PRESIDENTIAL DECREE 7845, NOVEMBER 14, 2012

Regulates procedures for the accreditation for treatment and security of classified information at any secrecy level, and provides for the Security and Accreditation Center.

The PRESIDENT OF THE REPUBLIC, using the powers conferred upon her by Article 84, caput, items IV and VI, subparagraph "a" of the Federal Constitution and in view of the provisions of Articles 25, 27, 29, 35, Paragraph 5, and Article 37 of Law 12527, of November 18, 2011,

DECREES:

CHAPTER I
GENERAL PROVISIONS

Article 1. This decree regulates procedures for the treatment accreditation and security of classified information at any secrecy level within the federal executive branch, and provides for the Security and Accreditation Center, as determined in Articles 25, 27, 29, 35, Paragraph 5, and Article 37 of Law 12527, of November 18, 2011.

Article 2. For the purposes of this Decree, the following shall be considered:

I – a State algorithm – a mathematical function used in encryption and decryption, developed by the State for sole use in the interests of the service of federal executive branch agencies or entities;

II – encryption – the act of encrypting through symmetric or asymmetric algorithms, using cryptographic signs to replace the clear language signs by others unintelligible to unauthorized people;

III – an indexing code – an alphanumeric code that indexes documents with classified information at any secrecy level;

IV – impairment - the loss of security resulting from unauthorized access;

V – a confidential contract – an adjustment, agreement or cooperation agreement whose object or performance involves handling classified information;

VI – a security credential – a certificate authorizing a person to handle classified information;

VII – security accreditation – a process used to enable a public or private agency or entity, and to accredit a person, to handle classified information;

VIII – decryption – the act of deciphering through use of symmetric or asymmetric algorithms, with a cryptographic resource, to reverse the original encryption;

IX – mobile devices – portable devices equipped with computing power or removable memory storage devices;

X – a security and accreditation manager – a person responsible for the security of classified information at any secrecy level with the registry agency and the control checkpoint;

XI – marking – affixing a tag that indicates the secrecy level of classified information;

XII – security measures – measures to ensure secrecy, sanctity, integrity, authenticity and availability of classified information at any secrecy level;

XIII – level 1 registry agency – a ministry or equivalent level agency enabled by the Center for Security and Accreditation;

XIV – level 2 registry agency – a public agency or entity linked to and enabled by a level 1 registry agency;

XV – a checkpoint – a unit body or public or private entity, empowered, responsible for the storage of classified information at any secrecy level;

XVI – a security breach – an action or omission that jeopardizes or risks compromising classified information at any secrecy level;

XVII – a cryptographic feature – a system, program, process, isolated or network equipment that uses symmetric or asymmetric algorithms to perform encryption or decryption;

XVIII – treatment of classified information – a set of actions relating to production, reception, classification, use, access, reproduction, transportation, transmission, distribution, archiving, storage, disposal, valuation, disposition or control of classified information at any secrecy level.

CHAPTER II
SECURITY ACCREDITATION

Section I
Agencies

Article 3. It is the responsibility of the Security and Accreditation Center, the central agency of security accreditation, established under the Cabinet of Institutional Security of the Presidency, pursuant to Article 37 of Law 12527, 2011:

I – to enable level 1 registry agencies to provide security accreditation of public and private agencies and entities, and individuals for the treatment of classified information;

II – to enable level 1 agency checkpoints to store classified information at any secrecy level;

III – to enable private entities that maintain any kind of relationship with the Institutional Security Cabinet of the Presidency for the treatment of classified information;

IV – to accredit persons who maintain any kind of relationship with the Institutional Security Cabinet of the Presidency for the treatment of classified information;

V – to perform inspections and investigations for security accreditation necessary to implementation the provisions, respectively, in sections III and IV of the caput, and

VI – to monitor compliance with security accreditation and treatment of classified information standards and procedures.

Article 5. It is the duty of the Information Security Steering Committee established by Decree No. 9,637, of December 26, 2018:

I – to propose general guidelines for security accreditation to handle classified information;

II – to set parameters and minimum requirements for:

a) technical qualification of public and private agencies and entities regarding security accreditation, on the terms of Articles 10 and 11, and

b) granting security credentials for persons, pursuant to Article 12.

