


RISK ASSESSMENT STANDARD

AMCEL - AMAPA FLORESTAL E CELULOSE S.A.

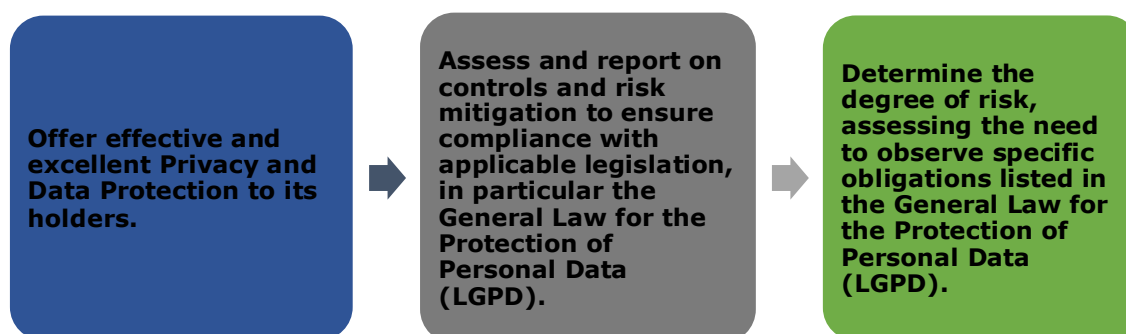
**JUNE
2021**

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

1. OBJECTIVE

This Risk Assessment Standard ("Standard") aims to define the assessment of the level of risk, in order to manage and protect Personal Data from unauthorized access, as well as from accidental, illicit and consequently undesirable situations of destruction, loss, alteration, communication or dissemination of these information assets, which may contain personal data of third parties, sensitive data and confidential information that are the effective responsibility of **AMAPA FLORESTAL E CELULOSE SA ("AMCEL")**.

The Risk Assessment must be carried out for the following reasons:




This Standard must be read and interpreted in accordance with the other Governance Policies on Privacy and Data Protection developed by **AMCEL**, with all the attributions and guidelines defined herein being approved by the Senior Management and mandatory for all involved.


This Standard applies to all **AMCEL** units, and the people involved in it, namely, its employees, service providers, third parties, partners and suppliers in any and all operations involving the processing of Personal Data.

2. DEFINITIONS

For the purposes of this Standard, the following definitions and terms are considered:

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

- **Risk**: Can be understood as the possibility of both situations and events that may occur that affect the achievement of business objectives. All activities may suffer some kind of risk to any activity and may affect assets, results, image, reputation, legal, regulatory aspects, identity, confidentiality or business continuity;
- **Event**: Is the set of circumstances that characterize the consummation of risk. In the circumstance of risk, events go beyond routine situations, dealing with broader business aspects, such as changes in the governance and operational structure, geopolitical and social influences and contract negotiations, among others;
- **Incident**: Is the undesirable and unforeseen event in relation to personal data that has the potential to cause inconvenience that can make it impossible to achieve the objectives, generating financial, operational, legal and file damages and losses, among others;
- **Severity**: Is metric based on aspects such as probability and impact of events or the time required to recover from events;
- **Probability**: Indicates the possibility of occurrence of a given event. It can be expressed in terms such as: high, medium, low;
- **Impact**: Result or impact of risk. Several possible impacts related to risks include: finance, operation, image and social environment;
- **Risk Level**: Relation between probability and impact, the risk can be classified as: very high, high, moderate, low or very low;
- **Appetite for Risk**: The degree of exposure to risk that **AMCEL** is willing to accept or reject in the pursuit of value creation and to achieve its goals;
- **Risk Responses**: The decision to accept, avoid, reduce and share the risk. It is the decision that will be taken after identifying the inherent Risk or evaluating the

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

residual Risks control environment, with the objective of promoting discussions that ensure the efficiency of **AMCEL**'s Internal Controls environment;


- **Action Plan:** Planning and monitoring the activities necessary for the risk response selected by management to be effectively executed to achieve the desired results.

3. RISK ASSESSMENT ASSUMPTIONS

This Standard seeks to provide guidelines in order to guide the assessment of risks related to the processing of Personal Data.

This process aims to ensure that **AMCEL** is safe and alert about unwanted acts that may lead to risks and incidents for the company.

- Practical adaptations: **AMCEL** adopts several governance practices in privacy and data protection, through policies and standards aimed at the rules and guidelines that should guide the treatment of Personal Data by the company. Thus, there is priority for the Subjects of Personal Data under their control to have the legitimate and legal treatment of such information and to comply with the applicable legislation;
- Standards and formalizations: With a model based on formalizations and standards recognized by the market and disseminated throughout the **AMCEL** structure, the risk management related to the processing of Personal Data is able to adapt to organizational strategies, initiatives and structures, in addition to meeting the sectorial and regulatory and supervisory requirements;
- Recognition and risk reduction: In accordance with what has been established so far, and with other Privacy and Data Protection Policies and Rules, **AMCEL** establishes that all risk assessments must include consideration of the benefits of treatment, including the benefits to individuals, the organization, third parties and society, aiming at preserving the desired benefits in the implementation of any mitigations to deal with the identified risks. Benefits should be considered at the beginning of the risk

