AMCEL - AMAPÁ FLORESTAL E CELULOSE S.A.

INTRODUCTION

The information security policy, also known as ISP, is the document that establishes the guidelines, norms, procedures and good practices of the company's technological resources, always seeking to protect its "**INFORMATION**" strategically valuable asset.

This ISP is based on the recommendations proposed by the ABNT NBR ISO/IEC 2700 standards; 27002:2005; ISO/IEC 17799; BS 7799; RFC 2196 recognized worldwide as a code of good practices and information security management, as well as complying with the laws in force in our country, including the LGPD.

1. OBJECTIVE

Establish guidelines that allow employees, service providers and visitors to follow standards of behavior related to information security, adapting them to the company's business needs and the country's current legislation.

Guide the definitions of standards, procedures, guide its employees in the best practices of technological resources, as well as implement controls and processes seeking to protect information and maintain the continuity of the company's business.

Preserve AMCEL - Amapá Florestal e Celulose SA information, regarding:

* **INTEGRITY**: Ensuring that information is kept in its original state, in order to protect it from leakage, intentional or accidental misuse inside and outside the corporation.

* **CONFIDENTIALITY**: Ensure that all access to information is obtained only by persons authorized by the company.

* **AVAILABILITY**: Ensuring that authorized users gain access to the corresponding information and assets whenever necessary. PSI APPLICATIONS

2. ISP APPLICATIONS

The guidelines established here must be followed with the utmost rigor, covering all employees, without exception. Also extending to its providers and visitors who make use of the company's technological environment (Systems, Hardware, Software, Cell Phones, Printers, Scanner, Copier, Desk Phone, Notebook, Tablet, Wifi, IP Camera, DVR, or any other technological asset not mentioned here).

All employees, service providers and visitors must be aware that any equipment that is connected to the company's technological environment, regardless of the means used (Cable, Wifi or Bluetooth) may be monitored and/or audited without prior notice by the IT or at the request of the area manager via email, always justifying your request so that the IT Department can present its Technical Opinion.

3. ISP PRINCIPLES

Any and all information produced by AMCEL employees or service providers as a result of their professional activity will belong to that company, except in explicit cases in a contract between the parties.

All information and telecommunications resources provided by AMCEL to its employees and service providers must be for the exclusive use of professional activities, except for emergencies authorized by IT and that do not cause any damage to the company's technological infrastructure. PSI REQUIREMENTS

4. ISP REQUIREMENTS

For uniformity and the flow of information and the guidelines of this PSI, it must be communicated to all AMCEL employees, as well as to its service providers from all its units, so that the policy is complied with inside and outside of the company when there is use of its information assets.

There should be a **Personal Data Protection Commission** (PDPC) to gather, analyze and judge, together with IT, the most appropriate guidelines for the company, aiming at the continuity of its business

Both the ISP and the good information security practices must be periodically reviewed and updated, whenever any member of the management committee presents at its monthly meetings any relevant fact or event that motivates its review or update.

From the approval of this ISP, all contracts of employees and service providers must include the annex to the confidentiality agreement or the confidentiality clause of the information in contract renewals or in new contracts, making them aware that this condition will be essential for access to the assets and information made available by the AMCEL company may be granted.

Legal responsibilities in relation to information security must be communicated to employees and service providers during the hiring and integration phase in the company. All employees must be instructed on information security procedures, as well as the correct use of assets, in order to reduce possible risks of misuse or leakage of the

company's data, and they are required to sign a term of responsibility and in accordance with this ISP.

Any Incident that affects information security must be initially communicated to the IT area management and, if it deems it necessary, it must subsequently forward it to the Personal Data Protection Commission for due analysis and presentation of improvements.

A contingency and business continuity plan for the main systems and services must be presented by IT, they must be implemented and tested at least every 4 months, in order to reduce the risk of data loss, the contingency plan must be fully documented for that in an eventuality the responsible professional can use it as a basis for recovery.

The production environment (Data Center) and its controllers must be segregated so that there is no interference or visibility of employees or third parties in their activities, aiming at the confidentiality of information.

