OFFICIAL DIARY OF THE UNION

Published: 12/27/2021 | Edition: 243 | Section: 1 | Page: 1

Body: Presidency of the Republic/Institutional Security Cabinet

NORMATIVE INSTRUCTION No 6, OF DECEMBER 23, 2021

Establishes information security guidelines for the safe use of social media in federal public administration bodies and entities.

THE STATE MINISTRY HEAD OF INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF THE REPUBLIC, in the use of the powers conferred on him by art. 87, single paragraph, items I and II, of the Constitution, and in view of the provisions of art. 12 of Decree No. 9,637, of December 26, 2018, resolves:

Art. 1 To establish information security guidelines for the safe use of social media in the bodies and entities of the federal public administration, with regard to institutional profiles.

CHAPTER I

PRELIMINARY PROVISIONS

Art. 2 For the purposes of this Normative Instruction, the concepts contained in the Glossary of Information Security, approved and updated by decree of the Institutional Security Cabinet of the Presidency of the Republic, will be considered.

Art. 3 The institutional profiles maintained on social media must be administered and managed by teams composed of military personnel, permanent civil servants or public employees.

Single paragraph. When it is not possible to follow the provisions of the **caput**, the team may be mixed, with the participation of outsourced or unrelated civil servants, provided that it is under the coordination and responsibility of a military, permanent civil servant or public employee.

CHAPTER II

OF THE SKILLS

Art. 4 It is incumbent upon the administration and management team of institutional profiles in social media:

I - to create, change, delete and control institutional profiles on social media of the body or entity;

II - to remove, as soon as it becomes aware, posts that violate information security; and

III - to prepare a monthly report on the use of social media under its administration and present it to the information security manager of the body or entity.

Single paragraph. The monthly report referred to in item III of the **caput** must contain, at least:

I - the total of created and deleted accounts;

II - the total number of registered followers; and

III - the number of posts made and removed.

Art. 5 It is incumbent upon the agent responsible for the safe use of social media:

I - to continuously manage, monitor and analyze the practices of safe use of social media, with respect to information security aspects;

II - to check if the normative act on the safe use of social media is being followed properly by the body or entity and if there is a need for revision;

III - to implement the culture of safe use of social media and carry out the information security actions appropriate in this context in their respective body or entity; and

IV - to prepare a report containing a description of the security incidents that occurred in institutional profiles on social media and the corrective measures adopted, as well as forward it to the information security manager for information.

Art. 6 It is incumbent upon the information security manager:

I - to propose actions for continuous improvement in the management of the safe use of social media;

II - to promote the strengthening of the information security culture in its respective body or entity, with regard to the safe use of social media;

III - to designate the agent responsible for the safe use of social media;

IV - to establish and coordinate the team responsible for preparing and revising the normative act on the safe use of social media;

V - to present the report on the use of social media referred to in item III of art. 4th; and

VI - to forward for approval by senior management the draft and review drafts of the normative act on the safe use of social media.

Art. 7 It is incumbent upon the Information Security Committee or equivalent structure:

I - to analyze the information security risks arising from the presence of the body or entity on social media;

II - to promote actions to address information security risks arising from the presence of the body or entity on social media;

III - to analyze, conclusively, the draft and review drafts of the normative act on the safe use of social media;

IV - to analyze the reports referred to in item III of art. 4 and item IV of art. 5th; and

V - to advise on the implementation of information security actions for the safe use of social media.

Art. 8 It is incumbent upon the top management of the body or entity:

I - to approve the draft and revisions of the normative act on the safe use of social media;

II - to designate the administrators of institutional profiles on social media; and

III - to promote participation in training and professionalization actions of human resources, on topics related to the safe use of social media.

CHAPTER III

OF THE NORMATIVE ACT ON THE SAFE USE OF SOCIAL MEDIA

Art. 9 The bodies and entities of the federal public administration shall issue a normative act on the safe use of social media, approved by the senior management.

Single paragraph. The act referred to in the **caput** shall:

I - comply with the legal information security requirements in force and be aligned, as appropriate, with the Information Security Policy, with the

internal information security management processes, with the strategic objectives and competences of the body or entity; and

II - establish guidelines, criteria, limitations and responsibilities for managing the safe use of social media by users who have permission to manage institutional profiles or who have credentials to access any institutional social media.

Art. 10. A team should be created to prepare and revise the normative act on the safe use of social media, comprising at least:

I - an agent responsible for the safe use of social media;

II - a responsible one for the administration and management of institutional profiles on social media;

III - representative(s) of the communication area of the body or entity; and

IV - server(s) from areas interested or involved with institutional profiles on social media, if applicable.