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

assessment as they are related to the purpose of the treatment. The benefits and purposes of treatment should be kept in mind when designing mitigations to avoid unnecessary reduction of benefits or weakening of purposes;

○ Infrastructure: To efficiently manage risks, **AMCEL** must have an adequate infrastructure and **AMCEL** of processes, people and technology, establishing clear and objective communication mechanisms for this;


○ Threat Assessment and Recognition: The risk assessment should consider potential threats in treatment activities, such as:

- Unjustifiable or excessive data collection;
- use or storage of inaccurate or outdated data;
- inappropriate use or misuse of data, including:
 - Use of data beyond the reasonable expectations of individuals;
 - Unusual unreasonable use of data where any average individual in this context would object;
 - Inference or unjustifiable decision making, which the organization cannot objectively defend.
- lost or stolen data or destruction and alteration of data; and
- unjustifiable or unauthorized access, transfer, sharing or publication of data.

➤ The probability and severity of damage that may result from risk treatment, such as:

- Material, tangible, physical or economic risks to individuals:
 - Loss of freedom or movement, damage to finances and earning power.
- Non-material, intangible risks to individuals:
 - Damage to reputation, loss of autonomy, identity theft.

4. RESPONSIBILITIES

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

➤ The **Data Protection Officer (DPO)** must act in such a way as to consider the risks of the fundamental rights and freedoms of individuals in the performance of their tasks, so that they are able to create alternatives capable of meeting any potential risks.

➤ The **Internal Privacy and Data Protection Committee** must assist in the identification and assessment of risks and routinely conduct control procedures in order to mitigate the vulnerabilities of its activities, together with the Supervisor, implement the company's action plans approved by the High Management.

5. RISK TREATMENT PROCESS AND MANAGEMENT


➤ **First step - Risk Identification:**

- As a first step, the identification of risks must recognize and describe which events that may cause risk that the company is exposed to, and it must also describe changes in its business environments;
- Therefore, events, causes, consequences and those responsible for each risk must be defined;
- This identification of risks must be carried out with the participation of all the main area leaders and involved in the company's business processes, at their different levels, accompanied by the Person in Charge of Personal Data Protection.

➤ **Second step - Risk Assessment:**

- As a second step, and having already identified risks, qualitative and/or quantitative analyzes must be carried out through dynamic processes that aim to define the impact and probability attributes, to be used in the process of prioritizing the risks that must receive treatment by first;
- This risk assessment should consider the survey and analysis of existing controls and mitigating actions.

➤ **Third step - Risk treatment:**

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

- After the assessment has been carried out, it is necessary to continue with the step of defining the treatment that will be given to the prioritized risks and verifying how these should be monitored and reported to the various parties involved;
- Addressing risks is about deciding whether to avoid or mitigate them, share them or accept them. It must always be in accordance with the definition of action plans and internal controls;
- The decision on the strategy adopted to address each risk depends mainly on the company's Degree of Appetite for risk, previously approved by **AMCEL's** Senior Management.

✓ **Risk treatment in accordance with the General Data Protection Law**

- According to the General Data Protection Law, controllers will have to carry out a risk assessment in several cases due to specific requirements, although the risk assessment is not explicitly mentioned in these provisions.

✓ **Balancing Test**


- In the case of processing personal data based on legitimate interest, in order for AMCEL to determine whether it can follow the treatment, the Balance Test must be carried out in order to assess whether its legitimate interests are nullified by the interests or fundamental rights and freedoms of the data holder. This test should include risks and potential damages, impacts and probabilities, and include a risk assessment.

✓ **legitimate treatment**

- **AMCEL** must consider and analyze, among other points, the impact and consequences for the holders of Personal Data, including risks and damages that may arise from the treatment of that information collected.

✓ **Action plan**

- In this management, the action plan involves pointing out actions that are necessary and subject to correction to reduce exposure to residual risks, based on the mapping of weaknesses indicated in the risk assessment process.

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

✓ **Risk monitoring**

- In the risk monitoring process, you must:
- Oversee the implementation and maintenance of action plans.
- Check the achievement of the established action goals, through continuous management activities and/or independent evaluations.
- Ensure controls are effective and efficient.
- Detect changes in the external and internal context, identifying emerging risks and analyzing changes in risk events, trends, successes and failures and learning from them.


✓ **Risk communication**

- Communication during all the steps described here in conducting the risk management process must be accessible and available to all interested parties, in a clear and objective manner, striving for respecting the good governance practices required by **AMCEL**.

➤ **Risk reduction:**

- A wide variety of risk mitigation measures can be performed by **AMCEL**, ranging from pseudonymization, data minimization and security measures. These mitigation measures are context-dependent and must take into account the risks involved, the cost of implementation and the effectiveness of these measures, their impact on the objectives, interests or benefits being pursued, as well as the reasonable expectations of the holders, transparency and the elements of legitimate treatment.

6. REVISION

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

History of the last revision of this Standard:
--

Prepared by:	Verified by:
Position	Position
Name	Name
Approved by:	