AMCEL shall act with the utmost rigor in complying with this ISP, when proven irregularity, irresponsibility, negligence or recklessness of the employee or service provider in the use of their information. The IT Department, whenever it observes any suspected irregularity, shall audit, analyze, and collect evidence and present it to the Personal Data Protection Commission - PDPC so that the situation is discussed and, if necessary, the relevant administrative sanctions are applied. ATTRIBUTIONS, RESPONSIBILITIES AND ROLES

5. DUTIES, RESPONSIBILITIES AND ROLES

In order to regulate the responsibilities and roles that will be undertaken by each agent and each area of AMCEL in the current Governance and Data Protection Program, the roles, responsibilities and indications of management and the respective definitions are distinguished, according to the provisions below. RESPONSIBILITIES OF THE PERSONAL DATA PROTECTION COMMITTEE

5.1. DUTIES OF THE PERSONAL DATA PROTECTION COMMISSION

These are duties of the Personal Data Protection Commission, as determined by the Internal Regulation and approved by the AMCEL Board of Directors:

- Implement the activities foreseen in the work of structuring and Governing the Privacy and Protection of Personal Data;

- Implement, monitor, evaluate and propose changes to the Information Security Policy, Personal Data Processing and its complementary internal rules;
- Formulate proposals and recommend tools and adequacy measures related to Information Security and Personal Data Processing, which will be submitted to the Executive Board for deliberation;
- Supervise and monitor the training schedule of teams on the subject;
- Propose the adoption of corrective measures and regulatory and procedural adjustments necessary to prevent situations of vulnerability to Information Security and violation of the General Law for the Protection of Personal Data;
- Establish an Incident Handling and Response Team in cases of breach of security and violation of the General Law for the Protection of Personal Data;
- Request investigations when security breaches are suspected;
- Provide knowledge of the most modern and appropriate practices affecting information security and personal data protection, as well as share information about new technologies, products, threats, vulnerabilities, risk management, security policies and other activities related to corporate security in this area;
- Assess the classification, reclassification and declassification of information regarding the degree of secrecy and the deadlines for restricting access to information within the scope of the Personal Data Processing Policy;
- Analyze the Internal Regulation and its amendments;
- Assess the effectiveness and sufficiency of **AMCEL**'s internal control structure and processes, presenting recommendations for the improvement of policies, practices and procedures that it deems necessary;
- Give an opinion on the matters submitted to it by the Board, as well as on those it deems relevant within its competence;
- Constantly monitor the Privacy Governance and Personal Data Protection Program.
- Propose ideas and investments related to information security in order to reduce risks and incidents that may affect AMCEL's information assets.

- Propose changes to versions of this ISP as long as it has a technical basis and approved by the majority of PDPC and Board members;
- Evaluate information security incidents and propose preventive or corrective actions;
- Define the appropriate measures in cases of non-compliance with this ISP and/or the normal and complementary information security procedures.

5.2. DUTIES OF THE PERSON IN CHARGE FOR PROCESSING OF PERSONAL DATA (DPO)

The duties of the Person Responsible for the Processing of Personal Data are:

- Receive requests and send notices to the holders of personal data, provide the necessary clarifications and take the necessary measures to exercise the rights that the LGPD grants them;
- Manage and update the mapping of data;
- Send and receive any notices and demands from public authorities, including the National Data Protection Authority (ANPD), regarding the protection of personal data and take the necessary measures to comply with them, immediately reporting to the Personal Data Protection Committee and other areas involved;
- Carry out, whenever necessary, the impact assessments, writing the respective reports (RIPD's), obtaining the approval of the Board and transmitting the document to the public authorities;
- Provide guidance to employees, third parties, suppliers and all other parts and units of the Company, on the best practices to be adopted in relation to the protection of personal data;
- Provide advisory support to the Personal Data Protection Committee in its deliberations and functions;
- Provide support in the management of threats and incidents involving personal data, ensuring adequate treatment and communicating, within a reasonable period, the competent authorities and affected holders, whenever this represents a relevant

risk or damage to the holders;

