Presidency of the Republic
General Secretariat
Subheading for Legal Affairs

DECREE No. 9,637, OF DECEMBER 26, 2018

Establishes the National Information Security Policy, provides for the governance of information security, and amends Decree No. 2,295, of August 4, 1997, which regulates the provisions of art. 24, caput, item IX, of Law No. 8,666, of June 21, 1993, and provides for the exemption from bidding in cases that may compromise national security.

THE PRESIDENT OF THE REPUBLIC, in the use of the attribution conferred on him by art. 84, **caput**, item VI, point "a", of the Constitution,

DECREES:

CHAPTER I

GENERAL PROVISIONS

~~Art. 1 The National Information Security Policy - PNSI is hereby established, within the federal public administration, in order to ensure the availability, integrity, confidentiality and authenticity of information at the national level.~~

Art. 1 The National Information Security Policy - PNSI is hereby established, within the federal public administration, in order to ensure the availability, integrity, confidentiality and authenticity of information at national level. (Wording given by Decree No. 10,641 of 2021)

Art. 2 For the purposes of the provisions of this Decree, information security covers:

I - cyber security;

II - cyber defense;

III - physical security and organizational data protection; and

IV - actions aimed at ensuring the availability, integrity, confidentiality and authenticity of information.

CHAPTER II

THE PRINCIPLES

Art. 3 Are principles of the National Information Security Policy - PNSI:

I - national sovereignty;

II - respect and promotion of human rights and fundamental guarantees, especially freedom of expression, protection of personal data, protection of privacy and access to information;

III - comprehensive and systemic view of information security;

IV - responsibility of the Country in the coordination of efforts and in the establishment of policies, strategies and guidelines related to information security;

V - scientific and technological exchange related to information security between the bodies and entities of the federal public administration;

VI - preservation of the national historical collection;

VII - education as a fundamental foundation for the promotion of information security culture;

VIII - guidance on risk management and information security management;

IX - prevention and treatment of information security incidents;

X - articulation between actions of cyber security, cyber defense and protection of data and information assets;

XI - duty of public bodies, entities and agents to ensure the secrecy of information essential to the security of society and the state and the inviolability of the intimacy of private life, honor and image of people;

XII - **need to know** for access to confidential information, in accordance with the legislation;

XIII - consent of the owner of confidential information received from other countries, in the cases of international agreements;

XIV - cooperation between investigative bodies and public bodies and entities in the process of accrediting persons for access to confidential information;

XV - integration and cooperation between the public authorities, the business sector, society and academic institutions; and

XVI - international cooperation, in the field of information security.

CHAPTER III

THE OBJECTIVES

Art. 4 The following are objectives of the National Information Security Policy - PNSI:

I - to contribute to the security of the individual, society and the State, through the guidance of information security actions, observing the fundamental rights and guarantees;

II - to promote scientific research, technological development and innovation activities related to information security;

III - to continuously improve the legal and regulatory framework related to information security;

IV - to promote the training and qualification of the human resources necessary for the area of information security;

V - to strengthen the culture of information security in society;

VI - to guide actions related to:

a) security of data held by public entities;

b) security of the critical infrastructures information;

c) protection of the information of natural persons who may have their security or the security of their activities affected, in compliance with specific legislation; and

d) processing of access-restricted information; and

VII - to contribute to the preservation of the Brazilian cultural memory.

CHAPTER IV

THE INSTRUMENTS

Art. 5 The following are instruments of the National Information Security Policy - PNSI:

I - the National Information Security Strategy; and

II - the national plans.

Art. 6 The National Information Security Strategy will contain the strategic actions and objectives related to information security, in line with the public policies and programs of the Federal Government, and will be divided into the following modules, among others, to be defined at the time of its publication:

I - cyber security;

II - cyber defense;

III - critical infrastructure security;

IV - security of confidential information; and

V - protection against data leakage.

Single paragraph. The construction of the National Information Security Strategy will have the broad participation of society and the public bodies and entities.

