CORPORATE INFORMATION SECURITY POLICY

Intercorp Retail

InRetail Perú adopted Intercorp Retail's Corporate Information Security Policy

Modifications approved at Board of Director's Meeting of August 27th, 2026

.

1. OBJECTIVE

Establish policies that ensure the confidentiality, integrity, and availability of information and resources of the Business Units (UN) and the Corporate Unit (UC) that are part of Intercorp Retail and InRetail Perú Corp.

2. SCOPE

This policy applies to the Corporate Unit (UC) and all current and future Business Units (UN) of Intercorp Retail and InRetail Perú Corp.

3. DEFINITIONS

3.1. **Information Assets:** Anything that has value for the Business Unit (UN), such as electronic and physical information, software, hardware, data network, people, and services.

3.2. **Personal Data Bank:** An organized set of personal data, whether automated or not, regardless of the medium—physical, magnetic, digital, optical, or others—created by any means or modality of creation, formation, storage, organization, and access.

3.3. **Employee (Collaborator):** A person who provides a specific service within the facilities of the UN in exchange for remuneration.

3.4. **Confidentiality:** The characteristic of information that ensures it is known and used only by authorized individuals, and not disclosed to unauthorized persons, entities, or processes, nor used for unauthorized purposes. Personal data is a type of confidential information.

3.5. **Personal Data:** Any information about a natural person that identifies them or makes them identifiable through reasonably usable means.

3.6. **Sensitive Data:** Personal data including biometric data that can identify the holder; information regarding racial and ethnic origin; income; political, religious, philosophical, or moral opinions or beliefs; union membership; and information related to health or sexual life.

3.7. **Mobile Devices:** Portable electronic devices such as laptops, tablets, smartphones, etc.

3.8. **Home Office (VPN):** A portal that provides remote access to an employee's equipment to manage information and/or resources.

3.9. **Internet:** A global communication network that interconnects academic, corporate, and commercial networks.

3.10. **Supplier:** An external person or company responsible for providing goods or services to the UN for a given period.

3.11. **IT Resources:** Refers to software applications and computer equipment (hardware).

3.12. **Office Services:** Refers to services such as photocopying, printing, and scanning to optimize document management in offices.

3.13. **Network Services:** Services such as access to the internal network, instant messaging, internet, or directories.

3.14. **Spam:** The mass sending or receiving of unauthorized or unsolicited email messages.

3.15. **Data Subject:** The natural person to whom the personal data belongs.

3.16. **Processing of Personal Data:** Any operation or technical procedure, automated or not, that allows the collection, registration, organization, storage, preservation, elaboration, modification, extraction, consultation, use, blocking, deletion, communication by transfer or dissemination, or any other form of processing that facilitates access, correlation, delivery, or interconnection of personal data.

3.17. **Availability:** The characteristic of information that ensures it can be accessed and used when required.

3.18. **Integrity:** The characteristic of information that refers to its accuracy and reliability. Integrity aims to prevent unauthorized modifications, alterations, or destruction.

3.19. **Privacy:** The right to maintain the confidentiality of information, meaning to safeguard and protect it from unauthorized access.

4. RESPONSIBILITIES OF THE SERVICE PROVIDER

4.1. The Head of Cybersecurity is responsible for ensuring that this policy is communicated, complied with, and reflects the vision of Intercorp Retail.

4.2. All employees of the Business Units (UNs) and the Corporate Unit (UC) are responsible for complying with and enforcing this policy.

5. POLICY GUIDELINES

5.1. General Guidelines

- All data contained in an information asset is the property of the Business Units (UNs) and must therefore be protected, maintained, and properly managed to prevent it from being improperly altered or destroyed.

- The company’s information systems contain proprietary information and may contain confidential information. Therefore, all users are responsible for ensuring that data, information, and IT resources are used solely, exclusively, and directly to support the company’s practices and business.

- All devices used to protect, maintain the integrity, availability, and confidentiality of information must be considered private information, and therefore their disclosure to unauthorized persons (employees or third parties) is prohibited.

- Employees are required to keep confidential all documents, information, or material considered confidential information of the Corporate Unit (UC) or Business Unit (UN). As such, they may not publish, use, retain for themselves or third parties, commercialize, transfer, sell, share, donate, or carry out any form of transfer to third parties of any document, information, instrument, contributions, acquisitions, or knowledge including: general databases, personal data, software development, projects, strategies, management indicators, information related to sales, purchases, costs, negotiations, strategic partners, suppliers, employees, clients, and any other similar information.

- Access to the information mentioned above will only be granted to employees who are essential to fulfilling the relevant purpose in each case. These employees must use the information solely and exclusively for those purposes.