- Promote actions and support inspections to ensure compliance with the terms of the Privacy and Personal Data Protection Policies. DUTIES OF THE DEPARTMENT OF INFORMATION TECHNOLOGY

5.3. DUTIES OF THE INFORMATION TECHNOLOGY DEPARTMENT:

The duties of the Information Technology Department are:

- Preserve information with evidential value for auditing, legal and judicial purposes, in the correct form and for the correct period;
- Act so that the computational assets of hardware and software are always updated and reflect the best practices in the market, in order to ensure the security and privacy of information;
- Provide support to managers in provisioning, managing, auditing and canceling people's access to **AMCEL**'s directories and systems, so that personal information and data are only accessed by authorized persons and for legitimate purposes;
- Support departments in defining adequate Information Security controls;
- Assess, monitor and treat vulnerabilities, risks and incidents with the formalization of procedures to ensure quick, effective and orderly responses, triggering the impacted/responsible department when necessary;
- Assess the information security aspects necessary for each process and, whenever possible, employ encryption to protect strategic assets;
- Implement measures to sanitize **AMCEL**'s database, so that information and personal data are stored only for the time necessary to fulfill their purpose, and subsequently disposed of in a secure manner;
- Support the dissemination and propagation of the Information Security and Privacy culture, supporting other departments, promoting events, training and other awareness actions;
- Periodically report to the Personal Data Protection Commission the Information

Security and Personal Data Protection status and indicators;

- Establish, manage and disclose a channel to receive communications of risks or incidents associated with Information Security and Personal Data Protection, widely disclosing its existence and form of use to Users, who must be able to submit anonymous or identified communications;
- Promote or request the performance of external audits on employees, service providers, third parties, partners and suppliers;
- Test the effectiveness of the controls used and inform the IT area manager of residual risks;
- Agree with managers on the level of services that will be provided and the incident response procedures;
- Configure the equipment, tools and systems granted to employees with all the necessary controls to comply with the security requirements established by this ISP and the complementary information security standards, if any.
- Computer system administrators and operators can by characteristic of their access as admin users have privileges to access files of other users. However, this will only be allowed when it is necessary to perform operational activities, monitoring or auditing under its responsibility, as well as for maintenance of computers and/or backup copies.
- Segregate administrative and operational functions in order to restrict the powers of each individual to the minimum necessary, reducing and eliminating the existence of people who can exclude the logs and audit trails of their own actions.
- Ensure special security for systems with public access such as the Internet, being able to keep evidence that allows traceability for auditing or investigation purposes.
- Implement integrity controls to make them legally valid as evidence.
- Administer, protect and test backup copies of programs and systems related to critical processes relevant to **AMCEL**.
- Implement controls that generate auditable records for accessing, withdrawing

and transporting IT media and equipment from both its headquarters and branches.

- The user of the information must be previously informed about the end of the retention period so that they can have the alternative of altering it or removing their personal files before the information is definitively discarded by IT.
- When moving IT assets internally, ensure that a user's information is not removed in an irretrievable way before making the asset available to another user.
- Plan, implement, supply and monitor the storage, processing and transmission capacity needed to ensure the security required by the business areas.
- Assign each account or device for accessing computers, systems, databases and any other information asset to a responsible individual, provided that:
    - Individual users (logins) of employees will be the responsibility of the employee himself.
    - Third-party Users (Logins) are the responsibility of the contracting area manager.
- Actively protect all company information assets from malicious code, and ensure that all new assets only enter the production environment once they are free of malicious and/or unwanted code.
- Define the formal rules for installing software and hardware in corporate production environments, requiring compliance within the company.
- Conduct periodic audits of technical configurations and risk analysis.
- It is responsible for the use, handling, keeping of signature and digital certificates.
- Ensure, as quickly as possible, with formal request, the blocking of access of employees or third parties for reasons of termination or termination of the company, incidents, investigation or other situation that requires restrictive measures for the purpose of safeguarding the company's assets.
- Ensure that all servers, stations and other devices with access to the company's network operate with the clock synchronized with the region's official time.
- Monitor IT environments generating indicators and history of:
    - Use of installed capacity of the network and equipment;