Art. 7 The national plans referred to in item II of the **caput** of art. 5 shall contain:

I - the details for the implementation of the strategic actions and objectives of the National Information Security Strategy;

II - the planning, organization, coordination of activities and the use of resources for the execution of strategic actions and the achievement of the objectives of the National Information Security Strategy; and

III - the assignment of responsibilities, the definition of schedules and the presentation of the risk analysis and contingency actions that guarantee the achievement of the expected results.

Single paragraph. The national plans will be divided into themes and assigned to a responsible body, as established in the National Information Security Strategy.

CHAPTER V

THE INFORMATION SECURITY MANAGEMENT COMMITTEE

Art. 8 The Information Security Management Committee is established, assigned to advise the Institutional Security Cabinet of the Presidency of the Republic in activities related to information security.

Art. 9 The Committee will be composed of a titular representative and their alternate appointed by the following bodies:

I - Institutional Security Cabinet of the Presidency of the Republic, which will coordinate it;

II - Civil House of the Presidency of the Republic;

~~III - Ministry of Justice;~~

III - Ministry of Justice and Public Security; (Wording given by Decree No. 9,832 of 2019)

~~IV - Ministry of Public Security;~~

IV - Ministry of Defense; (Wording given by Decree No. 9,832 of 2019)

~~V - Ministry of Defense;~~

V - Ministry of Foreign Affairs; (Wording given by Decree No. 9,832 of 2019)

~~VI - Ministry of Foreign Affairs;~~

VI - Ministry of Economy; (Wording given by Decree No. 9,832 of 2019)

~~VII - Ministry of Finance;~~

VII - Ministry of Infrastructure; (Wording given by Decree No. 9,832 of 2019)

~~VIII - Ministry of Transport, Ports and Civil Aviation;~~

VIII - Ministry of Agriculture, Livestock and Supply; (Wording given by Decree No. 9,832 of 2019)

~~IX - Ministry of Agriculture, Livestock and Supply;~~

IX - Ministry of Education; (Wording given by Decree No. 9,832 of 2019)

~~X - Ministry of Education;~~

X - Ministry of Citizenship; (Wording given by Decree No. 9,832 of 2019)

~~XI - Ministry of Culture;~~

XI - Ministry of Health; (Wording given by Decree No. 9,832 of 2019)

XI-A – Ministry of Labor and Welfare (Wording given by Decree No. 10,849 of 2021)

~~XII - Ministry of Labour;~~

XII - Ministry of Mines and Energy; (Wording given by Decree No. 9,832 of 2019)

XII-A - Ministry of Communications; (Included by Decree No. 10,641 of 2021)

~~XIII - Ministry of Social Development;~~
~~XIII - Ministry of Science, Technology, Innovation and Communications; (Wording given by Decree No. 9,832 of 2019)~~

XIII - Ministry of Science, Technology and Innovation; (Wording given by Decree No. 10,641 of 2021)

~~XIV - Ministry of Health;~~

XIV - Ministry of Environment; (Wording given by Decree No. 9,832 of 2019)

~~XV - Ministry of Industry, Foreign Trade and Services;~~

XV - Ministry of Tourism; (Wording given by Decree No. 9,832 of 2019)

~~XVI - Ministry of Mines and Energy;~~

XVI - Ministry of Regional Development; (Wording given by Decree No. 9,832 of 2019)

~~XVII - Ministry of Planning, Development and Management;~~

XVII - Comptroller General; (Wording given by Decree No. 9,832 of 2019)

~~XVIII - Ministry of Science, Technology, Innovations and Communications;~~

XVIII - Ministry of Women, Family and Human Rights; (Wording by Decree No. 9,832 of 2019)

~~XIX - Ministry of Environment;~~

XIX - General Secretariat of the Presidency of the Republic; (Wording given by Decree No. 9,832 of 2019)

~~XX - Ministry of Sport;~~

XX - Secretariat of Government of the Presidency of the Republic; (Wording given by Decree No. 9,832 of 2019)

~~XXI - Ministry of Tourism;~~

~~XXI - Attorney General's Office; and~~ (Wording given by Decree No. 9,832 of 2019)

