1. Introduction

1.1. BBC's mission is to supply thermoplastic and thermoset processing additives to customers in various segments such as footwear, toys, rigid profiles, linings, films, tarpaulins, wire and cable, etc., with the highest quality and performance, creating stable long-term relationships.

1.2. BBC understands that corporate information is an essential asset for its operations and for ensuring the quality and warranty of the products offered to its customers.

1.3. The BBC understands that the processing of its information passes through various means of maintenance, storage and communication that are vulnerable to external and internal factors that may compromise the security of corporate information.

1.4. The BBC has thus established its General policy on information security as an integral part of its corporate governance system, in accordance with internationally accepted best practices and standards, in order to ensure adequate levels of protection for the organization's information on or under its responsibility.

2. Purpose

2.1. The purpose of this policy is to set out information security guidelines and standards to enable BBC employees to adopt standards of secure behavior appropriate to the BBC's purposes and needs;

2.2. Provide guidance on the adoption of controls and processes to meet information security requirements;

2.3. Protect the BBC's information by ensuring the basic requirements of confidentiality, integrity and availability;

2.4. Prevent possible causes of incidents and legal liability for the institution and its employees, customers and partners;

2.5. Minimizing the risks of financial loss, loss of market share, loss of customer confidence or other negative impact on the BBC's business as a result of security breaches.

3. Scope

3.1. This policy applies to all users of BBC information, including any person or organization who has or has had a relationship with the BBC, such as employees, former employees, contractors, former contractors, employees, former employees who have, have or will have access to BBC information and/or have used, are using or will use computer resources included in the BBC infrastructure.

4. Guidelines

4.1. The objective of information security governance at the BBC is to ensure systematic and effective management of all aspects related to information security, providing support for critical business operations and minimizing identified risks and their potential impact on the institution.

4.2. The Chair, Executive Board and the Information Security Management Committee are committed to effective management of Information Security at the BBC. In this way, they adopt all appropriate measures to ensure that this policy is properly communicated, understood and followed at all levels of the organization. Periodic reviews will be carried out to ensure they remain up to date and relevant to the BBC's needs.

4.3. It is BBC policy:

4.3.1. Fully develop, implement and follow information security policies, standards and procedures, ensuring that the essential requirements of confidentiality, integrity and availability of BBC information are achieved by adopting controls against threats from external and internal sources;

4.3.2. Provide access to security policies, standards and procedures to all interested and authorized parties, such as: Employees, contracted third parties and, where appropriate, customers.

4.3.3. Provide training and awareness of the BBC's accepted information security practices to employees, contracted third parties and, where appropriate, customers.

4.3.4. Fully comply with applicable information security requirements or those required by regulations, laws and/or contractual provisions;

4.3.5. Fully handle information security incidents, ensuring that they are properly logged, classified, investigated, corrected, documented and, where necessary, reported to the appropriate authorities;

4.3.6. Ensure business ongoing by adopting, implementing, testing and continuously improving continuity and disaster recovery plans;

4.3.7. Continuously improve information security management by systematically setting and reviewing security objectives at all levels of the organization.

5. Roles and Responsibilities

5.1. INFORMATION SECURITY MANAGING COMMITTEE - CGSI

5.1.1. The INFORMATION SECURITY MANAGING COMMITTEE is hereby established, with the participation of at least one representative of the board of directors and one senior member from the following areas: Technology and Information Security (GreenTec), Human Resources, Purchasing, Sales, Accounting, Labor Safety, and Product/Laboratory Development.

5.1.2. It is the responsibility of the CGSI:

5.1.2.1. Analyze, review and propose approval of policies and standards related to information security;

5.1.2.2. Ensure the availability of resources required for effective Information Security Management;

5.1.2.3. Ensure that information security activities are performed in accordance with the PGSI;

5.1.2.4. Promote the dissemination of the PGSI and take the necessary actions to disseminate an information security culture in the BBC environment.

5.2. INFORMATION SECURITY MANAGEMENT

5.2.1. It is the responsibility of Information Security Management:

5.2.1.1. Conduct Information Security Management and Operation, based on this policy and other CGSI resolutions;

5.2.1.2. Support the CGSI in its deliberations;

5.2.1.3. To elaborate and propose to the CGSI the information security norms and procedures, necessary to enforce the PGSI;

5.2.1.4. Identify and assess the main threats to information security, as well as propose and, when approved, implement corrective measures to reduce the risk;

5.2.1.5. Take appropriate action to enforce the terms of this policy;

5.2.1.6. Perform information security incident management, ensuring proper handling.

5.3. **INFORMATION MANAGERS**

5.3.1. It is the responsibility of the Information Managers:

5.3.1.1. Manage the information generated by or under the responsibility of your business area throughout its life cycle, including creation, handling and disposal according to the standards established by the BBC;

5.3.1.2. Identify, classify and label the information generated by or under the responsibility of your business area according to the standards, criteria and procedures adopted by BBC;

5.3.1.3. Periodically review the information generated by or under the responsibility of your business area, adjusting its classification and labeling as needed;

5.3.1.4. Authorize and review accesses to information and information systems under your responsibility;

5.3.1.5. Request the granting or revocation of access to information or information systems in accordance with the procedures adopted by the BBC.

