CONTENTS

1. OBJECTIVES

Establish guidelines to protect Klabin's information and operations in matters of cyber security, as well as to ensure that it is properly treated throughout the life cycle of information.

1.1 Principles of Cybersecurity

- Confidentiality - a condition where only authorized users are allowed to access the information;
- Availability - a condition where the information should be available to authorized users when requested;
- Integrity - condition where only authorized changes can be made to the information.
- Authenticity – condition in which we guarantee that the information has been forwarded by the author, that is, it generates non-repudiation.

2. SCOPE

This policy applies to all Klabin SA units, its subsidiaries, in Brazil and abroad, and to shareholders, administrators, own employees and third parties, when they represent the interests or act on behalf of Klabin SA.

3. TERMS AND DEFINITIONS

Authenticity: Guarantee of origin and reliability about the property, who created, when and where.

Backup: This is the act of copying entire files, folders, or disks (physical or virtual) to secondary storage systems, seeking data preservation.

Information Classification: Information should be classified according to its criticality and sensitivity to the business and its customers, so that appropriate security is applied in order to reduce vulnerabilities, as per levels:

Confidential	Restricted	Internal	Public
It is information that, if internal disclosure or externally, they have potential to bring great damage financial or in the image of company.	They should be available only for restricted groups of employees.	They can be disclosed only for employees and third parties.	They may be knowledge public, however disclosure is responsibility specific areas (communication and marketing).
Employee's salary, strategic information (e.g. purchase of a company, from machine, development products, new technologies), sensitive personal data, price list, etc.	Information specific to department (e.g. audit report, information and data employees), personal data, etc.	Policies, procedures, instructions work, intranet corporate, etc.	Information provided in Klabin’s website, newspaper, relations public, etc.

Collaborators: All persons with employment link to Klabin SA, associated with a record.

Confidentiality: This is the level of restriction of information, whose access will be granted only to authorized persons.

Personal data: Information related to an identified and identifiable natural person.
Availability: Ensure that information and ICT resources are available where necessary and with appropriate authorization for access or use.

HD (hard drive): Used to store files, programs, folders, and all kinds of content on your computer.

CIS: Acronym for Industrial Control Systems (in Portuguese: Industrial Control Systems), being all physical or logical features programmable for the control and monitoring of discrete or continuous industrial processes. Examples: DCS, PLC, SCADA, BMS, including their equipment such as controllers, computers, switching, gateways, routers, access point, etc.

Information: Is the set of data that, processed or not, can be used for the production, transmission, and sharing of knowledge, contained in any medium, medium, or format.

Integrity of Information: Guarantee that the authenticity of the information has not changed without authorization.

Malware: Acronym for malicious Software. Generic designation given to any type of unwanted software, installed without the knowledge and consent of employees, in order to change or steal information, as well as to cause data proven by computer viruses, Trojan horses, Spyware, Adware, which are examples of malware.

Non-repudiation: Methods (usually encrypted) that prevent an individual or an entity from denying the execution of a particular action.

Owner of the Information: Person responsible for the information and its protection.
Patches: Software updates and firmware updates to correct security failures, vulnerabilities, or malfunctions.

Information and communication technology resources (ICT resources): These are all the physical and logical resources used to create, store, handle, transport, share and discard information. Example: Computers, notebooks, smartphones, tablets, pen drive, HD, media, printers, scanners, etc.

Third, owners or employees of other employers who do not have an employment relationship with Klabin, who work in or to, supported by a service contract as a physical or legal person.

ICT: Information and Communication Technology.

Vulnerability: This is a weakness that enables an attacker to reduce the assurance of information from a system. It is also the intersection of three elements: Susceptibility or system failure, access to failure, and the attacker's ability to exploit the failure.
RESPONSIBILITIES

4.1 Board

The approval of the Cybernetic Security Policy is the responsibility of the corporate services and people's boards, Legal and Industrial Technology, Innovation and Sustainability.

4.2 Cybernetic Security Management Committee (GSC)

- Prepare and submit to the Board proposals for rules and policies for the use of information resources;
- Resolve doubts and resolve issues not covered by Cybernetic Security Policy and related norms;
- Support in the deliberations of behavioral and technical cyber security incidents;
- Direct cyber security actions based on Klabin's integrated risk management and best practices;
- Review Cybernetic Security Policy and related standards for a maximum of four years.