- Response time in accessing the Internet and **AMCEL**'s critical systems;
- Period of unavailability in access to the Internet and to **AMCEL**'s critical systems;
- Security incidents (virus trojans, ransoware, sniffer, trojan, malware, keylog, fishing thefts and unauthorized access);
- Activities of all employees during access to external networks, including internet (sites visited, emails received and sent, file upload/downloads);

5.4. INFORMATION SECURITY AREA

- Propose specific methodologies and processes for information security, as well as risk assessment of processes and systems, always defining their classification.
- Propose, analyze and support initiatives presented by the PDPC (Personal Data Protection Commission) aimed at securing **AMCEL**'s information assets.
- Publish and promote the versions of this ISP, as long as they are analyzed by the PDPC and **AMCEL** Board of Directors.
- Promote the awareness of all employees and service providers of the relevance of information security for **AMCEL**'s business, through campaigns, lectures, training, news and other means of internal marketing.
- Support the assessment and adequacy of specific information security controls for new systems or services.
- Critically analyze incidents together with the PDPC and Board of Directors.
- Present the minutes and summaries of PDPC meetings, highlighting matters that require intervention by the committee itself or by members of the Board of Directors.
- Maintain effective communication with the PDPC (Personal Data Privacy Commission) on matters related to the subject that affect or have the potential to affect **AMCEL**'s assets.
- Seek alignment with the institution's corporate guidelines. RESPONSIBILITIES OF THE HUMAN RESOURCES DEPARTMENT:

5.5. DUTIES OF THE HUMAN RESOURCES DEPARTMENT:

The duties of the Human Resources Department are:

- Ensure that employment contracts or similar provide for the application and compliance with the Policies and Rules established by **AMCEL**'s Privacy Governance Program;
- Ensure that during the integration of new employees, training is applied related to periodic Information Security and Data Protection routines;
- Ensure that in all procedures adopted by the Department of Human Resources/Personnel, the Privacy and Personal Data Protection of employees and their respective dependents is observed;
- Assist the Personal Data Protection Officer in carrying out his responsibilities;
- Support training and awareness actions to spread the culture of Privacy and Information Security;
- Ensure that the Information Technology Department is informed in advance about the suspension or cut of access of employees, on vacation, on leave, changes in positions, functions, dismissed.

5.6. DUTIES OF THE MANAGEMENT BODY:

The duties of the AMCEL Management body (Directors, Managers, Supervisory Coordinators and Process Managers) are:

- Having an exemplary posture in relation to information security, serving as a model of conduct, complying with and monitoring compliance with the Policies and Norms instituted by **AMCEL**;
- Ensure that their subordinates are trained to handle and operate **AMCEL**'s Information and Personal Data Assets in accordance with the Policies and Rules;
- Ensure that safe information disposal measures are used correctly in accordance with the Information Handling and Disposal Standard adopted by **AMCEL**;

- Indicate to the Information Technology Department the definition of access profiles to the systems and software adopted by **AMCEL**, including third parties that may have access to such systems, always guaranteeing the minimum access to perform the necessary functions;
- Maintain control over the levels of access to information and Personal Data of members in your area and third parties under your responsibility;
- Carry out or request the Information Technology Department to review the access level of its subordinates every six months or whenever deemed necessary;
- Participate, whenever called, in Committee meetings and provide all requested clarifications;
- Execute and make the classification of suppliers and third parties be correctly executed, according to their criticality levels, in accordance with the Standard for Contracting Third Parties;
- In the development of new work processes, products and services, respect and ensure that the privacy of those affected is considered from conception to execution, in accordance with the Guidebook – Privacy in the Design of Products and Services.
- Before granting access to **AMCEL** information, require the signature of a confidentiality agreement from employees and service providers who are not covered by an existing contract, during the survey phase for the presentation of a commercial proposal.
- Adapt the standards, processes, procedures and systems under its responsibility to meet this ISP, as well as the terms of the company's standards. DUTIES OF THE LEGAL DEPARTMENT

