AMCEL

ACCESS MANAGEMENT STANDARD

JULY

2021

1. OBJECTIVE

Through this Access Management Policy ("Policy"), **AMCEL - AMAPA FLORESTAL E CELULOSE S.A.**, will establish the necessary security criteria for the control of access to information and data stored in systems, applications or other information assets belonging to the **AMCEL**'s technological infrastructure.

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 begins its validity from the date of its issuance, for an indefinite period.

3. ACCESS CONCEPT

Access is understood as any and all form of interaction with the information made available and the data contained therein, including everything from simple viewing or consultation to extracting copies, changing, deleting etc., accessing this, to data, information and files contained in any medium, whether physical or digital. The concept of access is subdivided into three:

- **Public Access**: All access allowed, without restrictions, to passwords, bookmarks, etc.;
- **Restricted Access**: All authorized access to indicated Users. Unauthorized access can cause serious damage to the business and/or compromise the Company's business strategy;
- **Confidential Access**: It is the restricted access for a specific group of people, being able to be composed by employees, customers and/or suppliers. Unauthorized access can cause several impacts to **AMCEL**, such as financial, image and the like. Failure to comply will result in administrative, civil and criminal sanctions.

4. GUIDING PRINCIPLE

The control of access to information will be guided by the Principle of Necessity (art. 6, III, of the General Data Protection Law - LGPD), which determines that access to personal data and information of third-party holders can and should only occur when there is a verification of the effective need to obtain access to that information, system or application for their work function.

5. RESPONSIBILITY

Failure to comply with the rules established in this Policy, whether isolated or cumulatively, may give rise to, according to the offense committed, the following measures to the employee:

(A) NOTICE OF NON-COMPLIANCE:

- It will be forwarded to the employee, communicated informing the non-compliance with the standard, with the precise indication of the violation practiced.

(B) CONTRACT TERMINATION:

- In cases of serious faults and/or reiteration of the practice, after effective communication to the employee, the contract with the employee may be terminated, as well as the adoption of the applicable legal measures.

6. CRITERIA FOR GRANTING ACCESS AND LIMITING PERMISSION

The granting of access will be defined both according to the need for access to data and information, as well as the analysis of the function performed by the employee. Access permission will be granted upon request by the area manager, and such access may even be determined for a limited period of time.

The granting of access and temporary permission may occur in cases where it is necessary to have access to information that did not exist before, for lack of need or for not needing to use it. In this way, the access permission will be in effect for as long as it is necessary to carry out specific activities that are not within the scope of the employee's work and which will also not be necessary to continue with access in the near future.

There is no time limit for this access, it can be either a few hours or days or weeks, as long as it is always in the light of the need.

7. GENERAL GUIDELINES

- Only previously identified and authorized end users may have access to **AMCEL**'s information assets;
- All access to systems, applications or other information assets, users must enter their ID and password, so that they can be identified (identification) and verify (authentication) the user's identity unambiguously, the password being individual and non-transferable;
- To define the criteria to be used in access control, the following should be considered:
    - The nature of the user (ie, internal and external, visitor, consultant, etc.);
    - Existing roles in the company (eg director, manager, supervisors, coordinators, assistants, intern, apprentices).

- The access criteria must be specific for each application, according to the privilege definitions defined by the information owners;
- The only way for users to access information assets stored in production environments should be through applications;
- Applications will control user access through mechanisms to ensure that users do not have access with distinct privileges to others other than those authorized by the owner of the information;
- One session must be defined as a limit (01) for the same application and data source by the end users;
- Anonymous access to any resource within the technology platform available at **AMCEL** must not be allowed;
- The previous application opening screens, the credential prompt screens, including the latter should show minimal information about the application it is intended to enter (ie

not display information about the operating system). Passwords must not be displayed in the sign-in procedure;

- Identifiers are automatically blocked after five failed attempts. Automatic locks can be more restrictive if applications guarantee them based on the importance of the information assets they manage;
- In the case of multi-user systems where the authentication procedure is successful, the following must appear immediately after access:

  " Notice:

  *These resources are exclusively for the use of authorized staff or employees of **AMCEL**, its subsidiaries and affiliates. Unauthorized use is prohibited and subject to sanctions. All individuals using this computer system are subject to their activities being monitored and recorded by the systems staff."*

- In the case of systems or applications that do not allow the above message to be presented immediately after a successful authentication procedure, the systems must respect before trying to access the text network:

  " Attention:

  *To access this system, you will need prior authorization, which is strictly limited to the use specified in the authorization. Unauthorized access or misuse is strictly prohibited and constitutes a violation of **AMCEL**'s information security. The usage of this system can be monitored. "*

- All connection attempts (success or failure) must generate a record.

8. ASSIGNMENT TO SPECIFIC SECTORS

8.1 Assignments of the Information Technology Department

The Information Technology (IT) Department will be responsible for creating and updating accesses, separated by function – title and access need. This matrix will contain the definition of each access profile, justifications, directories and systems accessed by each profile, persons responsible and other details necessary for access management. In addition, the Information Technology sector will have a horizontal dialogue with both the Internal Managers and the Personnel Department to ensure that access information is always up to date.

The sector will also be responsible for granting, changing and canceling user access to directories and systems after receiving the request, verifying information to carry out the permissions adjustments when it is verified that the access is excessive and does not meet the user's need - how can occur, for example, when there is an internal change of position/role and access has become unnecessary, as described in the general guidelines.

8.2 Assignments of Internal Sector Managers

It will be up to each Manager of the Internal Sectors to provide support to the Information Technology Department during the definition of the necessary accesses for the employees of their department, ensuring that each user accesses only the information they need to perform their function.

In addition, Managers must request the Information Technology Department, upon prior justification and for a specified period, to release privileged access to users of their department, in specific cases and which it deems necessary to release such access.

8.3 Assignments to the Personnel Department

It will be up to the Personnel Department to notify the Information Technology Department about the need to grant, change or cancel user access, in addition to informing, immediately, the change of position or the dismissal of employees, as a measure to control in a manner effective access to information systems.

8.4 Assignment to Users

The user will have the necessary access to perform their work functions, and must inform the Information Technology Department if there is the possibility of accessing surplus directories or other functions.

In addition, to enhance the secrecy and security of information assets, Information Access Control also has a directive that Users do not record, record or share logins, passwords, ID's, tokens, etc. In case of suspicion of use of your User by third parties, the User must immediately inform the Information Technology (IT) Department so that the necessary measures can be taken.

9. REVISION

History of the last revision of the Standard:

Prepared by:	Verified by:	
Approved by:		

10. DOCUMENT LOCATION

It is possible to consult this Standard in your copy physically with the Information Technology area.