INCIDENT MANAGEMENT STANDARD

AMCEL - AMAPÁ FLORESTAL E CELULOSE S.A.

June | 2021

SUMMARY

1. INTRODUCTION

Through its internal governance and management that encompasses Privacy and Data Protection, **AMCEL - AMAPA FLORESTAL E CELULOSE SA** establishes, through this Standard, the procedures related to the management of Information Security as a response to effectively expanding the values of commitment and security to the protection and processing of data to which anyone has access, directly or indirectly.

2. OBJECTIVE

2.1 This Standard has the specific purpose of establishing the roles, responsibilities and measures to be adopted and to ensure a consistent and effective focus on the management of Security Incidents involving Personal Data ("Incident"), including internal communication, functions of each team, the recognition of the weaknesses and events that can cause damage to **AMCEL**.

2.2 by this Standard, the purpose of recording and reporting incidents and risks is ensured, in order to ensure, by taking a timely decision, minimize any impacts to **AMCEL**'s business, or risks and damages to data subjects, whether customers and partners, mainly, but not restricted to those related to Sensitive Data, (referring to health or sex life, genetic or biometric data) and any data that, when treated in combination with other information, may allow inferring information of this nature.

3. APPLICATION AND SCOPE

3.1. Initially, it is verified that this Standard is applied to any case of Security Incident involving Personal Data, being broadly in line with other **AMCEL** policies and management, in force since its presentation to the community.

3.2. Therefore, this scope includes all partners, directors, administrators, employees and other members of **AMCEL** or who have relationships and may have access to areas where **AMCEL** information, equipment, files, networks, documents or other related data are found.

4. RESPONSIBLE

4.1. The review of this Standard will be the responsibility of the Internal Privacy and Data Protection Committee and shall take place annually or less frequently, when necessary.

5. DOCUMENT LOCATION

5.1. This document can be consulted digitally in the directory or physically with the Information Technology Department.

6. TERMS AND DEFINITIONS RELATING TO THE INFORMATION SECURITY INCIDENT

6.1. Initially, it should be noted that an Information Security Incident involving Personal Data is any and any breach of security that, accidentally or intentionally, gives rise or is capable of giving rise to destruction, loss, alteration, disclosure or non-use or non-access authorized to Personal Data processed by **AMCEL**.

6.2 These incidents can be configured in different ways, it is explained:

Personal Data Leakage	It is configured as the Incident in which Personal Data is *improperly* exposed and made available by physical or digital means to an indeterminate number of people, in Brazil or in any country.
Denial of Service **Unauthorized access**	It is configured as the Incident in which access (*logical or physical*) to a *system that stores Personal Data is impaired or made impossible*, so that the integrity of Personal Data (existence and/or veracity) may be permanently compromised, given the unavailability of access. It is configured as the Incident in which access (logical or physical) to a system that has Personal Data is attempted or obtained, without having proper authorization for such access. Therefore, unauthorized access is one whose permission to connect, read, write, authenticate, modify, delete or create has not been granted.
inappropriate use	It is configured as the Incident in which there is a violation of the Company's data, information and systems use policies, including the Information Security Policy, and other internal management used to ensure Privacy and Data Protection.

6.2. It is through this Incident management that the "reliability" management is implemented, consisting of three basic aspects, namely:

Reliability	Ensure that the information, when necessary, is accessible only to authorized employees and/or processes, and is properly protected from the knowledge of others.
Integrity	Ensure that the information is correct, true and not tampered with, mirroring reality.
Availability	Participate in training and awareness programs for Incident mitigation.

6.3. Thus, it should be noted that an Incident is not only characterized by information leakage, the invasion of crakers or the infection of the system by malicious files, but it is provided for in the previously established tables, it may be an inappropriate use, for example. Check the difference between incidents and risks:

Incidents	Riscos
Thus, all events that compromise aspects of information reliability will be considered incidents. Therefore, the ideal is that the incident is avoided when it is still only a risk, thus, it is not necessary for an incident to materialize for corrective actions to be taken.	We can classify the ***risk as the probability of a threat*** (eg a malicious file, a malicious user, a phishing, an electrical discharge, a storm, etc.), or acts aimed at taking advantage of a vulnerability, (ex. an outdated antivirus, files without access control, unprepared employees, a server located in a location susceptible to flooding or no UPS, etc.) and compromising some of the aspects of information reliability through an incident.