XXI – Attorney General's Office; (Wording given by Decree No. 10,849 of 2021)

~~XXII - Ministry of National Integration;~~

~~XXII - Central Bank of Brazil.~~ (Wording given by Decree No. 9,832 of 2019)

XXII – Central Bank Of Brazil; and (Wording given by Decree No. 10,849 of 2021)

XXII-A – National Data Protection Authority." (Wording given by Decree No. 10,849 of 2021)

~~XXIII - Ministry of Cities;~~ (Revoked by Decree No. 9,832 of 2019)
~~XXIV - Ministry of Transparency and Comptroller General;~~ (Revoked by Decree No. 9,832 of 2019)
~~XXV - Ministry of Human Rights;~~ (Revoked by Decree No. 9,832 of 2019)
~~XXVI - General Secretariat of the Presidency of the Republic;~~ (Revoked by Decree No. 9,832 of 2019)
~~XXVII - Secretariat of Government of the Presidency of the Republic;~~ (Revoked by Decree No. 9.832 of 2019)
~~XXVIII - Attorney General's Office; and~~ (Revoked by Decree No. 9,832 of 2019)
~~XXIX - Central Bank of Brazil.~~ (Revoked by Decree No. 9,832 of 2019)

~~§ 1 The members of the Committee shall be appointed by the members of the bodies mentioned in the **caput** , within ten days from the date of publication of this Decree, and shall be appointed by act of the Minister of State Head of the Institutional Security Office of the Presidency of the Republic, within twenty days from the date of publication of this Decree.~~

§ 1 The members of the Information Security Management Committee and their alternates shall be appointed by the members of the bodies they represent and appointed by act of the Minister of State Head of the Institutional Security Cabinet of the Presidency of the Republic. (Wording given by Decree No. 10,641 of 2021)

~~§ 2 The appointment of the titular member of the bodies mentioned in the **caput** shall be made by the information security manager referred to in item III of the **caput** of art. 15, and the respective alternate shall hold a commissioned position of the Senior Management and Advisory Group, level 4 or higher, or equivalent.~~
~~§ 2 The titular member of the Information Security Management Committee shall be the information security manager referred to in item III of the **caput** of art. 15, and their alternate shall hold a commissioned position or trust function equivalent to or higher than level 4 of the Senior Management and Advisory Group.~~ (Wording given by Decree No. 9.832 of 2019)

§ 2 The members covered by § 1 must be appointed from among the public agents who have the task to define policies or regulations related to information technology or information security in their respective bodies. (Wording given by Decree No. 10,641 of 2021)

§ 3 The full members of the Committee shall be replaced by their alternates, in their absences or impediments.

~~§ 4 Participation in the Committee shall be deemed to provide relevant, unpaid public service.~~

§ 4 Participation in the Information Security Management Committee and in the subcollegiates shall be considered as providing a relevant unpaid public service. (Wording given by Decree No. 9,832 of 2019)

~~§ 5 Within ninety days from the date of publication of this Decree, internal rules will be approved to provide for the organization and functioning of the Committee.~~

§ 5 The Coordinator of the Information Security Management Committee will approve the internal rules, which shall provide for the organization and functioning of the Committee, within ninety days from the date of publication of Decree No. 9,832 of June 12, 2019. (Wording given by Decree No. 9,832 of 2019)

Art. 10. The Committee shall meet, on an ordinary basis, biannually and, on an extraordinary basis, by convocation of its Coordinator.

§ 1 The meetings of the Committee shall take place, at first convocation, with the presence of a simple majority of its members or, fifteen minutes after the established time, at second convocation, with the presence of at least one third of its members.

~~§ 2 The committee may establish working groups or technical chambers to deal with specific issues related to information security and may invite representatives of the public or private sector and experts with notable knowledge.~~ (Revoked by Decree No. 9,832 of 2019)

~~§ 3 The composition, functioning and competences of the working groups or technical chambers shall be established by the Committee.~~ (Revoked by Decree No. 9,832 of 2019)

§ 4 The deliberations of the Committee will be approved by a simple majority of the members present and the Coordinator, in addition to the regular vote, will have the casting vote.