Art. 11. The normative act on the safe use of social media must define the following criteria, at least:

I - regarding information security management in the safe use of social media, in addition to the competencies provided for in Chapter II:

a) the responsibility for authorizing and vetoing the creation of new institutional accounts on social media, considering aspects of convenience, opportunity and information security;

b) the responsibility for the decision and procedures related to the closure of institutional accounts on social media;

c) the responsibility for procedures for managing any institutional crisis resulting from the use of social media;

d) the responsibility for designating the area or agent responsible for authorizing military, civil servant or public employee to carry out or authorize posting on behalf of the institution; and

e) the responsibility of the military, civil servant or public employee when carrying out or authorizing posts according to the institutional profile assigned;

II - regarding the information security procedures necessary for the creation of institutional accounts on social media:

a) the objectives to be achieved with the use of the account by the body and entity;

b) the existence of content verification procedures before and after posting;

c) the existence of visual elements that undoubtedly identify the body and the entity, following the normalized standards;

d) the existence of information security and privacy policies and procedures by the company that owns or manages the social media application; and

e) the definition of the procedures that must be adopted in order to prevent and correct cases of posts that could damage the image of authorities or of bodies and entities of the federal public administration, including the use of the message moderation feature;

III - regarding the information security requirements necessary for the maintenance of institutional accounts on social media:

a) verification of compliance with the provisions of the Information Security Policy of the body or entity;

b) the adoption of post content verification processes, in accordance with the standard for the safe use of social media;

c) the joint decision of the responsible agent and the administrator and manager of institutional profiles on social media on the need to create an institutional account on social media; and

d) the existence and correct use of the minimum visual elements of standardization and identity of the body or entity, in accordance with standardized standards; and

IV - regarding the general requirements:

a) posts that violate information security;

b) the rules of compliance with privacy laws, specifying:

1. how should the interaction with external users be; and

2. the requirements to be observed to, if necessary, move this interaction to a private channel or direct it to another level of treatment;

c) the rules of compliance with confidentiality guidelines, specifying:

1. the type of information that may be disclosed; and

2. information that should not be disclosed, as it is classified or with restricted access;

d) actions for cases of violation of the normative act on the safe use of social media; and

e) procedures for managing institutional crises related to information security resulting from the use of social media.

Single paragraph. Social media moderation is understood to mean the management and review of user-generated content and the administration of their activities on online social platforms.

Art. 12. The normative act on the safe use of social media will establish the periodicity for its review or the rules derived from it, which shall not exceed two years.

Art. 13. The normative act and its updates must be disclosed to all civil servants, public employees, military personnel and service providers of the body or entity.

CHAPTER IV

OF THE INFORMATION SECURITY GUIDELINES FOR INSTITUTIONAL USE OF SOCIAL MEDIA

Art. 14. Only duly authorized civil servants, public and military employees may carry out or authorize posts on social media in the name of the body or entity.

Art. 15. Classified information or restricted access cannot be published on social media.

§ 1º Changes in the classification of posted subjects must be informed to the administrator of institutional profiles on social media, so that the necessary measures are taken to ensure compliance with the provisions of the **caput**.

§ 2 It is at the discretion of the body or entity to define the deadlines for permanence of posts, considering the risk of information security due to posts with outdated information.

§ 3 The publication of personal data on social media must comply with the provisions of Law No. 13.709, of August 14, 2018 (General Law for the Protection of Personal Data), and related rules.

Art. 16. Civil servants, public employees, military personnel and service providers may not provide content considered inappropriate on social

media, and the offender is subject to the sanctions provided for in the legislation.

§ 1 It is considered inappropriate content, among others, material that is:

I - offensive;

II - obscene;

III - pornographic;

IV - sexually suggestive;

V - abusive;

VI - discriminatory;

VII - defamatory;

VIII - threatening;

IX - of hate;

X - a violation to Law No. 7716, of January 5, 1989;

XI - a violation to intellectual property laws; and

XII - a violation to privacy laws.

§ 2 When receiving any material as described in § 1, through an institutional profile on social media, including access links to the material, the server, public employee, military or service provider must communicate the fact to the profile manager institutions in social media, so that measures are taken with the agent responsible for the safe use of social media.

Art. 17. The use of institutional accounts on social media to make professional recommendations or those aimed at promoting products or companies not authorized by the body or entity is prohibited.

Art. 18. The bodies and entities of the federal public administration may define other procedures that they deem necessary for the safe and proper use of social media by their servers and service providers.

Single paragraph. Alternatives should be sought that allow tracking of those responsible for publishing content in institutional accounts, avoiding, when possible, the use of shared accounts for accessing social media.

CHAPTER V

FINAL PROVISIONS

Art. 19. Ordinance No. 38, of June 11, 2012, of the Executive Secretariat of the National Defense Council is hereby revoked.

Art. 20. This Normative Instruction enters into force on January 3, 2022.

AUGUSTO HELENO RIBEIRO PEREIRA