6.4. Therefore, information security risks and incidents must be communicated and dealt with in accordance with the guidelines established in this standard, find out how, through the roles and responsibilities, designated below:

7. ROLES AND RESPONSIBILITIES

7.1. Each of **AMCEL**'s areas, whether the areas directly involved in governance or not, have responsibilities when an Incident occurs or is merely suspected, as described below:

7.2. Obligation of all areas:

- It is up to everyone to ensure immediate communication about the occurrence or mere suspicion of an Incident, or a Risk.

- It will be up to everyone to strictly comply with the Policies and management in force that may contribute to **AMCEL**'s information security and incident management, contributing to the mitigation of risks; and

- It will be up to everyone to actively participate in training and awareness programs for Incident mitigation

7.3. It will be up to the Information Technology Department:

7.3.1. Develop security tests, perform preventive and reactive assessments, produce reports on indicators related to the security of **AMCEL**'s computer network;

7.3.2. Implement and receive from the Data Protection Committee suggestions for technical measures aimed at monitoring the results in the Quarterly Incident Report;

7.3.3. Map, treat, diagnose and monitor files, malicious programs (such as malware), or possible actions by users with the potential to generate incidents and risks to the company's system;

7.3.4. Receive, register, classify and monitor, together with the competent Manager or User, the risk or incident communications, aiming to implement necessary measures for neutralization, systems restoration, asset recovery, in order to ensure that the risk and incidents happen;

7.3.5. Inform the Supervisor of all risks relating to personal data;

7.3.6. To jointly produce an Incident Handling Report, which will contain all the details of the event, such as assessment, possible reasons, evidence, classification as to criticality, compromised assets, extent of damage and other details useful for handling and recording the incident;

7.3.7. Extract the didactic content of incidents that occurred in the company, using the document in training in order to prepare materials to make Users aware of how to prevent and react to incidents that harm Information Security;

7.3.8. Create and manage a channel to receive communications of risks or incidents associated with information security and data protection, widely disclosing its existence and form of use to Users;

7.3.9. Create and disseminate a form designed to instruct the process of communication of risks and incidents by Users;

7.3.10. Carry out internal audits to identify the causes of incidents, implementing corrective actions;

7.3.11. Inform the communicators of risks or incidents about the result of the treatment.

7.4. <u>It will be up to the Person in Charge</u>:

7.4.1. Support the Information Technology Department in the performance of its duties;

7.4.2. Offer guidance to other employees, third parties, suppliers and customers of **AMCEL**, regarding the prevention of incidents;

7.4.3. Communicate in the meetings of the Data Privacy Committee any occurrence of non-compliance with the Information Security Policies by employees, in order to demand the application of disciplinary measures.

7.4.4. Communicate the **National Data Protection Authority - ANPD** and the holder about the occurrence of security incidents that may lead to relevant risks or damages to the holders. The release must contain at least:

- A description of the nature of the personal data affected;
- Information about the holders involved;
- The indication of the technical and security measures used for data protection, observing commercial and industrial secrets;
- The risks related to the incident;
- The reasons for the delay, in case the communication was not immediate; (should always respect the deadline of 02 (two) days for its report, and;
- The measures that have been or will be taken to reverse or mitigate the effects of the damage.

7.4.5. Receive and respond to communications from the **National Data Protection Authority - ANPD** regarding incidents, developing, when applicable, together with the Committee, plans to publicize the incident and measures to reverse or mitigate its effects.

7.5. <u>It will be up to the Department Managers:</u>

7.5.1. Manage the monitoring, communication and treatment of risks and incidents that affect your area;

7.5.2. Supervise employees, third parties and suppliers related to its department in relation to compliance with security rules, aimed at preventing risks and incidents, providing guidance and applying sanctions, when non-compliance with this and other security policies is detected.

7.5.3. Communicate to the DPO and the Data Privacy Committee any occurrence or suspicion of data breach that does not comply with the information security policies within the company.

7.6. <u>It will be up to the Users</u>:

7.6.1. Observe and comply with all security measures provided for in **AMCEL**'s Policies and Standards regarding Information Security and Personal Data Protection;

7.6.2. Immediately report to the Information Technology Department and the Data Protection Officer possible and any indications of risk or incident that affect **AMCEL**'s information security and personal data protection;

7.6.3. Register via documents and communicate to the Information Technology Department and the Data Protection Officer about vulnerable security points with the potential to cause incidents, as well as suggest substantiated improvements.