~~§ 5 The members of the Information Security Management Committee that are in the Federal District will meet in person and the members that are in other federal entities will participate in the meeting through videoconference.~~ ~~(Included by Decree No. 9,832 of 2019)~~

§ 5 The members of the Information Security Management Committee who are in the Federal District will meet in person or by videoconference, in accordance with the provisions of Decree No. 10,416 of July 7, 2020, and members who are in other federal entities will participate in the meeting by videoconference. (Wording given by Decree No. 10,641 of 2021)

Art. 10-A. The Information Security Management Committee may establish subcollegiates with the aim of dealing with specific issues related to information security. (Included by Decree No. 9,832 of 2019)

Art. 10-B. The subcollegiates referred to in art. 10-A: (Included by Decree No. 9,832 of 2019)

I - will be composed in the form of an act of the Information Security Management Committee; (Included by Decree No. 9,832 of 2019)

II - may not have more than seven members; (Included by Decree No. 9,832 of 2019)

III - will have a temporary character and duration not exceeding one year; and (Included by Decree No. 9,832 of 2019)

IV - are limited to four operating simultaneously. (Included by Decree No. 9,832 of 2019)

~~Art. 11. The Institutional Security Cabinet of the Presidency of the Republic will provide the necessary technical and administrative support to the Committee.~~

~~Art. 11. The Executive Secretariat of the Information Security Management Committee will be exercised by the Information Security Department of the Systems Coordination Secretariat of the Institutional Security Cabinet of the Presidency of the Republic.~~ ~~(Wording given by Decree No. 9,832 of 2019)~~

Art. 11. The Executive Secretariat of the Information Security Management Committee will be exercised by the Information Security Department of the Institutional Security Cabinet of the Presidency of the Republic. (Wording given by Decree No. 10,641 of 2021)

CHAPTER VI

THE POWERS

Section I

Of the Institutional Security Cabinet of the Presidency of the Republic

~~Art. 12. It is the responsibility of the Institutional Security Cabinet of the Presidency of the Republic, in matters related to information security, advised by the Information Security Management Committee:~~

Art. 12. It is the responsibility of the Institutional Security Cabinet of the Presidency of the Republic, in matters related to information security: (Wording given by Decree No. 10,641 of 2021)

I - establish standard on the definition of methodological requirements for the implementation of risk management of information assets by bodies and entities of the federal public administration;

II - approve guidelines, strategies, regulations and recommendations;

III - develop and implement programs on information security aimed at the awareness and training of federal public servants and society;

IV - follow the doctrinal and technological evolution, at national and international level;

V - prepare and publish the National Information Security Strategy, in conjunction with the Interministerial Committee for Digital Transformation, created by Decree No. 9.319, of March 21, 2018;

VI - support the preparation of national plans linked to the National Information Security Strategy;

VII - establish criteria that allow the monitoring and evaluation of the implementation of the National Information Security Policy - PNSI and its instruments;

~~VIII - propose the editing of the normative acts necessary for the implementation of the National Information Security Policy - PNSI; and~~

VIII - propose the edition of the normative acts necessary for the execution of the National Information Security Policy - PNSI; (Wording given by Decree No. 10,641 of 2021)

~~IX - establish minimum security requirements for the use of products that incorporate information security features, in order to ensure the availability, integrity, confidentiality and authenticity of information and ensure interoperability between information security systems, subject to the specific competences of other bodies.~~

IX - establish the minimum security requirements for the use of products that incorporate information security features, in order to ensure the availability, integrity, confidentiality and authenticity of information and ensure interoperability among information security systems, subject to the specific competences of other bodies; and (Wording given by Decree No. 10,641 of 2021)

X - articulate with national centers for prevention, treatment and response to cyber incidents belonging to other countries. (Included by Decree No. 10,641 of 2021)

Single paragraph. In the cases covered by item IX of the **caput**, when it comes to the power of another body, it will be up to the Institutional Security Cabinet of the Presidency of the Republic to propose updates regarding information security.