4.3 Cybernetic Security Area

- Apply layers of protection technologies to mitigate possible security risks;
- Maintain the ability to prevent, detect, and reduce vulnerability to cyber environment-related incidents using logs;
- Conduct incident monitoring and response;
- Develop incident scenarios for periodic continuity testing;
- Working on cyber security awareness;
- Assess security requirements present prior to software acquisition or development and new architectures;
- Ensure the deployment of controls according to Cybernetic Security policies;
- Manage cyber risks and deploy controls according to Cybernetic Security policies, performing mappings, ratings, and monitoring in conjunction with the Internal Controls and risk Management Area.

4.4 Information Technology Area

- Ensure that all ICT resources used by Klabin meet the recommendations of its manufacturers or developers;
- Ensure that Business continuity Plan procedures in Information Technology are performed in accordance with Cybernetic Security requirements;
- Support in dealing with cyber security incidents reported by the area where necessary;
- Support Klabin’s departments in defining appropriate controls on cyber security;
- Maintain an asset management process according to IEC62443 and ISO27001 settings to support incident response actions;
- Maintain a vulnerability management process that involves the analysis and application of patch updates;
- Assist in defining the architecture of new technologies;
- Maintain a Backup and Restore process to ensure the availability of information and the productive process, respecting the storage period of applicable information, regulations and regulations.

4.5 Automation Technology Area

- Ensure that all ICS resources used by Klabin meet the recommendations of its manufacturers or developers;
- Ensure that business continuity plan procedures are performed in the ICS systems environment in compliance with Cybersecurity requirements;
- Support in dealing with cyber security incidents reported by the area where necessary;

4.6 Legal area

- To issue formal guidelines on legal compliance in the subjects that share the Cybersecurity discipline.

4.7 Communication Area

- Perform brand monitoring for the proactive purpose of identifying possible incidents;
- To assist Cybersecurity in the dissemination of campaigns and materials for training and awareness among Klabin’s employees.

4.8 Information Owner

- Know the criticality of Information;
- To authorize, or not, the release of any proprietary information or data or under Klabin’s responsibility, complying with the levels of confidentiality.

4.9 Area of People & Management

- Support Cybersecurity in the dissemination of training and workshops;
- Support in safety controls, specifically related to hiring, shutting down, and transferring processes of employees;
- Make Klabin’s regulations available, in addition to costing and collecting the signature of the “term and Code of Conduct” in the admission of new employees.

4.10 Manager

- Maintain investments that allow operational continuity in Cyberethical Safety at Klabin;
- To request and authorize the granting and revocation of access by its collaborators and third parties in accordance with the functions to be performed and to ensure that Klabin’s proprietary information is accessed and used only for the performance of its functions and by duly qualified persons;
- Communicate immediately and formally to the Unit's Information and Automation Technology area, the termination of the third party contract, so that access to ICT resources and automation systems are revoked.

5. GENERAL GUIDELINES

- Comply with and enforce this policy and other supporting documents;
- Observe and report potential cyber threats to the operation;

- To ensure the safe keeping of Klabin's information, customers and the general public in an ethical and sensitive manner, in accordance with current laws and internal rules. Avoid misuse and improper exposure, using it appropriately and solely for the purpose which it was collected and accessed only by duly authorized persons;
- To ensure compliance with the General Data Protection Law and Internet Civil Framework;
- The hiring or use of any technology, software, application, hardware, and any technology, digital, or services applied to these technologies that are not previously approved by it, TA, and Cybernetic Security is prohibited;
- It is not allowed access to sites that publish inappropriate content (pornography, pedophilia, racist weapons and attacks, among others). Avoid sites of doubtful content;
- Sharing users, passwords, and access is not allowed. The identification of any associate or third party must be unique, personal and non-transferable, qualifying him as responsible for the actions taken;
    - Users are not allowed to store data and information on local disks or removable media, and are responsible for handling and saving logical files only on the corporate network and/or cloud (office 365 only).