5.7. DUTIES OF THE LEGAL DEPARTMENT:

The User's duties are:

- Monitor Information Security and Personal Data Protection Incidents that significantly violate the Information Security and Data Protection Policies and Standards;
- Legally support and assist the Personal Data Protection Commission, Information Technology Department and the Personal Data Protection Officer;
- Guide for the best way to collect and preserve electronic evidence, in order to maintain its effectiveness for use in court, when necessary;
- Support the review of documents, Policies, Rules, contracts and consultations related to Information Security and Personal Data Protection, as well as in the analysis and interpretation of the Data Protection regulation applicable to **AMCEL**;
- Advise procedures, processes and audits aimed at evaluating incidents, misuse, inappropriate use of Information Assets and Personal Data;
- Analyze and support Managers, Directors and the like in defining the level of requirement with Suppliers, pursuant to the Standard for Contracting Third Parties;
- Ensure that all contracts signed by **AMCEL** contain clauses aimed at Information Security and Privacy and Personal Data Protection;
- Provide support, together with the Supervisor, to those responsible for information security and privacy to any and all applicable legislation, especially in matters relating to:
    - *Data protection and privacy of personal information;*
    - *Intellectual property right;*
    - *Protection of organizational records;*
    - *Prevention of misuse of information processing resources;*
    - *Legislative Updates.*

- Be responsible for losses or damages that **AMCEL** and/or third parties suffer or cause as a result of non-compliance with the guidelines and standards referred to herein.

5.8. DUTIES OF USERS

The duties of all employees, regardless of hierarchical level or competence of action, role and responsibility to fulfill, observe compliance and respect the Policies and Standards instituted by **AMCEL**, as well as:

The User's duties are:

- Watch over the Information and Personal Data Assets, ensuring that no access, alteration, sharing, disclosure, destruction and elimination occur without proper authorization;
- Use **AMCEL**'s Information Assets and information and communication technology assets ("ATICs", e.g. internet network, computers, cell phones, printers, electricity, etc.) of **AMCEL** for the sole and exclusive purpose of **AMCEL**'s interest, subject to exceptions authorized;
- Ensure that all Information or Personal Data is being treated and operated correctly and, if in doubt, seek guidance in the Policies, Rules or hierarchical superiors;
- Participate in the training provided and, in mandatory cases, obtain a minimum pass mark;
- Immediately notify the Personal Data Protection Officer and the Information Security and/or Information Technology Department if you suspect any threat, risk or incidents of information security or data protection.

6. MONITORING AND AUDITING THE ENVIRONMENT BY IT

To ensure the rules mentioned in this ISP, as well as its versions, one can:

Implement monitoring systems on workstations, servers, email, internet connection, mobile or wireless devices and other network components, the information generated by this system can be used to identify users and their respective accesses, as well as manipulation or company data leaks;

Only make the information obtained by the monitoring and auditing system public, in cases of judicial demand, by formal request by the area's management, or by determination of the PDPC or Board of Directors;

Carry out, at any time, physical inspection of machines owned by the **AMCEL** Company;

Install protective, preventive and detectable systems to ensure the security of information and access to any information asset of the company.

7. USE OF E-MAIL

* The use of AMCEL's e-mail is for corporate purposes only, and the user may use his/her personal e-mail as long as it does not harm the company and also does not impact network traffic or the Internet link.

Never send e-mails unnecessary, in order to compromise the traffic of the internal network and Internet link, eg: Sending an e-mail to the All@amcel.com.br group, as well as answering e-mails to this group.

Never use corporate or personal e-mail within the company's premises to send malicious content, in order to put the recipient at risk or putting AMCEL in embarrassing situations.

Never disclose information, screen images, systems, documents without express and formal authorization granted by the owner of the information asset.

Never falsify addressing information, tamper with headers to hide the identity of the sender and/or recipients, in order to camouflage the standards provided for in this ISP.