III – to regularly evaluate the compliance with this Decree.

Article 6. It is the responsibility of the Institutional Security Cabinet of the Presidency:

I – to issue additional acts and to establish procedures for security accreditation and for the treatment of classified information;

II – to participate in treaty, agreement or international act negotiations related to the treatment of classified information, jointly with the Ministry of Foreign Affairs;

III – to monitor investigations and evaluation processes, and recovery of damages resulting from security breaches;

IV – to report on any damage, referred to in item III of the caput, to the country or international organization of origin, where necessary, through diplomatic channels, and

V – to advise the President of the Republic on matters related to security accreditation to handle classified information, including the ones regarding treaties, agreements or international acts, subject to the jurisdiction of the Ministry of Foreign Affairs.

Sole paragraph. The Institutional Security Cabinet of the Presidency of the Republic shall act as the national security authority for handling classified information arising from treaties, agreements or international acts.

Article 7. It is the duty of the level 1 national registry agency;

I – to enable level 2 registry agencies to accredit persons for the treatment of classified information;

II – to enable checkpoints within public or private agencies and entities that maintain any kind of link with the national agency, to store classified information at any secrecy level;

III – to accredit persons who maintain relationships of any kind with the national agency, for the treatment of classified information;

IV – to perform inspections and investigations for security accreditation, required to implement the provisions of item III of the caput, and

V – to monitor the compliance with security accreditation and classified information treatment standards and procedures, within its responsibilities.

Article 8. It is the duty of the level 2 national registry agency to undertake the investigation and accreditation of persons who maintain any relationship whatsoever with it, in the treatment of classified information.

Sole paragraph. The responsibility for carrying out inspection and investigation provided in Article 7, item IV, caput, may be delegated to a level 2 registry agency.

Article 9. It is the duty of the checkpoint:

I – to control of the security credentials of the people who maintain a relationship with it, and

II – to guarantee the security of classified information at any secrecy level, under their responsibility.

Section II

Procedures

Article 10. Enabling public authorities and bodies for security accreditation shall be subject to the following requirements:

I – evidence of technical skills necessary to the security of classified information at any secrecy level, and

II – the designation and accreditation of a Security Manager, and a substitute.

Article 11. Enabling a private entity as checkpoint shall be subject to the following requirements:

I – the entity’s tax compliance;

II – evidence of technical skills necessary to the security of classified information at any secrecy level;

III – expected signature of confidential contract;

IV – the designation and accreditation of a Security Manager and a substitute, and

V – approval upon a security clearance inspection.

Article 12. The granting of a security credential to a person is subject to the following requirements:

I – a request from the public or private agency or entity in which the person is employed;

II – the filled out form with personal information and authorizing its investigation;

III – aptitude for the treatment of classified information, verified through investigation, and

IV – a declaration of knowledge of the rules and procedures for security accreditation and treatment of classified information.

Article 13. Enabling for security accreditation and granting security credentials will result from the objective analysis of the requirements foreseen in this Decree.

Article 14. The level 1 and level 2 agencies may sign adjustments, covenants or terms of cooperation with other public agencies or entities, entitled to:

I – grant security accreditation and treat classified information, and

II – conduct inspections and investigations for security accreditation.

Article 15. Each agency will have at least one enabled checkpoint.

Article 16. In case of exchange and treatment of classified information at any secrecy level with a foreign country or organization, security accreditation in national territory will be granted only upon a treaty, agreement, or memorandum of understanding or technical adjustment, signed between the country or foreign organization and the Federative Republic of Brazil.

CHAPTER III
CLASSIFIED INFORMATION TREATMENT

Section I
General Provisions

Article 17. The agencies and entities shall adopt measures so that public officials know the rules and comply with the security accreditation and classified information treatment procedures.

Sole paragraph. The provisions set forth in the caput apply to the person or private entity which, by reason of any link with the government, runs security accreditation or classified information treatment activities.

Article 18. Access, disclosure and treatment of classified information will be restricted to people who need to know it and are accredited in accordance with this Decree, notwithstanding the powers of public officials authorized by law.