Section II

Of the Ministry of Defense

Art. 13. It is responsibility of the Ministry of Defense to:

I - support the Institutional Security Cabinet of the Presidency of the Republic in activities related to cyber security; and

II - elaborate the guidelines, the devices and the defense procedures that act in the systems related to the national defense against cyber attacks.

~~**Section III**~~
~~**The Ministry of Transparency and Comptroller General**~~

Section III

Of the Comptroller-General

(Wording given by Decree No. 10,641 of 2021)

~~Art. 14. The Ministry of Transparency and Comptroller General is responsible for auditing the execution of the actions of the National Information Security Policy of the bodies and entities of the federal public administration.~~

Art. 14. It is the responsibility of the Comptroller General to audit the execution of the actions of the National Information Security Policy - PNSI of responsibility of the bodies and entities of the federal public administration. (Wording given by Decree No. 10,641 of 2021)

Section IV

Of the bodies and entities of the federal public administration

Art. 15. The bodies and entities of the federal public administration, in their scope of action, are responsible for:

I - implementing the National Information Security Policy - PNSI;

II - elaborating its information security policy and internal information security regulations, observed the information security regulations published by the Institutional Security Office of the Presidency of the Republic;

III - designating an internal information security manager, appointed by the senior management of the body or entity;

IV - establishing information security committee or equivalent structure, to deliberate on matters related to the National Information Security Policy - PNSI;

V - allocating budgetary resources for information security actions;

VI - promoting training and professionalization of human resources in topics related to information security;

~~VII - instituting and implementing a computer networks incident treatment and response team , which will compose the network formed by the teams of the bodies and entities of the federal public administration, coordinated by the Brazilian Government Response Team for Computer Security Incidents of the Institutional Security Office of the Presidency of the Republic;~~

VII - instituting and implementing a cyber security incident prevention, treatment and response team, which will compose the network of teams of the bodies and entities of the federal public administration, coordinated by the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, of the Information Security Department of the Institutional Security Cabinet of the Presidency of the Republic; (Wording given by Decree No. 10,641 of 2021)

VIII - coordinating and executing information security actions within the scope of its activity;

IX - consolidating and analyzing the results of audit work on information security management; and

X - applying the corrective and disciplinary actions applicable in cases of violation of information security.

§ 1 The internal information security committee referred to in item IV of the **caput** shall be composed of:

I - the information security manager of the body or entity referred to in item III of the **caput**, who will coordinate it;

II - a representative of the Executive Secretariat or equivalent unit of the body or entity;

III - a representative of each finalistic unit of the body or entity; and

IV - the holder of the information and communication technology unit of the body or entity.

~~§ 2 The members of the internal information security committee covered by items II and III of § 1 shall hold a commissioned position of Senior Management and Advisory Group, level 5 or higher, or equivalent.~~

~~§ 2 The members of the internal information security committee covered by items I to III of § 1 shall hold a commissioned position or trust function of level 5 or higher of the Senior Management and Advisory Group or equivalent.~~ ~~(Wording given by Decree No. 9,832 of 2019)~~ ~~(Revoked by Decree No. 10,641 of 2021)~~

§ 3 The internal information security committee of the bodies and entities of the federal public administration has the following tasks:

I - advise on the implementation of information security actions;

II - establish working groups to deal with issues and propose specific solutions on information security;

III - propose changes to the internal information security policy; and

IV - propose internal regulations regarding information security.

§ 4 The information security manager shall be appointed from among the public servants occupying effective office, public and military employees of the body or entity, with education or technical training compatible with the regulations established by this Decree. (Included by Decree No. 10,641 of 2021)

Art. 16. The bodies and entities of the federal public administration will edit acts to define the way of functioning of the respective information security committees, observing the provisions of this Decree and the legislation.