5.5 Removable Media

É The use of removable media (Pen Drive) in the IT environment is authorized only to perform corporate activities related to the financial process (bank token and digital certificate). In the ICS environment the external connection interfaces of removable media must be disabled (including the use for battery charging devices).

É The use of removable media for file transfer is forbidden. For this activity, use OneDrive from Office 365.

5.6 Access Security

5.6.1 Physical Security

Physical access control measures to ICT resources and ICS systems should be implemented, restricting access only to persons duly authorized by those responsible for the assets, such as data centers, technical rooms, control towers, etc.

5.7 Prevention and Policy Management

5.7.1 Education and Awareness

Establish a knowledge track for Klabin employee's Cybersecurity development.

5.7.2 Social Media

Only the Internal Communication team is authorized to maintain social media profiles under Klabin’s name. All communications on behalf of the company must be made by this team. Employees and third parties must remain watchful of audio, video, pictures and text posted on their own social media accounts so that such posts, shares and/or comments do not cause embarrassment, information leaks, defamation, exposure, etc.

5.7.3 Workplace

We must keep the workplace orderly and the information stored in safe places. No confidential and/or restricted information must be left in plain sight, be it on paper or any devices, whether electronic or not.

5.7.4 E-mail and Communication Applications

E-mail and other instant messaging services (e.g.: Teams) provided by Klabin are working tools and must be used to support the execution of functional activities. Use of these tools for personal purposes is not allowed.

The email addresses and mailboxes made available to users are Klabin’s property. Personal e-mail accounts must not be used to convey or store Klabininformation/data.

5.7.5 Incident Response

In the presence of suspected fraud or incident compromising Klabin’s information security, or in the event of an information leak or any other kind of cybersecurity incident, the employee or third party must immediately record the fact and give notice of it to the Information Security area (segurandadainformacao@klabin.com.br) or https://www.canalconfidencial.com.br/klabin/#home Klabin has an incident response process in pace and strives to reduce impact on information availability, confidentiality and integrity and on production processes.

5.7.6 Audit and Monitoring

Klabin may audit or inspect the ICT resources (e-mail, mobile phones, notebooks, systems, etc.) and automation systems inside its facilities or that interact with its logical systems whenever it deems necessary and according to the principles of proportionality, reasonability and privacy of their owners or bearers.

Klabin may carry out risk ICS Cybersecurity risk assessments in the company’s business units.

5.7.7 Disciplinary Sanctions

Violations of this policy are subject to the disciplinary sanctions provided for in the internal rules, code of conduct, and in the legislation in force in Brazil and in the countries where the companies are located.

