Corporate Policy - PTC	Issue Date: **5/30/2021**
Cybersecurity	Identification: **PTC.014**
	Version - 02 Review without amendments: **8/21/2023**
Approval: Executive Committee	Classification of information: **Public**

1. PURPOSE

Describe the guidelines that everyone can execute of cybersecurity principles and commitments of our business.

2. APPLICATION

It applies to the entire the Carrefour Brazil Group and stakeholders

3. ACRONYMS AND DEFINITIONS

Cybersecurity: damage prevention, protection and restoration of computers, electronic communications systems, electronic communications services, wired communications and electronic communications, including the information contained therein, to ensure their availability, integrity, authentication, confidentiality, and non-repudiation

Cyber incident: an occurrence that actually or potentially compromises confidentiality, integrity or availability of an information system or the information that the system processes, stores and transmits or that constitutes a breach or imminent threat of breach of security policies, security procedures or acceptable use policies.

Risks: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically as a function of the adverse impacts that would arise if the circumstance or event were to occur and the occurrence likelihood.

4. GENERAL GUIDELINES

Aligned with our Code of Ethical Conduct to further strengthen the Group's culture of integrity, building our image and the success of our business, we have prepared this Policy to define the standards and expected behaviors regarding Cybersecurity.

Digital transformation is one of the pillars of the company's global strategy. Therefore, we work continuously to ensure that the information we need to carry out our commercial activities continues to be protected by all business units belonging to the Group. Therefore, this Policy aims to establish the principles to achieve our security commitments, which are:

- Provide a safe digital environment, protecting information against misuse, loss or theft through robust Cyber Security practices;
- Manage risks while maintaining the ability to prevent, detect and reduce the likelihood of incidents;
- Comply with regulations and laws applicable to the topic.

Carrefour Group aims to continuously improve its cybersecurity capabilities to reduce potential risks considering the main commitments:

- Provide customers, their employees and business partners with a good experience when using our products and services, combined with a safe digital environment;
- Continuously seek synergy actions between the group's business units for operational excellence;

- Be recognized as a business facilitator through robust cybersecurity practices, being one of the main pillars for protection of data, information and operations;
- Be recognized as a Group that ensures the security of its information, that of its customers and business partners;
- Comply with regulations and laws applicable to the topic.

It is essential that we all know the importance of acting appropriately, avoiding the exposure of Carrefour Group to cyber risks, not only to comply with laws and regulations, but also to be aligned with the Group's purpose of being a great market transformative on digitalization, without forgetting corporate governance actions necessary to achieve this purpose.

Carrefour Group's Cybersecurity Policy is a document that is constantly updated. Therefore, reviews, changes and adaptations may be made at any time, as necessary, to ensure the topic evolution.

4.1 Cybersecurity Principles

Using information to carry out our activities is essential, whether electronically, when available in information systems, as well as during routine activities, such as a work meeting or exchanging messages through a mobile application. Except in cases where the information is explicitly declared as public, for all other situations, information related to Carrefour Group and its business units must be duly protected throughout its life cycle, from creation to deletion, passing through phases such as handling, modification, storage and transfer. Therefore, during the information life cycle, these fundamental principles must be considered:

- Confidentiality: Ensure that information is accessed only by authorized people;
- Integrity: Ensure that information is not unduly altered during its life cycle;
- Availability: Ensure that information are accessible whenever necessary;
- Traceability: Ensure that relevant transaction records are stored so that they can be checked when necessary.

4.2 Cybersecurity Guidelines at the Carrefour Group Brazil

Actions related to Cybersecurity must be carried out to protect business activities, and consequently the information of Carrefour Group, in a manner proportional to the potential risks. Below we present our main guidelines:

4.2.1 Cybersecurity Role

In each business unit, a cybersecurity role must be established, which will be responsible for actions to promote the topic in the unit, act continuously to reduce security risks, implement and improve controls, as well as act along with the Carrefour Group's cybersecurity structure in search of synergy and operational excellence.

4.2.2 Cybersecurity Governance

Cybersecurity governance is based on close collaboration between Cybersecurity teams of Global Carrefour Group and Carrefour Group Brazil (considering all their business units).

These units must generate, consolidate, and share on a recurring basis, indicators and information on their respective environments with the security teams of Carrefour Group Brazil, and when applicable, with Global Carrefour Group, to promote uniform, synergistic and continuous Cybersecurity Governance.

4.2.3 Cybersecurity Policy

The business units must regularly maintain, review, and comprehensively communicate their respective Cybersecurity Policy to all people with access to their systems and information. This policy must be in accordance with the other corporate policies of Carrefour Group, regulations and legislation in force in the country.

4.2.4 Cybersecurity Risk Management

The business units must regularly conduct assessments to identify potential cybersecurity risks. If identified, these risks must be assessed by the responsible teams and, when applicable, action plans must be assigned to monitor and reduce these risks to an acceptable level.

4.2.5 Cyber Incident Management

The Group's business units must have processes and procedures to manage cyber incidents in accordance with established guidelines. The main events/incidents must be communicated in a timely manner to the Group's Cybersecurity area.

4.2.6 Cybersecurity Culture

Business units must act continuously in the process of creating and maintaining a Cybersecurity culture, through awareness raising actions, guidance and training for all individuals who have access to their systems and information.