Art. 17. It is the responsibility of the senior administration of the bodies and entities of the federal public administration the governance of information security, and especially to:

I - promote administrative simplification, modernization of public management and integration of public services, especially those provided by electronic means, aiming at information security;

II - monitor the performance and evaluate the design, implementation and results of its information security policy and internal information security regulations;

III - incorporate high standards of conduct to ensure information security and guide the behavior of public agents, in line with the functions and assignments of their bodies and entities;

IV - planning the execution of programs, projects and processes related to information security;

V - establish guidelines for the information security risk management process;

VI - observe the regulations that establish requirements and procedures for information security published by the Institutional Security Cabinet of the Presidency of the Republic;

VII - implement internal controls based on information security risk management;

VIII - establish an information security management system;

IX - implement immediate communication mechanism on the existence of vulnerabilities or security incidents that impact or may impact the services provided or contracted by federal public administration bodies; and

X - observe the applicable specific regulations and procedures, implement and maintain mechanisms, instances and practices of information security governance in accordance with the principles and guidelines established in this Decree and in the legislation.

§ 1 The planning and execution of programs, projects and processes related to information security covered by item IV of the **caput** will be oriented to:

I - the use of cryptographic resources appropriate to the degrees of secrecy required in the processing of information and the access restrictions established for the sharing of information, observed the legislation;

II - increasing the resilience of information and communication technology assets and services defined as strategic by the federal Government;

~~III - the continuous cooperation among the security incident response and treatment teams in the direct, municipal and foundational federal public administration and the Government Network Incident Treatment Center of the Institutional Security Cabinet of the Presidency of the Republic; and~~

III - the continuous cooperation among the teams of prevention, treatment and response to cyber incidents in the direct, municipal and foundational federal public administration and the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, of the Information Security Department of the Institutional Security Cabinet of the Presidency of the Republic; and (Wording given by Decree No. 10,641 of 2021)

IV - prioritizing the interoperability of technologies, processes, information and data, with the promotion of:

a) the integration and sharing of information assets of the federal government or those in its custody;

b) the standardization and reduction of fragmentation of information bases of interest to the federal Government and society;

c) the integration and sharing of the telecommunications networks of the direct, autarchic and foundational federal public administration; and

d) the standardization of communication among systems.

§ 2 The information security management system referred to in item VIII of the **caput** will identify the needs of the organization regarding information security requirements and implement the information security risk management process.

~~Art. 18. All the bodies and entities of the direct, autarchic and foundational federal public administration, on the administrative acts that involve information technology assets, without prejudice to the other legal provisions, shall incorporate the information security regulations established by the Institutional Security Cabinet of the Presidency of the Republic, and the standards for information and communication technology management and information security of the Ministry of Planning, Development and Management.~~

Art. 18. The bodies and entities of the direct, autarchic and foundational federal public administration, in administrative acts involving information technology assets, without prejudice to other legal provisions, shall incorporate the information security regulations established by the Institutional Security Cabinet of the Presidency of the Republic. (Wording given by Decree No. 10,641 of 2021)

CHAPTER VII

FINAL PROVISIONS

Art. 19. The Minister of State Head of the Institutional Security Cabinet of the Presidency of the Republic will publish, within ninety days from the date of publication of this Decree, a glossary with the definition of technical and operational terms relating to information security, which will be used as a conceptual reference for the rules and regulations related to information security.

Art. 20. The Minister of State Head of the Institutional Security Cabinet of the Presidency of the Republic may issue additional acts necessary for the application of this Decree.

~~Art. 21. Decree No. 2,295 of August 4, 1997, comes into force with the following amendments: (Revoked by Decree No. 10,631 of 2021)~~

~~"Art. 1 ....~~

~~III - acquisition of equipment and hiring of specialized technical services for the areas of intelligence, information security, cyber security, communications security and cyber defense.~~

~~....."~~

~~(NR)~~

Art. 22. Are revoked:

I - Decree No. 3,505 of June 13, 2000; and

II - Decree No. 8,135 of November 4, 2013.

Art. 23. This Decree comes into force on the date of its publication.

Brasília, December 26, 2018; 197th of Independence and 130th of the Republic.

MICHEL TEMER
Sergio Westphalen Etchegoyen

This text does not replace the one published in the DOU of 12/27/2018