Never produce, transmit or disseminate emails that:

- Contains any act or provide guidance that conflicts or contradicts **AMCEL**'s interests;

- Contain electronic threats such as spam; bombs emails; computer viruses or any malicious code;

- Aim to obtain unauthorized access to another computer, server or any equipment in **AMCEL**'s IT infrastructure;

- Aimed at disrupting a service, servers or computer network through any illegal or unauthorized method (DDOS attack, etc.);

- Aim to bypass any security system;

- Aim to secretly watch over another user, except in cases of express request by a management or board and/or audits carried out by IT in cases of suspicion of something illegal in the company;

- Aim to access confidential information without explicit formal authorization from the data owner;

- Include encrypted or otherwise masked images without the consent of the asset owner;

- Content deemed inappropriate or obscene or illegal within the company's premises;

- Information of a libelous, defamatory, degrading, infamous, offensive, violent, threatening, pornographic nature, among others that may harm the recipient;

- Contains harassment, prejudice based on sex, race, physical or mental disability;

- Have local or national political purposes (political advertising);

Email signature messages should always have the following data below, to mitigate possible social engineering attacks:

- Company Logo

- Company Name;

- Employee Name;

- Department

- Business phone for contact;

The information on the employee's badge must always contain the following data, reducing possible social engineering attacks:

- Company Name/Logo;

- Department;

- Badge;

- 3x4 photo

8. INTERNET

All current **AMCEL** rules are basically aimed at developing an eminently ethical and professional conduct in the use of the Internet. Although it is permanently filtered by the company's firewall, it still poses a potential risk to the company when misused. In this way, any information that is accessed, transmitted, received or produced on the Internet will be subject to audit by the IT department. Therefore, **AMCEL** has full legal compliance to monitor any and all access that is made within its IT infrastructure.

The technological equipment and systems provided by **AMCEL**, as they are its property, may be analyzed and, if necessary, sites, files, email or any application stored on the network/internet or intranet may be blocked, in order to ensure compliance with its policy information security.

AMCEL, by monitoring the internal network, intends to ensure the integrity of its information assets, therefore, any attempt to change the security parameters by any employee without proper accreditation or authorization to do so will be deemed inadequate and the related risks will be informed to the PDPC and the Board to assess and judge the situation. The use of any resource for illegal activities may lead to administrative actions and penalties arising from civil and criminal proceedings, in which case, **AMCEL** shall actively cooperate with the competent authorities when requested.

The internet made available by **AMCEL** to its employees and partners, regardless of their contractual relationship, may be used for personal purposes, provided that it does not affect the progress of its activities and that it is not used for illegal purposes. This paragraph is valid for all your units.

As it is in **AMCEL**'s interest that its employees are well informed, the use of news sites or services will be acceptable as long as it does not compromise the link and internet bandwidth during business hours and does not disturb the smooth running of the work or imply conflicts of interests with your business goals.

Only employees authorized by the institution may copy, print or send computer screen images to third parties or government agencies, always complying with Copyright Laws and the General Data Protection Law (LGPD).

The disclosure and/or sharing of company information to third parties and government agencies is prohibited, unless authorized in writing by the area manager justifying such situation.

Employees with internet access may only download programs or software directly linked to their functional activities, as long as it is licensed. It is up to IT to analyze and authorize its installation on the workstations.

Under no circumstances may employees use **AMCEL** resources to download pirated software distributions (cracked) for use in their activities, such practice will be considered criminal according to the legislation in force in the country,

The download and use of entertainment programs, social networks, digital TV, games or music (in any format) cannot be carried out within the company's infrastructure, unless authorized in writing and justified by the area manager.

As a general rule, material of a sexual nature may not be displayed, stored, distributed, edited, printed or recorded through any **AMCEL** information resource, and those involved are subject to administrative penalties when deemed valid by the PDPC and the DPO.

All employees, without exception, may not use remote access software such as (Teanviwer, Anydesk, Tmbuktu, Webex, VNC, TightVNC or any other related software) without proper IT analysis and authorization, where it may put the infrastructure of **AMCEL** Information Technology.

