PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA


# NATIONAL STRATEGY OF INFORMATION SYSTEMS SECURITY

2025 - 2029

# *Preface by the President of the Republic*

*Our country has launched an ambitious policy aimed at the widespread adoption of digitalization within its public administration, with the objective of facilitating citizens daily lives and supporting the recovery of the national economy on solid and sustainable foundations.*

*Aware that such a policy will undoubtedly become a prime target for the enemies of our country, it has appeared imperative to equip ourselves with appropriate mechanisms capable of protecting it from these malicious intentions.*

*It is by relying on this strategic vision that our country has equipped itself, by virtue of presidential decree n°20-05 of January 20, 2020, with a National Information Systems Security Framework which gave birth to the Information Systems Security Agency. The conceptual model adopted is based not only on a spirit of intersectoral cooperation of all the entities involved where the search for useful, safe and effective information must be accompanied by its immediate operational exploitation, but also on the need to channel all our energy to give rise to innovative approaches, in line with the objectives sought.*

*Thus, the National Strategy of Information Systems Security does not constitute an end in itself; it only has value if it is evaluated, as much as possible, to ensure its alignment with technological developments and the expected objectives.*

*In short, anticipating situations, identifying shortcomings and weaknesses, understanding their underlying causes, and then considering possible actions to enhance the effectiveness of both the organizational interface and the operational mechanism—this is the approach adopted by our country to address the numerous surrounding cyber threats.*

***Abdelmadjid TEBBOUNE***

# Contents

# I. Introduction

The digital transformation of State has always been put at the center of the concerns of the Highest Authorities of the country, who have constantly insisted on the importance and advantages of introducing Information Technologies in the administrative, economic, industrial sectors, as well as within the whole Algerian society.

In this regard, the President of the Republic has accorded a particular interest to accelerate the process of digital transformation of State institutions as well as the economic sector, which is a strategic objective of the public policies, being implemented, currently in all fields.

Indeed, digitization is a key instrument that is crucial for our country's socio-economic development, providing a transparent and efficient management of public properties, smooth functioning of public utilities, as well as enhancement and protection of the State's information assets and the national heritage in general.

The success of such digital transformation objective is necessarily depending on effective management of information systems and critical infrastructures, through the implementation of the requirements and measures needed for the legislative and regulatory levels as well as organizational, functional and technical levels so that it is achieved in compliance with the cross-cutting requirement of securing national cyberspace.

Aware of this challenge, the Highest Authorities have decided to provide the State with an appropriate instrument for information systems security, through the establishment of a national information systems security framework, composed of a National Council and an Information Systems Security Agency (ASSI), pursuant to Presidential Decree No. 20-05 of January 20$^{th}$, 2020.

> **Thus, the primary objective of this framework is the development and implementation of the national strategy of information systems security, to establish a favorable environment for all national actors contributing to cybersecurity, through reuniting all the necessary requirements to effectively contribute to the protection and preservation of national digital sovereignty.**

The adopted approach for the elaboration of the first national strategy of information systems security is based on the involvement of State institutions as well as the concerned public and private organization, the analysis of the national digital landscape and the identification of the difficulties and constraints encountered, taking into consideration the evolution of digital technologies as well as the cyber threat typology.

It is also necessary to point out that the national strategy is based on the existing legislative and regulatory texts, governing the various aspects of cybersecurity as well as related areas, an arsenal which needs to be constantly updated and strengthened.

**Furthermore, and in view of the complexity and sensitivity of the missions entrusted to the national information systems security mechanism, the focal point in this area, regarding to national security and sovereignty, the first imperative of this strategy is not only to emphasize the need to provide our country with operational capabilities guaranteeing the availability, integrity and confidentiality of information, but also the security and resilience of both critical systems and infrastructure, all according to the three-pillar framework of securing human resources, processes as well as technologies.**

Therefore, it appears perfectly natural that the national strategy underlines the Imperative to train, employ, value and preserve a highly qualified human resource in the cutting-edge areas of cybersecurity. This resource, extremely sought worldwide, constitutes, both in fact, a major advantage and a key success factor for the State.

The present national strategy of information systems security falls fully under the framework of the national vision for the digitization of State institutions and the socio-economic sector, while taking into consideration the regular emergence of new digital technologies, as well as the evolution of the cyber threat, likely to present a risk for the security of national information systems.

# II. Vision

The vision conveyed by this national strategy of information systems security is stated as follows:

**«Ensure national cyber resilience by strengthening capabilities to prevent, detect and respond to cyber incidents, to assist the digital transformation of our country and preserve the national digital sovereignty»**

# III. Strategy Objectives

The main objective of this national strategy of information systems security is to accompany State institutions as well as public and private organization, through the implementation of a progressive, inclusive and controlled approach in matters of security and resilience of both national information systems and critical infrastructures, over the next four (4) years.