8. GENERAL RULES FOR HANDLING INCIDENTS

8.1 The handling of **AMCEL** threats and incidents will occur according to the following schedule:

a) Communication: Once the Information Security Risk or Incident has been identified, the reporting person (the first person who notices it), must, within a maximum period of 24 (twenty-four hours), report immediately to the Information Technology Department through of the Priv. and Data Protection on the AMCEL website or via email eduardo.marques@amcel.com.br

It is preferable that this communication contains:

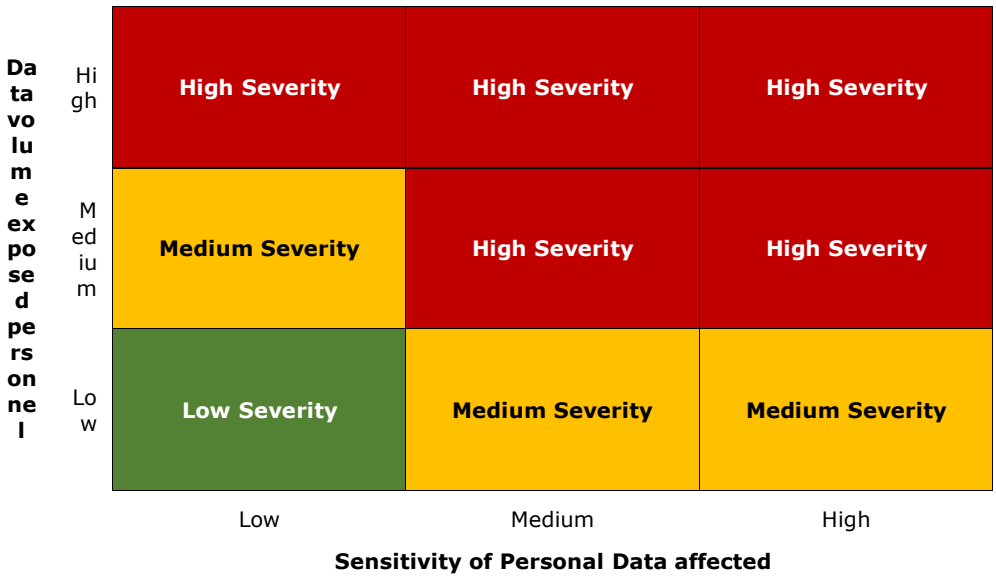
- The date and time the suspected Incident or Risk was discovered;
- The types of information involved;
- The causes of the possible Incident, Risk or an Actual Incident;
- The context in which it occurred;
- Additional information to facilitate understanding of the event, its causes and consequences.

ATTENTION: COMMUNICATION ABOUT RISKS OR EVEN SUSPECTED INCIDENT INFORMATION IS EXTREMELY NECESSARY. THUS, IF THE COMMUNICATOR CONSTATE SUSPECTS AND DOES NOT COMMUNICATE IT, DISCIPLINARY SANCTIONS MAY OCCUR. NOTIFY US!

b) **Analysis:** After the communication, the immediate risk or incident analysis by the Information Technology Department will follow, which shall:

(i) File the communication if you identify that it is not a risk or incident related to information security;

(ii) Produce the Incident Handling Report, classifying it according to its criticality level, pursuant to the tables below.



CORRECT MANAGEMENT: OBSERVE: THE VOLUME OF PERSONAL DATA EXPOSED AND THE SENSITIVITY OF THIS DATA, with support from the tables below:

criticality	Description
Level 01: Very High	Compromise of critical directories or systems, paralyzing one or more departments; compromise of confidentiality, integrity and/or availability of strategic information and personal data.
Level 02: High	Risk or incident of compromised directories or systems, with the possibility that the affected users will continue to perform their role, but without the guarantee of the same quality; high probability of

	compromising Confidentiality, Integrity and/or Availability of strategic information and personal data.
Level 03: Medium	Users are able, with some effort, to perform the tasks by the incident with the same quality. The probability of compromising the confidentiality, integrity and/or availability of strategic information and personal data is low.
Level 04: Low	The risk or incident does not generate any impact on directories or systems, nor does it compromise the confidentiality, integrity and/or availability of strategic information and personal data. However, if the risk or incident is not addressed, its criticality may be aggravated.