Sole paragraph. Access to classified information at any secrecy level to personnel non accredited or non authorized by law may be exceptionally permitted, subject to the signature of the Secrecy Maintenance Commitment Statement – TCMS, in Annex I, in which the person shall undertake the maintenance of information secrecy under the penalty of criminal, civil and administrative accountability provided by law.

Article 19. The decision of classification, declassification, reclassification or reduction of the secrecy period of classified information at any secrecy level will follow the procedures set forth in Articles 31 and 32 of Decree 7724 of May 16, 2012, and should be formalized in a decision embodied in the Information Classification Term.

Article 20. The publication of normative acts relating to classified information at any secrecy level or protected by law or court secrecy may be limited, when necessary, to their respective numbers, issuance dates and summaries, drafted so as not to compromise the secrecy.

Section II
Controlled Documents

Article 21. For the treatment of documents containing classified information at any secrecy level or considered classified by law, the agency or entity may adopt the following additional control procedures:

I – identification of the recipients in a specific protocol and receipt;

II – a custody term and a registry on a specific protocol;

III – an annual inventory term, by the issuing agency or entity and by the consignor or recipient agency or entity, and

IV – a custody or guardianship transfer term.

Paragraph 1 – The document in the caput will be called Controlled Document - DC.

Paragraph 2 – The inventory term provided in item number III of the caput shall contain at least the following elements:

I – sequential numbering and date;

II – DC producer and custodian agencies;

III – a list of controlled documents;

IV – place and signature.

Paragraph 3 – The transferring term provided in item IV of the caput should contain at least the following elements:

I – sequential numbering and date;

II – substitute and replaced officials;

III – identification of documents or inventory terms to be transferred, and

IV – place and signature.

Article 22. Ultra secret documents are considered DC since classification or reclassification.

Section III
Marking

Article 23. Marking shall be done on the headers and footers of the pages that contain classified information and on the document covers.

Paragraph 1 – The pages will be numbered in a sequence, each containing an indication of the total number of pages that make up the document.

Paragraph 2 – The marking shall be made so as not to impair comprehension of the information.

Article 24. The DC will possess the marking mentioned in Article 23 and will contain, on the cover and on every page, the expression "Controlled Document (DC)" diagonally, and the control number, which will indicate the public custodian official.

Article 25. The indication of the secrecy level on maps, photomaps, letters, photographs, any other type of images and electronic storage means will obey to the complementary procedures adopted by the agencies and entities.

Section IV
Expedition, Processing and Communication

Article 26. The expedition and processing of classified documents shall follow these procedures:

I – they will be placed in double envelopes;

II – the outer envelope shall not bear any indication of the document’s secrecy level or content;

III – on the inner envelope there shall be written the recipient’s name and the level of the document, so they can be identified as soon as removed from the outer envelope;

IV – the inner envelope shall be closed, sealed and issued upon receipt, specifying the sender, recipient and number or another indication that identifies the document, and

V – the word "PRIVATE" will be inscribed on the envelope that contains a document of the recipient’s exclusive interest.

Article 27. The expedition, conduction and delivery of a document containing classified information on an ultra secret secrecy level shall be made in person, by a licensed public agent, or transmitted by electronic means, provided that encryption features are used, compatible with the information classification level, and shall not be sent by regular mail.

Article 28. The issuance of documents with information classified at secret or reserved secrecy levels shall be made through the available media, with encryption features consistent with the secrecy level or, if applicable, through diplomatic channels, notwithstanding personal delivery.

Article 29. The recipient of the document containing classified information at any secrecy level, regardless of means and format, shall be responsible for:

I – registering the document receipt;

II – verifying the integrity of the means of receipt and recording evidence of irregularity or violation, informing the recipient, who shall immediately inform the sender; and

III – informing the sender of the receipt of the information, in the shortest time possible.

Paragraph 1 – In case the processing occurs by internal mail or correspondence, the inner envelope will only be opened by the recipient, his authorized representative or higher authority.

Paragraph 2 – Envelopes containing the "PRIVATE" internal mark shall be opened exclusively by the recipient.

Article 30. The information classified at any secrecy level shall be maintained or filed under special security conditions.

Paragraph 1 – For the maintenance and archiving of information classified at ultra secret and secret secrecy levels, it is mandatory to use equipment, environments or structures that provide security compatible with the secrecy level.