6. REFERENCES

6.5. Internal Policies and Procedures

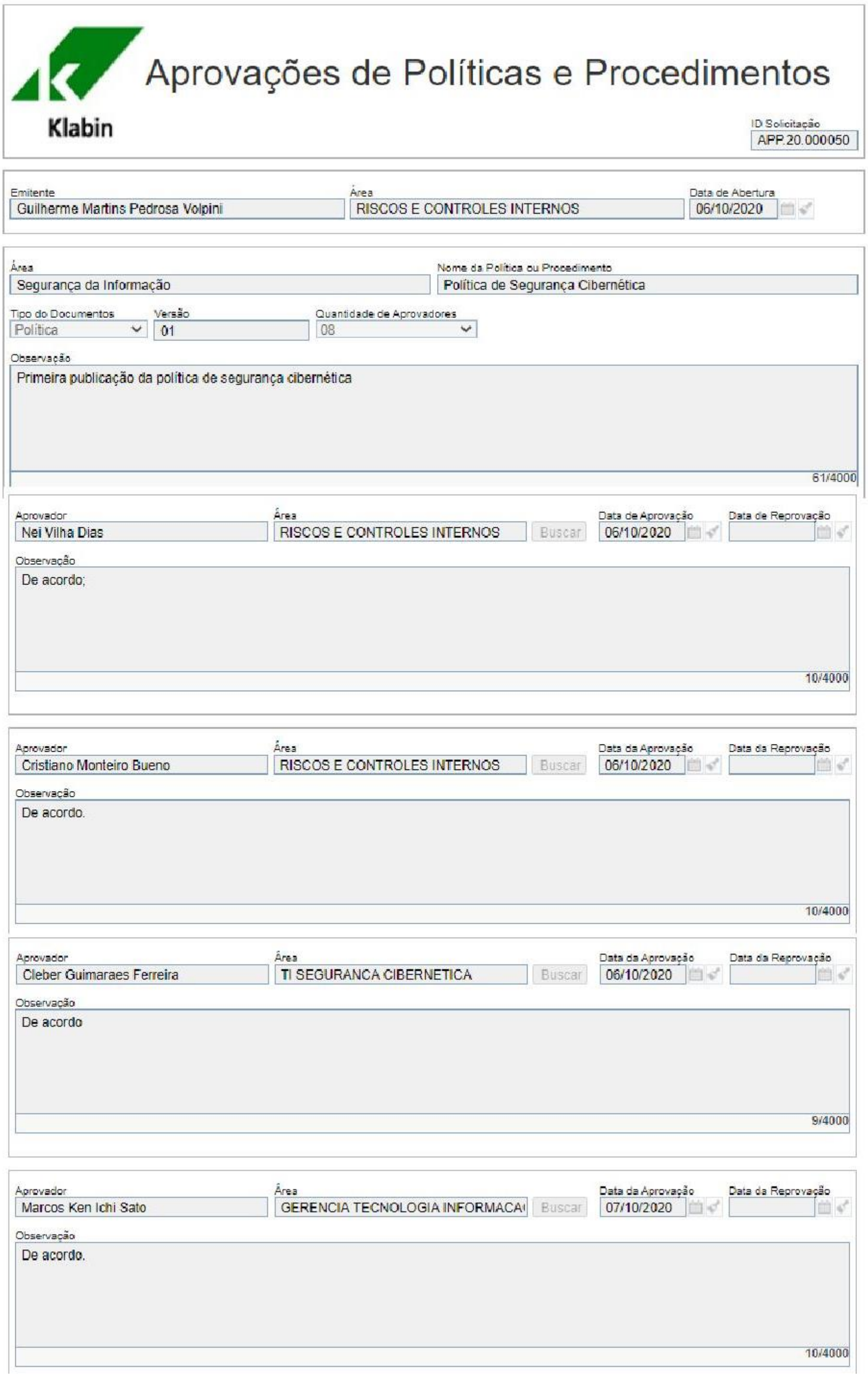
- Privacy Policy
- Intellectual Property and Technology Transfer Policy
- Risk Management Policy
- Code of Conduct

6.6. Standards

The following standards, in their latest available versions, were reviewed to draft this policy:

Standard	**Description**
NIST SP 800-82	*Guide to Industrial Control Systems (ICS) Security*
NIST SP 800-53	*Security and Privacy Controls for Federal Information Systems and Organizations*
ISA/IEC 62443	*Security for Industrial Automation and Control Systems*
ISO 27001	*Information security management system*
ISO 27002	*Security information management best practices code*
ICS.SecurityFramework ®	*IT Safe methodology for the protection of industrial environments*

7. APPROVALS



Klabin

Aprovações de Políticas e Procedimentos

ID Solicitação: APP.20.000050

Emitente	Área	Data de Abertura
Guilherme Martins Pedrosa Volpini	RISCOS E CONTROLES INTERNOS	06/10/2020

Área	Nome da Política ou Procedimento
Segurança da Informação	Política de Segurança Cibernética

Tipo do Documentos	Versão	Quantidade de Aprovadores
Política	01	08

Observação

Primeira publicação da política de segurança cibernética

61/4000

Aprovador	Área		Data de Aprovação	Data de Reprovação
Nei Vilha Dias	RISCOS E CONTROLES INTERNOS	Buscar	06/10/2020	

Observação

De acordo;

10/4000

Aprovador	Área		Data da Aprovação	Data da Reprovação
Cristiano Monteiro Bueno	RISCOS E CONTROLES INTERNOS	Buscar	06/10/2020	

Observação

De acordo.