- Knowledge, contributions, and/or technologies developed during the employee's tenure remain the exclusive property of the UN.

- Information owners, in coordination with the Information Security area or its equivalent, must define mechanisms that guarantee the integrity, availability, protection against unauthorized access, and confidentiality of the information.

5.2. **Information Security Governance**

The Information Security and/or Cybersecurity Governance includes the following structure at both the corporate and business unit levels:

5.2.1. At the Corporate Unit (CU) level:

- CISO: The role of CISO (Chief Information Security Officer) will be held by the Head of Cybersecurity at Intercorp Retail, with corporate responsibility for information security. Their main responsibilities include:
  - Defining the corporate strategic plan for information security and cybersecurity to control or mitigate information security risks with critical impact on the operations of the Business Units (BUs).
  - Supervising and advising the BUISO role in the performance of their responsibilities.
  - Providing periodic reports, including key indicators, to the Vice Presidency of IT and relevant General Managements.

5.2.2. At the BU (Business Unit) level:

- BUISO: The role of BUISO (Business Unit Information Security Officer) will fall to the Manager, Head, Supervisor of Information Security, or their equivalents within the Business Unit. Their main responsibilities include:

- Executing and complementing the corporate strategic plan for information security and cybersecurity to control or mitigate information security risks with critical impact on their Business Unit.
- Conducting cybersecurity or information security risk analysis to determine the risk exposure of their Business Unit.
- Performing security audits and, if applicable, reviewing security action plans.
- Delivering periodic reports, including KRIs and KPIs, to the IT Directorate or Management of their Business Unit.

5.3. Operational Continuity

- The data processing and transmission environments provided by the Business Unit (BU) must have contingency and recovery plans, which should be reviewed and tested periodically.

- The Vice Presidencies, Management, and/or Directorates of the BUs must appoint an application owner, who will be responsible for defining and requesting from the IT, Systems, or equivalent department the necessary recovery times to ensure the operational continuity of their business processes.

5.4. Acquisition of Information Technologies and Contracts with Third Parties:

- All agreements with third parties must be technically and commercially approved, complying with the company's security standards as approved by the Cybersecurity, Information Security area, or their equivalents.

- Any procurement and/or contracting process for suppliers of assets and/or services must follow the guidelines referenced in the Security Policy for Suppliers:

  - Access to any company-owned information must be granted to the supplier only after the formalization and signing of a “Non-Disclosure Agreement” and/or Contract.
  - Access to technological resources and information systems will be assigned individually to the supplier after the formalization and signing of a “Non-Disclosure Agreement” and/or Contract.
  - If the contract has a direct relationship with information security risks that could compromise the confidentiality, integrity, and availability of the company's information, the approval of the Business Unit's Head, Manager, or Leader of Information Security must be obtained.
  - The Business Unit's Information Security Manager or Leader must assess the related information security risks and require mitigating controls for the service to be accepted. For example: cyber insurance, liability clauses for financial impacts resulting from materialized cyber incidents, global security certifications and standards, periodic cybersecurity audit results, among others.

5.5. Physical and Environmental Security

- All employees must wear visible identification. Security personnel must be notified immediately if an unaccompanied visitor is found.

- Employees who have been assigned a laptop must secure it with a security cable while in the office and are responsible for safeguarding the assigned technological assets.

- Employees who come to work outside regular business hours, on weekends, or holidays must be registered.

- Employees responsible for overseeing services involving third-party personnel or vendors must coordinate with the security guard or receptionist on duty to facilitate entry during business hours.

- All physical documents containing personal data must be stored in cabinets, filing units, or other storage items located in areas protected by access-controlled doors (e.g., key locks or equivalent mechanisms). These areas must remain closed when access to the documents is not required.

- A list must be maintained of authorized personnel who have frequent access to areas where physical documents containing personal data are stored. Any access by unauthorized individuals must be recorded, including at least the following information:
  - Person who accessed the information
  - Reason for access
  - Date and time of access
  - Personal data consulted

5.6. Access and Credentials

- Access credentials to IT resources are personal and non-transferable, and must only be used on the device assigned to the account holder.

- In case the employee has issues with their access, they must not reveal their passwords, as the specialists must perform troubleshooting with the employee's assistance or using administrator credentials.

- Any action taken using access credentials (username and password) will be the sole responsibility of the account holder; therefore, the use of another employee's credentials is strictly prohibited.

- The employee must choose a password to access systems and IT resources.

- It is recommended to use strong passwords—combinations of 8 or more alphabetic characters, numbers, and symbols (e.g., '$3gurid4d')—and to avoid passwords that are only words or meaningful numbers (such as names, cities, birthdates, ID numbers, phone numbers, or others).

