therefore, it is important that Greece participate actively in the entire range of international cooperation on the issue of cyberspace security, within the context of existing objectives of the country's foreign policy and the directions for its application and in accordance with applicable legislation. More specifically, systemic cooperation with countries that have adopted a similar strategy in this regard, and whose choices are compatible to the corresponding Greek choices in this case, is required. The aim of the cooperation will be to exchange experiences and best practices and to determine the potential for the joint development of suitable means for handling threats and challenges pertaining to cyberspace security. In addition, the contribution of Greece

in the formulation and implementation of relevant decisions adopted under international organisations and to which Greece belongs will be exploited, to the greatest degree possible, with the aim of both strengthening cyber security at national level and allowing for harmonisation between similar international multilateral negotiation and action mechanisms, taking of course into account the autonomy of decision-making at national level.

### 3.13 Evaluation and revision of the National Strategy

The implementation of the National Cyber Security Strategy's strategic objectives is monitored by the National Cyber Security Authority, with the aim of evaluating and possibly revising the Strategy. Evaluation of the Strategy is based on a predetermined methodology, that utilises qualitative and quantitative efficiency indexes and on the basis of international standards, and ends with a report that will propose specific improvement measures, within a pre-determined timetable. The National Cyber Security Authority monitors the international standards in order to adopt best practices which are then indicated to the competent stakeholders for implementation. During this phase, it is imperative for all stakeholders involved in the National Strategy to participate in the context of their institutional and administrative competences.

## 4 CONCLUSION

The National Cyber Security Strategy will be developed based on the above action framework which will also create the conditions for the implementation of our national vision for our desired level of cyber security (see chapter 3). The implementation of the aforementioned entails the strengthening of the cooperation between the public and private sectors, which is deemed especially important for the success of the entire endeavour but also particularly difficult, given the low degree of maturity and experience. However, the benefits of such a cooperation will be multiple for the state and for public administration, for citizens and for the level of provided

security services but for the private sector as well (broadband service providers, private businesses).