Paragraph 2 – For the electronic storage of documents containing information classified at any secrecy level, it is mandatory to use information technology systems updated to prevent security threat breaches, subject to the provisions of Article 38.

Paragraph 3 – The storage media may be integrated into equipment connected to the internet, as long as through a secure channel with access control levels adequate for the treatment of classified information, also allowing connection to internal computer networks, provided that they are safe and controlled.

Article 31. Electronic storage of classified information at any secrecy level, including mobile devices, must use cryptographic features appropriate to the secrecy level.

Article 32. The agents responsible for the safekeeping or custody of controlled documents shall pass them on to their substitutes, after duly conferring them, upon the passage or transfer of responsibility.

Sole paragraph. the provisions in this Article apply to the ones responsible for the safekeeping or custody of restricted access material.

Section V
Reproduction

Article 33. The entire or partial reproduction of a document with classified information at any secrecy level will have the same secrecy level of the document.

Paragraph 1 – The total or partial reproduction of classified information at any secrecy level is conditioned to the permission of the classification authority or an authority with equal or higher prerogative.

Paragraph 2 – The copies shall be authenticated by the appropriate classification authority or by an authority with equal or higher prerogative.

Article 34. In the case of preparation, printing or reproduction of classified information at any secrecy level is made in typography, a printer, printing office or similar, this operation will be followed by an officially designated person responsible for ensuring the secrecy of the document.

Section VI
Preservation and Guard

Article 35. The evaluation and selection of documents containing declassified information, for permanent storage purposes or for disposal, shall follow the provisions of Law 8159 of January 8, 1991, and Decree 4073 of January 3, 2002.

Article 36. The permanent custody document that contains classified information at any secrecy level shall be forwarded, in the event of declassification, to the National Archives or the permanent archive of the public agency, entity or institution, for the purposes of organization, preservation and access.

Section 37. The document of permanent custody cannot be altered or destroyed, and these actions shall be subject to criminal, civil and administrative penalties, as required by law.

Section VII

Information Systems

Article 38. For the treatment of classified information, secure communication channels and information systems should be used that meet the minimum quality and safety standards set by the federal executive branch.

Paragraph 1 – The transmission of classified information at any secrecy level, through information systems, should be conducted within the corporate network and through a secure channel as a way to mitigate the risk of security breaches.

Paragraph 2 – The authenticity of the network user's identity must be guaranteed at least by the use of a digital certificate.

Paragraph 3 – The information systems mentioned in the caput shall have different levels of access control and use cryptographic features appropriate to the secrecy levels.

Paragraph 4 – The information systems mentioned the caput shall maintain control and registration of authorized and unauthorized access and of transactions carried out during a period equal or superior to the one of the information access restriction.

Article 39. The equipment and systems used to produce documents containing classified information at any secrecy level should be isolated or connected with secure communication channels that are physically or logically isolated from any other, and should have security and cryptographic features appropriate to their protection.

Article 40. The encryption and decryption of classified information at any secrecy level should use a State algorithm based cryptographic feature.

Sole paragraph. The Institutional Security Office of the Presidency is responsible for establishing parameters and standards for cryptographic capabilities based on State algorithms, after consultation with the Security Information Managing Committee, under Decree 3505 of June 13, 2000, Article 6.

Article 41. The procedures for the treatment of classified information at any secrecy level apply to cryptographic features, meeting the following requirements:

I – regular inspections, in order to ensure the execution cryptographic operations;

II – maintenance of complete and updated inventories of existing encryption material;

III - designation of cryptographic systems tailored to each recipient;

IV – communicating any abnormality related to the secrecy, sanctity, integrity, authenticity, legitimacy and availability of encrypted information to the superior or competent authority, and

V – identifying evidence of violation, interception or irregularities in the transmission or receipt of encrypted information.

Section VIII
Areas, Facilities and Materials

Article 42. Access to areas and facilities containing documents with classified information at any secrecy level, or which, for their use or purpose, demand protection, will be restricted to persons authorized by that agency or entity.

Article 43. The public agencies and authorities shall take measures for the definition, demarcation, signage, security and authorization for access to restricted areas under their responsibility.