This involves achieving a maximum level of performance in terms of security and cyber-resilience of both national information systems and critical infrastructures, all sectors combined.

To this end, the sensitivity levels of the different sectors and systems should be identified, with particular emphasis on those whose compromised functioning would have a major negative impact, either on the functioning and/or security as well as the image of institutions and public and private services, or even on the well-being and/or security of the population in general, these include government institutions, public administrative or financial organism, public security, energy, health, water resources, telecommunications, transport as well as the production and distribution of essential food products.

This strategy, which constitutes the reference framework for the work of State institutions and all stakeholders, sets out the actions to be undertaken and the directions to be followed to achieve the expected objectives, according to their importance and priority, and this is in a progressive, inclusive and controlled manner.

> **Indeed, in addition to qualified human, organizational, regulatory and functional resources in this area, this strategy aims at providing our country, with capabilities for prevention, detection and response to cyber incidents, whether these incidents are of accidental or malicious origins, through the implementation of effective means.**

Effectively and in the long term, this strategy sets objectives enabling our country to acquire and ensure sovereignty in cyberspace and to dispose of know-how in this complex and sensitive domain relating to national security.

These strategic objectives aim, in particular, to strengthen Algeria's technical-operational capabilities, through the establishment of an appropriate environment in terms of cybersecurity, capable of facing any threat or challenge, in a particularly sensitive context, marked by the emergence of new technologies and digital transformation, which constitutes an imperative that cannot be discarded from any prospective vision of our country and its development.

The strategic objectives of this strategy are as follows:

01 **Building the cyber-resilience of the national information systems.**

02 **Working towards a convenient national cybersecurity ecosytem.**

03 **Establishing a national framework for the development of qualified human resources in cybersecurity.**

04 **Promoting cooperation in cybersecurity.**

# IV. Guiding Principles

The following guiding principles will serve as a guide for the implementation of this strategy :

01 **Strenthening the national digital sovereignty.**

02 **Assisting the digital transformation intiated by the State.**

03 **Preserving the acquirements achieved.**

04 **Promoting inclusiveness.**

05 **Encouraging resources sharing.**

06 **Setting achievable and measurable goals.**

# V. Axes of the national strategy of information systems security

To materialize the strategic objectives that fall under this strategy, efforts to be made are divided over the following four (04) axes:

- **Axe 01** Technical-operational capabilities.
- **Axe 02** Legal, organizational and normative framework.
- **Axe 03** Training, research-development and awareness.
- **Axe 04** National and international cooperation.

### V.1. Axis 1 : Technical-operational capabilities

The development of technical-operational capabilities in terms of protection and resilience of national information systems as well as critical infrastructures aims to provide our country with means of prevention, detection and response to cyber incidents, through the fulfillment of the following objectives:

1. Consolidating the protection of national information systems as well as critical infrastructures ;
2. Strengthening national technical-operational capabilities for prevention, detection and response to incidents.

### V.2. Axis 2 : Legal, organizational and normative framework

Due to the transversal nature of this axis, the objectives included their aim at providing our country with an adequate legal, normative and organizational framework allowing it to achieve the strategic vision and, thus, guarantee national cyber-resilience. These objectives are as follows:

1. Strengthening the legal and organizational framework ;
2. Establishing a normative framework.

### V.3. Axis 3 : Training, research-development and awareness

The objectives, listed under this axis, aim at equipping the workforce, regarded as the most important link in the security chain, with the necessary skills and knowledge to enable them to carry out their missions in cyberspace in a safe and efficient way:

1. Disposing of qualified human resources in cybersecurity ;
2. Promoting research-development and innovation in cybersecurity ;
3. Fostering cybersecurity culture.

### V.4. Axis 4 : National and international cooperation

The national cooperation aims at optimizing as well as sharing means of action, also promoting information exchange in all aspects related to cybersecurity, not only between the public and private sectors but also with the Information Systems Security Agency.

Furthermore, and at the international level, this cooperation in the field of cybersecurity constitutes an essential vector for our country, with a view of harmonizing actions and of facing cyber threats in a collective way, through the establishment of efficient operations links.

The objectives set out under this axis are as follows:

1. Promoting and enhancing collaboration and partnership in the field of cybersecurity between all stakeholders at the national level ;
2. Supervising international cooperation at the strategic and technical-operational levels in the field of cybersecurity ;
3. Contributing actively to the process of establishing international legal, normative and framework in the field of cybersecurity.