


PASSWORD POLICY

AMCEL - AMAPÁ FLORESTAL E CELULOSE S.A.

**JUNE
2021**

	POLÍTICA DE SENHA	
	Revisão:	Norma:
Classificação da publicidade: INTERNA	Tipo de documento: POLÍTICA	Data de vigência: [xx]

1. OBJECTIVE

Based on this Password Policy (“Policy”), **AMCEL – Amapá Florestal e Celulose S.A. (“AMCEL”)** proposes criteria for the preparation, change and maintenance of passwords for all its employees and users of the systems used by **AMCEL**.


This Policy must be read and interpreted in accordance with the guidelines of the Information Security Policy, which sets out the general guidelines on the use of credentials and passwords at **AMCEL**.

In this way, it is possible to establish an efficient, disciplined practice that makes users aware that passwords are one of the main authentication mechanisms used today, being absolutely personal and non-transferable, and that it is the passwords that allow the recognition of each user in the systems used by AMCEL, as well as identify which data is accessed.

2. SCOPE/VALIDITY

This Policy applies to all users of information and communication technology resources, including employees, service providers or third parties who are in the service of **AMCEL** and enters into force from the date of its issuance, for an indefinite period. This Policy will be updated whenever necessary, due to changes in situations observed in the practice of **AMCEL** processes or depending on other rules, regulations and laws.


3. GENERAL GUIDELINES

	POLÍTICA DE SENHA	
	Revisão:	Norma:
Classificação da publicidade: INTERNA	Tipo de documento: POLÍTICA	Data de vigência: [xx]

Employees must be aware that the care with the information and confidentiality of their user and their password for accessing the internal network and AMCEL systems is their full and exclusive responsibility.

Thus, the following guidelines must be observed:

- a.** The sharing, disclosure and/or lending in any way of the individual and non-transferable password of each user is expressly prohibited, and the person responsible for the Information Technology Sector and the DPO must be informed immediately if there is any suspicion of non-compliance with the guideline;
- b.** The initial password will be developed by the Information Technology Sector upon admission of the employee, and must be provided to the employee himself personally without showing or informing third parties and must be changed and/or forced to change the password in the first authentication process performed;
- c.** It is expressly forbidden to write down passwords in easily accessible places, especially those near the employee's workstations (e.g. notes on the computer monitor, under the keyboard or even notes on the computer screen);
- d.** When creating a password, the following must be observed: the minimum length of 7 and maximum 14 characters, the use of lowercase and uppercase letters/characters, special characters and numbers; the use of public and personal information is prohibited (eg, date of birth or name of spouse);
- e.** It is prohibited for passwords to be visible on the screen when they are typed and used;
- f.** In case of suspicion of improper use of their profile and/or password, the users must notify the DPO immediately, via e-mail eduardo.marques@amcel.com.br;
- g.** Password reuses will not be allowed.
- h.** In case the employee forgets or wishes to change the password, he/she should contact IT.

	POLÍTICA DE SENHA	
	Revisão:	Norma:
Classificação da publicidade: INTERNA	Tipo de documento: POLÍTICA	Data de vigência: [xx]

3.1. Frequent password change. The user must change his password every 60 (sixty) days. After this period, it will not be possible for the user to access the system without changing his/her access password, and must contact the Information Technology department through the support channels for regularization.

3.2. User and password cancellation. The mandatory cancellation of user access by the Information Technology Sector will occur in the situations listed below:

- Employee Dismissal;
- Change of employee role/position;
- When, for any reason, there is no longer a need for user access to the system or information.


4. VIOLATIONS AND SANCTIONS

It should be noted that any and all violations of this Policy will be analyzed as Information Security incidents and treated as provided for in the incident management process, supervised by the person in charge of the Information Technology Sector, by the Data Protection Officer, by the Humans Resources Sector and the **AMCEL** Board of Directors.

5. REVIEW

Histórico da última revisão da Norma:

Elaborado por:	Verificado por:
-----------------------	------------------------

	POLÍTICA DE SENHA	
	Revisão:	Norma:
Classificação da publicidade: INTERNA	Tipo de documento: POLÍTICA	Data de vigência: [xx]

Aprovado por:	

6. DOCUMENT LOCATION

This document can be consulted digitally or physically at the Information Technology area and internal means of communication.