It is strictly prohibited to use any software that makes it possible to circumvent the company's firewall rules.

9. IDENTIFICATION

This procedure aims to establish criteria and rules for information security and responsibility for the use of computing devices, giving greater security to the company's assets.

The use and access by login and password of another employee to the company's computer systems in order to gain an advantage, for one's own benefit or for others, or to cause harm to others, is strictly prohibited. Such practice is characterized as a crime of false identity by the Brazilian penal code - art. 307.

All identification devices used in AMCEL. As the employee's registration number, the badge, the identifications for access to certificates, digital signatures, biometric data must be associated with a natural person and unequivocally linked to their official documents recognized by the current Brazilian legislation.

Users linked to such devices as identification tokens, who are responsible for the company, will be responsible for their correct use before government institutions and

bodies, being subject to administrative, civil and criminal sanctions when their misuse is proven.

Any and all personal identification devices cannot be shared with another user under any circumstances.

It is strictly prohibited to share the computer systems and database administrator login to any other employee or third party that is not part of the IT staff.

It is the responsibility of the IT Department to create, change, delete profiles and users from the network, as well as e-mail accounts and internal systems (Protheus, website, integrates, full controll, offline, etc.) .

All passwords created by users must contain the following technical specifications: have at least 7 (seven) alphanumeric characters, using special characters (@, #, $, %) and varying between uppercase and lowercase (uppercase and lowercase) and numbers, obligatorily.

Users who have an administrator profile or privileged access must use a password of at least ten (10) characters, alphanumeric, using special characters (@, #, $, %) and variations between uppercase and lowercase (uppercase and lowercase) and numbers, obligatorily.

Access to the wifi network must be requested by email, followed by the justification for use, always copying your manager to avoid information leakage and unauthorized access.

It is the responsibility of each user to memorize their own password, as well as the protection and custody of the devices assigned to them for their activities.

Passwords must not be written down or stored in electronic files. They should not be created based on personal information, such as name, date of birth, addresses, license plate, company name or department. Such practice could put the company's assets at risk.

After the user's 3rd wrong login attempt on the network, the account will be locked automatically, so that the account is unlocked, the user must contact the IT department to request the unlock and/or change the password for security reasons.

Network passwords must be automatically changed every 3 months, and the new password cannot be the same as any previous one or that does not meet the criteria established in the previous paragraphs.

10. COMPUTERS AND TECHNOLOGICAL RESOURCES

The computer equipment available to employees is owned by **AMCEL**, and each user is responsible for using and handling them correctly for activities of interest to the company, as well as complying with the recommendations contained in the operational procedures provided by the IT area.

Any physical or logical maintenance procedure, installation of programs, uninstallation, configuration or modification of the location of any equipment is strictly prohibited without the technical monitoring of the IT area, if necessary, the applicant must inform IT by and e-mail, 24 hours before execution so IT can assess and plan for change.

Personal files not relevant to **AMCEL**'s business (photos, music, videos, etc.) should not be copied or moved to network or computer drivers.

In the use of computers, equipment and information resources, some rules must be met:

- Employees have the duty to communicate to the IT Department or any member of the PDPC (Personal Data Protection Commission), whenever they observe any practices in disagreement with this policy on information caused by one of their co-workers, identity preserved by the information holders.

- Employees must immediately inform the IT Department when they observe any strange situation on their device so that appropriate measures can be taken as soon as possible.

- The opening and handling of computers, notebooks, smartphones, tablets or any other computer equipment is prohibited, except by an IT technician and/or specialized company when necessary, always informed in writing to the IT Department so that it is updated in its controls

- The use of a Modem, Pendriver, external HD or any external storage media (personal) on the company's computers is strictly prohibited, except when there is an extreme need and it is authorized by the IT team.

- The employee is prohibited from changing any configuration of the equipment assigned for his/her activity, and it is only up to IT to perform this procedure.

- It is the responsibility of the employee or third party to maintain and preserve any equipment or device that is under their care, and they may assume the costs for its misuse or damage when detected by IT.

- All default passwords must be changed at the employee's 1st login.