- Unlock requests must be made solely by the account holder or the person in charge of their department, identifying themselves to the Service Desk.

- Employees must not allow others to use the computers assigned to them, unless they supervise the use while authorized IT Support personnel access the equipment physically or remotely.

- The creation and modification of access to network services and IT resources must be requested by authorized personnel to the Service Desk (or equivalent), including user data, which will be assigned according to their role or corresponding approval.

- Access for vendors or guests to the network and services of the Business Unit (BU) must be requested by an internal employee acting as the responsible party, stating the purpose, access level, and validity period.

- All accounts with inactivity exceeding 90 days will be deleted. Any exceptions must be reported to Information Security (or its equivalent), specifying the reason and approval by the department head. Reactivation will follow the same procedure as a new account.

- All accounts of terminated personnel will be deactivated and/or deleted. Any exceptions must be reported in advance to Information Security (or its equivalent), specifying the reason, validity period, and approval by the department head.

- The BU reserves the right to revoke system access privileges from any user whenever deemed appropriate.

- Employees must report access issues or incidents regarding IT resources to the Service Desk or its equivalent.

- It is strictly prohibited to collect, store, process, or share personal data of the BU's clients or prospective clients without authorization from the Commercial Management or its equivalent.

- It is strictly prohibited to collect, store, process, or share personal data of the BU's employees and job applicants without authorization from Human Development Management or its equivalent.

- It is strictly prohibited to collect, store, process, or share personal data of individual vendors of the BU without authorization from the Finance Management or its equivalent.

- It is strictly prohibited to collect, store, process, or share personal data obtained through the BU's video surveillance system without authorization from Administration and Operations Management or its equivalent.

5.7. Acceptable Use

Employees and third parties who provide services for the Corporate Unit (CU) and/or Business Units (BUs) must accept and follow the guidelines defined in the document "Corporate Acceptable Use Policy for Assets," whose main security guidelines are as follows:

5.7.1. Use and Protection of IT Resources and Assets

- In case collaborators need software and/or hardware, the person responsible for their area must formalize the request with the Service Center or its equivalent. Any request for new software must be reviewed by the IT Support area or its equivalent and authorized by the Information Security area or its equivalent.

- Collaborators must not execute, use, or install software from untrusted sources, without corporate licensing or free distribution rights, including software acquired personally by the collaborator, in order to prevent legal claims or the introduction of computer viruses.

- Collaborators must use the IT resources assigned by the Business Unit solely for work-related purposes.

- Collaborators must assume that all software owned by the Business Unit is protected by copyright and requires a valid license; therefore, it is not permitted to copy, transfer, disclose, or install the software on another computer.

- Collaborators who need to use a personal mobile device connected to the internal network must receive approval from the Information Security area or its equivalent and be reviewed by IT Support, who will apply the policies of the Business Units before granting access to the network.

- To move IT assets within the same site, approval must be obtained from the responsible parties in both the origin and destination areas, and support should be requested from the appropriate personnel. If the asset is to be transported outside the Business Unit's premises, the move must be coordinated with the IT area or its equivalent and accompanied by an approved shipment guide.

- Access to web repositories is only authorized for resources licensed by the company. Uploading information from the Corporate Unit or Business Unit to public web repositories is restricted.

- The transfer of personal data and other confidential information to any destination outside the physical premises of the Business Unit, whether within or outside national territory, will only proceed with the authorization of the area's responsible party and must use authorized transportation methods, taking the necessary measures to prevent unauthorized access, loss, or corruption during transit. Electronic data transmission must be carried out using secure encrypted protocols.

- Collaborators must request, in a timely manner, that IT Support delete any removable media (CDs, DVDs, external hard drives, USB flash drives) containing personal data once their use has ended.

5.7.2. Use of Office Services

- Employees must request printer configuration through the Service Center or its equivalent.

- Whenever a password is required for printing, employees must request it from the Service Center or its equivalent.

- It is the responsibility of each employee to immediately destroy any printed documents containing internal and confidential information that are no longer needed, using a disposal method that prevents handling, reading, or reuse of the information.

- The generation of copies or reproduction of physical documents containing personal data may only be carried out when necessary, with prior authorization from the area's responsible party, using UN equipment (printers, photocopiers, scanners, or other reproduction devices), and maintaining a record of the copies and authorized personnel involved.

- Original documents and copies must be removed from the equipment (printer, photocopier, scanner, or other reproduction device) immediately after the copying or reproduction process is complete.

- System configurations of the UN, whether on desktop computers, laptops, and/or mobile devices provided by the UN or personal ones, must be carried out exclusively by the IT Support area or its equivalent.

5.7.3. Use of Network Services

- Employees must not use network services for activities unrelated to their job responsibilities.