Sole paragraph – Visits to restricted access facilities or areas shall be disciplined by the agency or entity responsible for their safety.

Article 44. Access to materials which demand protection, due to their use or purpose, shall be restricted to persons authorized by the agency or entity.

Article 45. Access shall be restricted to any material, product, system or substance containing, using or sharing knowledge or classified information at any secrecy level, economic information or scientific-technological information whose disclosure involve risk or harm to the interests of society and the State, such as:

I - equipment, machinery, models, molds, prototypes, artifacts, equipment, devices, instruments, cartographic representations, systems, supplies and instruction manuals;

II - ground, air and waterway vehicles, their parts and components;

III - weapons and their accessories, ammunition and equipment, supplies and related items;

IV – devices, equipment, supplies and programs related to information technology and communications, including the signals and imagery intelligence;

V - cryptographic resources; and

VI - explosives, liquids and gases.

Article 46. The public agencies or entities entrusted with the preparation of plans, studies and work to improve or design projects, tests, production, acquisition, storage or use of restricted access material shall provide additional instructions necessary to protect the issues related to them.

Article 47. The means used for restricted access material transportation is the responsibility of the custodian and shall respect the information’s secrecy level.

Paragraph 1 – The restricted material can be transported by contractors, taking measures necessary to maintain the secrecy of the information.

Paragraph 2 – The measures necessary for the safety of the transported material will be previously and explicitly stated in a contract.

Section IX
Conclusion of confidential contracts

Article 48. The conclusion of the contract, agreement, arrangement, adjustment, cooperation agreement or letter of intent whose object contains classified information at any secrecy level, or whose execution involves classified information, is subject to the signature of TCMS and to the establishment of contractual clauses providing for the following requirements:

I – the obligation to maintain secrecy concerning the object and its implementation;

II – the possibility to change the subject for inclusion or to change a security clause not stipulated in advance;

III – the obligation to adopt appropriate security procedures in the context of the activities under their control, to maintain secrecy concerning the object;

IV – the identification, for purposes of granting security credentials and the signature of the TCMS, of people who may have access to classified information at any secrecy level and to restricted access material;

V – the obligation to receive inspections for security clearance and its maintenance, and

VI – the responsibility for safety procedures relating to subcontracting, in whole or in part.

Article 49. Public agencies and entities that maintain relationships of any kind with contractors shall adopt procedures for the security of classified information at any secrecy level or restricted access material held by contractors or subcontractors.

CHAPTER IV
CLASSIFIED INFORMATION DOCUMENT INDEX

Article 50. Classified information at any secrecy level or a document that contains it shall receive a Classified Information Document Indexing Code– CIDIC.

Sole paragraph – The CIDIC will consist of elements that ensure the protection and temporary restriction of access to classified information, and will be structured in two parts.

Article 51. The first part of the CIDIC will consist on the Single Protocol Number – NUP, originally registered according to document management legislation.

Paragraph 1 – Classified information at any secrecy level or a document that contains that contains it, when declassified, shall keep only its NUP.

Paragraph 2 – No tables are used for classification of the document's matter or nature, due to demand for temporary access restriction to classified information at any secrecy level, under penalty of jeopardizing their protection and secrecy.

Article 52. The second part of the CIDIC will consist of the following elements:

I – secrecy level: the indication of the secrecy level, ultrasecret (U), Secret (S) or restricted (R), with initials in red, when possible;

II – categories: a two-digit warning of the category relating solely to the first level of the Controlled Vocabulary for Electronic Government (VCGE), according to Annex II;

III – the classified information production date: the record of the production date of classified information, according to the following composition: day (two digits) / month (two digits) / year (four digits);

IV – the date of declassification of classified information at any secrecy level: the potential record date for declassification of classified information, made in the act of classification in accordance with the following composition: day (two digits) / month (two digits) / year (four digits);

V – the indication of reclassification: the indication of the occurrence or not, Y (yes) or N (no), of reclassification of classified information, respectively, as in the following situations:

a) reclassification of information resulting from revaluation, or

b) the first record of the classification, and

VI – an indication of the date of extension for maintaining the classification: an indication solely for classified information at the ultrasecret level of secrecy, according to the following composition: day (two digits) / month (two digits) / year (four digits), in red when possible.