We have added some situations in which the use of AMCEL computers and technological resources is prohibited:

- Attempt or gain unauthorized access to another computer, server or network, except by IT being audited;

- Bypass any security system;

- Misusing confidential information of the company, in order to self-promote;

- Secretly use any type of packet analyzer (sniffer) on the network in order to obtain confidential information, except by IT;

- Interrupt a service, servers or computer network by any illegal or unauthorized method, except by IT;

- Use any type of technological resource to commit or comply with acts of violation, sexual harassment, disturbance, manipulation or suppression of copyright or intellectual property without proper legal authorization from the holder;

- Hosting, storing, saving, sharing or transferring pornographic, racist, or any other material that violates the legislation in force in the country, morality, good customs and public order using **AMCEL**'s infrastructure.

- Use any pirated software, using a cracker, as long as authorized by the IT manager.

11. MOBILE DEVICES

The employee is responsible for the cost of repairing a mobile device due to misuse, breakage or accident with spillage of liquid products in the equipment provided by **AMCEL** for their daily activities;

In case of theft or robbery, the employee must inform the IT Area Manager and then look for the police authority to register the police report (BO) for the appropriate dealings.

It is strictly prohibited, the use of portable equipment, such as smartphones, palmtops, pen drives HDs and players of any kind, when not authorized and analyzed by the IT management, cannot be used in the company's equipment.

12. DATA CENTER

- Access to the Data Center room premises are restricted to IT professionals and/or persons authorized by the area management, always accompanied by a professional in the area for security reasons.

- It is prohibited to use video cameras, cell phones and cameras on the Data Center premises, with the exception of security cameras in the room;

- All MASTER passwords for Network Administrator, Database, PABX, Internal Systems and Clou, must be restricted to the technical responsible for the area and the IT Manager;

- In branches where there are no employees in the IT area, the area must request the help of the most suitable employee to assist them in any emergency situations;

- Any and all incidents of great relevance in the Data Center Room, must be registered in the IT controls and presented when deemed necessary in the monthly PDPC meetings for knowledge and suggestions for improvements when it is something that puts the technological assets of the company.

- The Administrative department must quarterly submit to the IT Department the planning of preventive maintenance in the air centers of the Data Center Room, as well as inform any need for access to the room at least 24 hours in advance so that IT can schedule, except in emergency cases.

- There must be only 2 copies of the Data Center door key, one must be with the technical manager and the other with the IT area manager;

- The Data Center Room must always be kept clean and organized. Whenever necessary, the general services team must carry out the cleaning accompanied by an IT professional;

- The entry of any type of food, drink or flammable products is strictly prohibited;

- The entry or removal of any equipment from the Data Center will only occur with the formal authorization procedure by the technical responsible for the area or by the IT manager so that no downtime occurs in any service or system.

13. BACKUP

- All backups must be automated by automatic scheduling systems outside business hours, except in cases of extreme need, it may be manual;

- The technical responsible for the backups must carry out frequent research to identify updates and corrections to product versions, always looking for improvements in the processes;

- Backup copies must be stored in secure locations such as NAS 1 (DATA CENTER ROOM) and NAS 2 (SCALE ROOM), as well as being replicated to the GOOGLE DRIVER by NAS 1, always following the redundancy in more than one place.

- The maximum period for keeping backup histories of Zenith and Divamprod databases will be 30 days, with the technical responsible free to restore it at any time for consistency testing.

- Backup restore tests must be run once a week

- To formalize the backup and restore execution control, there must be a strict control form for the execution of this routine, which must be completed in detail with date and time and the result thereof, which will be presented when necessary at the meeting with the PDPC for knowledge.

- The controller responsible for the procedures may delegate the execution of this process to another technician due to force majeure, however, he must always certify that the procedure was done correctly, not exempting the technical responsibilities of the person who did it.

FINAL PROVISIONS

Like ethics, information security must be understood as a fundamental part of **AMCEL**'s internal culture. That is, any security incident derived from an employee must be investigated and the necessary punishments applied to maintain the preservation of the company's assets.