10/4000

Aprovador	Área		Data da Aprovação	Data da Reprovação
Cleber Guimaraes Ferreira	TI SEGURANCA CIBERNETICA	Buscar	06/10/2020	

Observação

De acordo

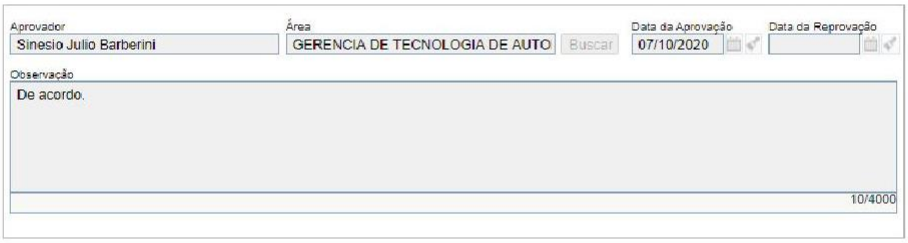
9/4000

Aprovador	Área		Data da Aprovação	Data da Reprovação
Marcos Ken Ichi Sato	GERENCIA TECNOLOGIA INFORMACA(	Buscar	07/10/2020	

Observação

De acordo.

10/4000

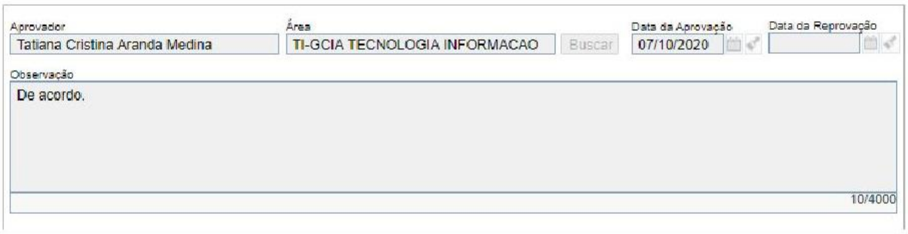


Aprovador	Área	Data da Aprovação	Data da Reprovação
Sinesio Julio Barberini	GERENCIA DE TECNOLOGIA DE AUTO	07/10/2020	

Observação

De acordo.

10/4000

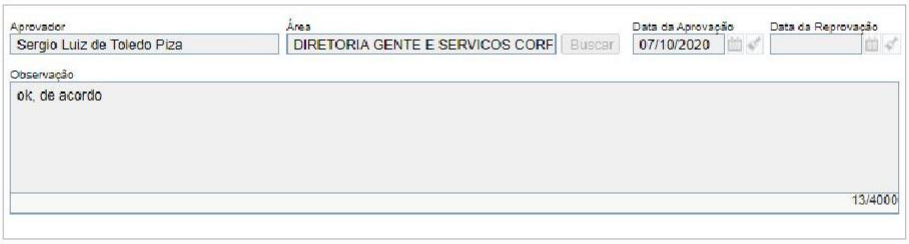


Aprovador	Área	Data da Aprovação	Data da Reprovação
Tatiana Cristina Aranda Medina	TI-GCIA TECNOLOGIA INFORMACAO	07/10/2020	

Observação

De acordo.

10/4000

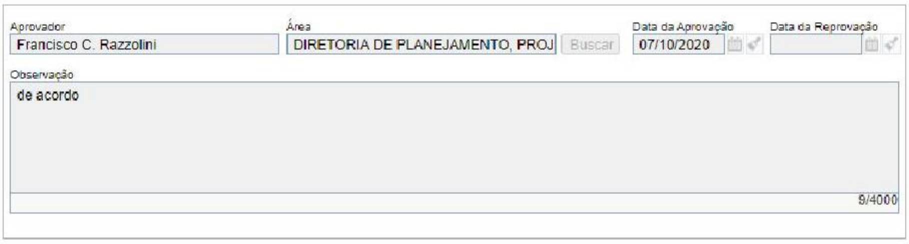


Aprovador	Área	Data da Aprovação	Data da Reprovação
Sergio Luiz de Toledo Piza	DIRETORIA GENTE E SERVICOS CORF	07/10/2020	

Observação

ok, de acordo

13/4000



Aprovador	Área	Data da Aprovação	Data da Reprovação
Francisco C. Razzolini	DIRETORIA DE PLANEJAMENTO, PROJ	07/10/2020	

Observação

de acordo

9/4000