- Permanent Home Office requests must be approved by the respective Vice Presidency, Directorate, or Management and submitted to the Service Center or its equivalent.

- The use of devices that provide internet access is not allowed unless they have been provided by the IT department or its equivalent.

- The Business Unit (BU) reserves the right to monitor, through technological security tools and/or similar systems, from its private network and with respect for individuals' right to privacy, the use of the Internet and to restrict access to websites, tools, systems, and/or applications that are contrary to ethics, morality, applicable laws, or policies established by the Human Development Management department or its equivalent.

- Employees are responsible for the information stored on their devices assigned by the BU. Freely sharing folders is not permitted; appropriate permission levels (read, write, or modify) must always be maintained for the individuals or groups granted access. If users have questions about how to share their resources, they are encouraged to contact the Service Center or its equivalent.

5.7.4. Use of Email

- Employees must only use corporate email for communications and functions assigned to their job position.

- Employees are responsible for all activities carried out through their email accounts. Employees must not use corporate email for personal purposes or as a means of storing personal information.

- Employees must not use email to send chain messages, spam, music files, videos, or executable files.

- Employees must not open emails from suspicious sources. If such a case arises, it must be immediately reported to the Information Security team or its equivalent by forwarding the email as an attachment for proper review.

- Once the employment relationship with the employee ends, the manager and/or immediate supervisor may request access to the user's email account only if the justification is strictly necessary to meet work-related needs affected by the employee's absence. This activity must be reviewed and approved by the Business Unit (BU) Management and the BU's Information Security team, ensuring proper documentation and the use of traceability mechanisms to prevent unauthorized alteration or leakage of information.

5.7.5. Clean Screen and Desk Policy

- Employees must lock their computer screens whenever leaving their workstations, regardless of the duration of their absence.

- At the end of the workday, employees must ensure that all drawers are properly locked. Under no circumstances should confidential information—such as account credentials or passwords—be left unsecured, whether on the desk surface or stored inside unlocked drawers.

5.8. Personal Data Protection

- The provisions of this section are without prejudice to the fact that personal data are also subject to the other provisions of this document, unless otherwise expressly stated.

- The BU respects the principles of legality, consent, purpose, proportionality, quality, availability of recourse, and adequate level of protection, in accordance with the provisions

set forth in Law No. 29733 – "Personal Data Protection Law," its regulations, amendments, and other related standards.

- The processing of personal data, including its delivery or transfer to any third party, must be carried out only with the prior, informed, free, express, and unequivocal consent of the data subject, unless otherwise authorized by law.

- Personal data must not be used for purposes other than those for which it was collected.

- Personal data must be deleted when it is no longer necessary for the purpose for which it was collected, when the period for its processing has expired, when the data subject withdraws their consent, or when any other cause for cessation of processing arises.

- All contracts with suppliers involving the collection, storage, processing, or delivery of personal data must include a personal data protection clause, confidentiality, and the secure and complete deletion of the data upon the termination of the service.

- The BU's internal processes involved in the processing of personal data must be adequate and comply with the requirements and standards established by Law No. 29733 – "Personal Data Protection Law," including the fulfillment of formal obligations such as registration in the National Registry for the Protection of Personal Data of personal data banks and, where applicable, the reporting of cross-border data flows.

- The BUs must formally designate representatives for each specific database.

- The BUs must implement customer service channels responsible for processing and responding, in accordance with the law, to requests submitted by data subjects seeking to exercise their rights of access, information, rectification, objection, deletion, and others.

5.9. Continuous Improvement of Information Security

- The Business Units (BUs) and Corporate must periodically review and continuously improve their information security controls, processes, and systems to address evolving cyber risks, technological changes, vulnerabilities, and business needs.

- The Information Security, IT, Systems, or equivalent departments must monitor the effectiveness of information security measures through internal/external assessments, audits, incident analysis, vulnerability management, and testing activities, ensuring that corrective and preventive actions are executed when necessary.

- Lessons learned from security incidents, audits, risk assessments, and business continuity tests must be incorporated into the continuous enhancement of the information security management framework.

5.10. Compliance Monitoring and Audits

- Business Units (BUs) and Corporate must perform periodic assessments and audits to verify compliance with this Information Security Policy and the effectiveness of implemented controls.

- Identified findings must include action plans, responsible parties, and follow-up activities to ensure timely remediation and the continuous improvement of the information security framework.

6. REGULATIONS / RELATED DOCUMENTS

- Law No. 29733 – “Personal Data Protection Law”
- IRC-TI-PT008 Corporate Policy on Acceptable Use of Assets
- IRC-TI-PT007 Corporate Access Management Policy
- IRC-TI-PT005 Security Policy for Vendors

7. ANNEXES

Not applicable