Article 53. For purposes of document management, the history of changes in the CIDIC shall be stored.

CHAPTER V
FINAL AND TRANSITIONAL PROVISIONS

Article 54. The implementation of the CIDIC shall be consolidated by June 1, 2013.

Sole paragraph. While the CIDIC is not implemented, the Information Classification Term shall be filled with the NUP.

Article 55. The document containing classified information at any secrecy level, produced before the enactment of Law 12527 of 2011, shall receive the CIDIC for purposes of the provisions in Decree 7724 of May 16, 2012, Article 45.

Article 56. The agencies and entities shall adopt the cryptographic resource based on State algorithms within one year from the definition of the parameters and standards mentioned in the sole paragraph of Article 40.

Sole paragraph. By the end of the period referred to on the caput, it is the Institutional Security Cabinet of the Presidency's responsibility to monitor and provide technical support to agencies and organizations on how to implement cryptographic resources based on State algorithms.

Article 57. The agencies and entities may issue supplementary instructions, within its powers, that will detail the procedures for security accreditation and treatment of classified information at any secrecy level.

Article 58. The Internal Rules of the Joint Information Revaluation Commission shall detail the necessary arrangements for the safeguarding of classified information at any secrecy level during its work and the ones of the Executive Secretariat, subject to the provisions of this Decree.

Article 59. This Decree shall enter into force on the date of its publication.

Article 60. The following are hereby revoked:

I – Decree 4553 of December 27, 2002, and

II – Decree 5301 of December 9, 2004.

Brasilia, November 14, 2012; the 191st year of the Independence of Brazil and the 124th year of the Declaration of the Republic.

DILMA ROUSSEFF

Márcia Pelegrini

Celso Luiz Nunes Amorim

Miriam Belchior

Marco Antonio Raupp

José Elito Carvalho Siqueira

Luís Inácio Lucena Adams

Jorge Hage Sobrinho

This does not replace the text published in the Official Gazette of November 16, 2012

ANNEX I

SECRECY MAINTENANCE COMMITMENT STATEMENT – TCMS

I, [Qualification: name, nationality, social security number, identity (the date and place of dispatch), affiliation and address], before the [agency or entity], declare being unequivocally aware of the legislation on the treatment of classified information whose disclosure may cause risk or harm to the security of the society or the nation, and I pledge to keep the necessary secrecy under Law 12527 of November 18, 2011, and:

a) to treat classified information at any secrecy level or restricted access materials that are provided to me by the [agency or entity] and to preserve its secrecy, in accordance with applicable law;

b) to preserve the content of the classified information at any secrecy level or restricted materials, without disclosing it to third parties;

c) not to take any actions that could affect the secrecy or integrity of classified information in any level of secrecy or restricted materials, and

d) not to copy or reproduce in any way or manner: (i) classified information in any secrecy level, (ii) information related to restricted access materials from (the) [agency or entity], unless authorized by the competent authority.

I declare that I [received] [had access] to (the) [document or material delivered or displayed to the signatory], and for being in accordance with this Agreement, I sign it in the presence of the undersigned witnesses.

[Place, date and signature]

[Two identified witnesses]

ANNEX II

DOCUMENT INDEX CODE

CONTAINING CLASSIFIED INFORMATION - CIDIC – CATEGORIES

CATEGORIES	NUMERICAL CODE
Agriculture, fishing and extractivism	01
Science, Information and Communication	02
Trade, Services and Tourism	03
Culture, Leisure and Sports	04
Defense and Security	05
Economy and Finance	06
Education	07
Government and Politics	08
Housing, and Urban Sanitation	09
Industry	10
Justice and Law	11
Environment	12
The individual, family and society	13
Foreign Affairs	14
Health	15
Labor	16
Transportation and traffic	17

Note:

1. Categories: they represent the aspects or issues related to information classified on any secrecy level, and shall be indicated by the Classification Authority. Thus, the first level of the Controlled Vocabulary for Electronic Government (VCGE) shall be used exclusively, defined by the Electronic Government Interoperability Standard (e-Ping), as shown above.

2. Composition in the CIDIC: 2 digits = numeric code