4.2.7 Security in Contracts

The business units must establish criteria and requirements related to cybersecurity in all contracts for their employees, providers, and business partners. These contracts must explicitly state the responsibilities of all parties involved, as well as comply with legal, regulatory, and contractual requirements that affect cybersecurity.

4.2.8 Information Protection

The business units must continually ensure and apply solutions and controls to protect information according to the classification and criticality criteria of their business. These must maintain their classification criteria in accordance with their respective particularities, if they comply with good market practices. Protection actions must be carried out during all the information life cycle.

4.2.9 Personal Data Privacy and Protection

The Business units must act in accordance with the Personal Data Privacy and Protection Policy established by Carrefour Group to protect personal data.

4.2.10 Identity and Access Management

The Business units must continually act to protect and properly manage identities and access to their systems and information. Access rights must follow the following standards:

- Have express authorization, and in the absence of this, not be permitted;
- Contain the minimum functionalities to perform the expected roles;
- Be duly authorized by their respective managers;
- Revoke promptly when necessary;
- Review periodically to identify potential deviations;
- Reinforce by automated control mechanisms;
- Assign individually to those responsible who will use it, having a unique and nominal identifier. Except in exceptional circumstances where there is no viable alternative.

4.2.11 Security in Business Critical Applications

The Business units must keep their inventories of critical business applications up to date. These applications must use strict security controls to reduce possible risks of loss of confidentiality, integrity and information availability.

These applications must regularly undergo risk analyzes and security tests to identify weaknesses that should be promptly addressed by an action plan.

4.2.12 Business Continuity

The Business units must establish, as well as regularly review and simulate their respective business continuity plans to prepare for possible events that may cause unavailability of their systems and services for an extended period, to maintain their operations business vitals.

4.2.13 Information Technology Equipment

The Business unit's cybersecurity teams must work together with their respective Information Technology teams, to protect their technological equipment used during the corporate information life cycle. These actions aim to:

- Ensure that business units have visibility over all equipment belonging to their technological ecosystem according to their respective importance to business operations;
- Ensure that the equipment have physical and logical security controls, implemented and operating;
- Ensure that the equipment are regularly subjected to security updates throughout their life cycle;
- Ensure that the equipment provide information necessary for traceability in case of potential security events;
- Ensure that the equipment and data contained therein are properly disposed, when applicable.

4. 2.14 Corporate Network Security

The Business units must maintain their security systems and controls active full-time to prevent potential unauthorized access to their communication networks, whether local, long-distance, voice, wired or wireless data networks. A set of solutions can be used to protect the corporate network and must be aligned with the cybersecurity principles, namely: confidentiality, integrity, availability, and traceability.

5. RESPONSIBILITIES

All employees, contractors and business partners must take the time to familiarize themselves with this Policy, read, understand, and adhere to the Cybersecurity Principles defined above, as well as other Policies and Procedures mentioned in this document. They must also ensure Carrefour Group's information and data protection continuously when using any information belonging to the Group during their work activities.

Whenever necessary, the Cybersecurity teams at Carrefour Group or business units will guide employees, contractors and partners on cybersecurity practices, who, in turn, must adopt them.

Communication channel:

In case of identification of a potential risk, cyber incident, report or guidance, our communication channel is available via email: csirt_br@carrefour.com

6. ASSOCIATED DOCUMENTS

Carrefour Brazil Group Code of Ethical Conduct, available at: https://ri.grupocarrefourbrasil.com.br/governanca-corporativa/estatutos-politicas-e-codigos/

Ethics and Social Code for Our Suppliers; available at: https://conexaoeticacarrefour.com.br/files/AF2_Digital_CodigoConduta_Fornecedores_PT_v2.pdf

Risk Management Policy, Data Protection and Privacy Policy, among other Corporate Policies of Carrefour Group Brazil, available at:https://ri.grupocarrefourbrasil.com.br/governanca-corporativa/estatutos-politicas-e-codigos/

7. DOCUMENT REVIEW AND UPDATE

This regulation must be reviewed every three years regarding adherence to Policies, Standards, Procedures, or whenever significant changes in the processes are identified.

8. CONSEQUENCE RULES

Deviations from regulations may lead to appropriate disciplinary measures, permitted under current legislation and the internal rules of the Carrefour Brazil Group.

In cases of non-compliance with these guidelines, reports can be made at: CONEXÃO ÉTICA: Website: conexaoeticacarrefour.com.br or Telephone: 0800 772 2975

The confidential channel - *Conexão Ética* is managed by an external and independent company, guaranteeing the whistleblower in good faith absolute secrecy and non-retaliation. All communication, to the extent permitted by law, will be treated confidentially, with all forms of retaliation against whistleblowers in good faith being prohibited.

9. REVISION HISTORY

DATE	VERSION	DESCRIPTION	AUTHOR
5/30/2021	01	Establishment	CISO
8/21/2023	02	Review and Layout Change	CISO and Internal Controls

10. RESPONSIBLE FOR THE DOCUMENT

RESPONSIBLE	VERSION	NAME	AREA	POSITION
Approval	02	-----------	Cybersecurity	CISO
Approval	02	-----------	Executive Committee	-----------