5.4. **INFORMATION USERS**

5.4.1. It is the responsibility of the Information Users:

5.4.1.1. Read, understand and fully comply with the terms of the General Information Security Policy, as well as the other applicable security standards and procedures;

5.4.1.2. Forwarding any questions and/or requests for clarification about the General Information Security Policy, its rules and procedures to the Information Security Management or, when pertinent, to the Information Security Management Committee;

5.4.1.3. Report to Information Security Management any event that violates this Policy or endangers the security of BBC's information or computing resources;

5.4.1.4. Sign the BBC's Information Systems Use Agreement, formalizing awareness and full acceptance of the provisions of the General policy on information security, as well as the other security rules and procedures, assuming responsibility for their compliance;

5.4.1.5. Be accountable for non-compliance with the General policy on information security, security rules and procedures, as defined in the item sanctions and punishments.

6. Sanctions and Penalties

6.1. Violation of this policy, as well as other security standards and procedures, even by omission or inadvertent attempt, is subject to sanctions that include verbal warning, written warning, removal from employment without pay, and dismissal for just cause;

6.2. The application of sanctions and penalties shall be carried out in accordance with the analysis of the Information Security Management Committee, taking into account the gravity of the violation, the effect achieved, repetition and the cases provided for in Article 482 of the Consolidation of Labor Laws.

6.3. In the case of third parties or service providers with whom a contract has been concluded, the CGSI analyses the event and decides on the application of sanctions and penalties in accordance with the conditions laid down in the contract;

6.4. In the case of violations that involve illegal activities or that may result in damage to the BBC, the violator shall be liable for damages and appropriate legal action shall apply, without prejudice to the conditions described in Sections 6.1, 6.2 and 6.3 of this policy.

7. Cases of omission

7.1. Omitted cases will be evaluated by the Information Security Management Committee for further consideration.

7.2. The guidelines set out in this policy and in other security standards and procedures are not exhausted due to continuous technological developments and the constant emergence of new threats. This is not an exhaustive list and it is the responsibility of the user of BBC information to adopt, where possible, other security measures in addition to those set out here to ensure the protection of BBC information.

8. Glossary

8.1. Threat: Potential cause of an incident, which could harm the BBC;

8.2. **Asset:** Everything that has value to the BBC;

8.3. **Information asset:** The BBC's intangible assets, consisting of information of any nature, including strategic, technical, administrative, financial, marketing, human resources, legal, and any information created or acquired through partnership, acquisition, licensing, purchase, or entrusted to the BBC by partners, customers, employees, and third parties, in written, oral, physical, or digital format, stored, transmitted, or transited through the BBC's computer infrastructure or through external infrastructure leased by the organization, in addition to documents in physical support, or electronic media transported inside and outside its physical structure.

8.4. **INFORMATION SECURITY MANAGING COMMITTEE– CGSI:** A standing multi-disciplinary working group, chaired by the BBC Board, whose purpose is to consider information security issues.

8.5. **Confidentiality:** Ownership of the BBC's information assets, which must not be provided or disclosed to unauthorized persons, processes or organizations.

8.6. **Control:** A safety measure adopted by the BBC to address a specific risk.

8.7. **Availability:** Ownership of BBC information assets, which must be accessible and usable on request by authorized parties.

8.8. **Information Manager:** An information user occupying a specific position who is assigned responsibility for one or more information assets created, acquired, processed, or placed under the responsibility of his or her area of activity.

8.9. **Information Security Incident** An adverse information security event or set of events that has a significant potential to affect BBC operations or compromise BBC information.

8.10. **Integrity:** Ownership of the BBC's information assets, which must be accurate and complete.

8.11. **Information security risk:** The impact of uncertainty on the BBC's information security objectives.

8.12. **Information Security:** Preserve the confidentiality, integrity and availability properties of BBC information.

8.13. **Information User:** Employees of any area of the BBC or third parties providing services to the BBC, regardless of their legal status, and other persons or organizations authorized to use BBC information assets in the course of their professional activities.

8.14. **Vulnerability:** Potential cause of an information security incident that could damage operations or compromise BBC information.

9. Reviews

This policy shall be reviewed annually or as understood by the Information Security Management Committee.