VOLUME OF EXPOSED PERSONAL DATA			**SENSITIVITY OF AFFECTED PERSONAL DATA**	
Criticality	**Description**		**Criticality**	**Description**
High	volume of Personal Data affected exceeding 10% of the database controlled by the Company		High	Personal Data of children or teenagers, Personal Data Sensitive data or that may generate discrimination to the holder; bank, payment or credit protection details
Medium	volume of Personal Data affected below 10% and above 2% of the database controlled by the Company		Medium	Immediately identifiable Personal Data (eg name, email, CPF), combined or not with behavioral information (e.g. activity history, preferences, etc.)
Low	volume of Personal Data affected less than 2% of the database controlled by the Company		Low	Anonymized Data, Pseudo-Personal Data (provided the deanonymization key has not also been compromised), Personal Data that is difficult to identify (eg IP address)

c) **Escalation:** Once the risk or incident is classified, if it involves personal data, the Information Technology Department will request support by email from the Person in Charge and/or the manager and users of the affected area, whose support it deems necessary.

- Depending on the criticality, complexity, extent of damage and affected assets (as analyzed by the aforementioned tables), the Information Technology Department will be involved in the treatment by the Privacy and Data Protection Committee.

d) **Treatment:** After the escalation, the Information Technology Department with the support of the Supervisor and other managers and Users, respecting the order of priority according to the criticality classification:

- Alimentará o Relatório de Tratamento de Incidente, documentando o impacto e quais ativos e departamento foram ou serão afetados;
- Implementará ações necessárias para estancar os danos gerados pelo incidente, isolando ambientes, diretórios e sistemas comprometidos;
- Identificará possíveis eventos que podem ter gerado o incidente, coletando e documentando evidências;
- Avaliará possíveis soluções com base em seu conhecimento, normas técnicas, apoio de demais áreas ou empresas terceirizadas, aplicando as ações necessárias para neutralização do incidente, restabelecimento de sistemas, recuperação de ativos, garantindo que o risco de recorrência foi eliminado ou mitigado, se não for possível sua eliminação;
- When so defined by the Strategic Committee for Information Security and Data Protection, the Supervisor will communicate to the affected holders and the **National Data Protection Authority - ANPD** about the occurrence of incidents involving personal data, following the determinations of the Committee and within a period no longer than to 02 (two) business days and following the guidelines and models provided by ANPD;
- It will make sure that there are no other incidents or related risks, opening additional calls if applicable;
- Once the treatment is finished, the case will be returned to the Management Committee for validation.

e) **Validation:** Once the treatment is completed, the Information Technology Department will report through the Incident Treatment Report to the Internal Committee, which will validate whether the treatment applied was sufficient for the complete resolution of the incident; whether there is a need to collect other data and evidence for teaching and auditing purposes;

f) **Closing:** Once the treatment has been validated, the Information Technology Department will close the call, entering all necessary data in the Incident Handling Report and informing the caller about the result of the treatment.

9. DIDACTIC ASPECT

9.1 In order to reduce risks and strengthen the Information Security Management System, the Committee:

a) It must produce a quarterly report with information related to Information Security incidents, which will contain a summary of the Incident Handling Reports for the period, indicators on incidents, analysis of the effectiveness of treatments, recommendations for neutralizing or reducing threats, risks and incidents. The report will be presented to the Committee for debate and planning of measures;

b) The quarterly report will guide the formulation of an inventory for monitoring and evaluating the risks, which should be discussed with the Committee;

c) Produce and update teaching materials, carry out training and events aimed at Information Security, based on information extracted from treatments, safeguarding the anonymity and confidentiality of information.

10. HISTORICAL SUMMARY OF REVIEWS AND VERSION CONTROLS

Elaboration date	Current revision date	Maker/Approver	Version
08.06.2021			01/2021

ANNEX I - DOCUMENT APPROVAL

Approver	Area	Signature	Date

ANNEX II - REVIEWS

Version / Revision	**Date**	**Revisor**	**Changed Items** (add brief description of change)
1.0			
1.1			
1.2			
1.3			
1.4			
1.5			
1.6			
1.7			