Security mechanisms for privacy protection

Interbank policies and guides to protect the privacy and personal data of our clients

Compliance guide for the Personal Data Protection Law

According to the Personal Data Protection Law (Law 29733) and its Regulations (Supreme Decree 003-2013 -JUS), we have a compliance manual, which establishes the guidelines and obligations that we must comply with. It also contains the organizational structure, functions and the responsible areas for supervising proper compliance. Its primary obligations are the following:

- Guarantee the correct handling of personal data according to the purpose for which they have been provided.
- Guarantee our customers´ right of access, rectification, cancellation and opposition to the processing of personal data.
- Protect the security and confidentiality of the personal data provided, maintaining the privacy and security of the information.
- Obtain the informed consent of the personal data owners.
- Communicate the cross-border flow.

Information Security Policy and Guide

Likewise, we have an Information Security Policy, which establishes general guidelines approved by our Board of Directors and our Information Security Committee. This policy seeks to reduce information security risks that could affect the confidentiality, availability and integrity of information assets. It regulates measures for all the information processed, transmitted or stored by Interbank, digital or physical, of its clients, collaborators or third parties.

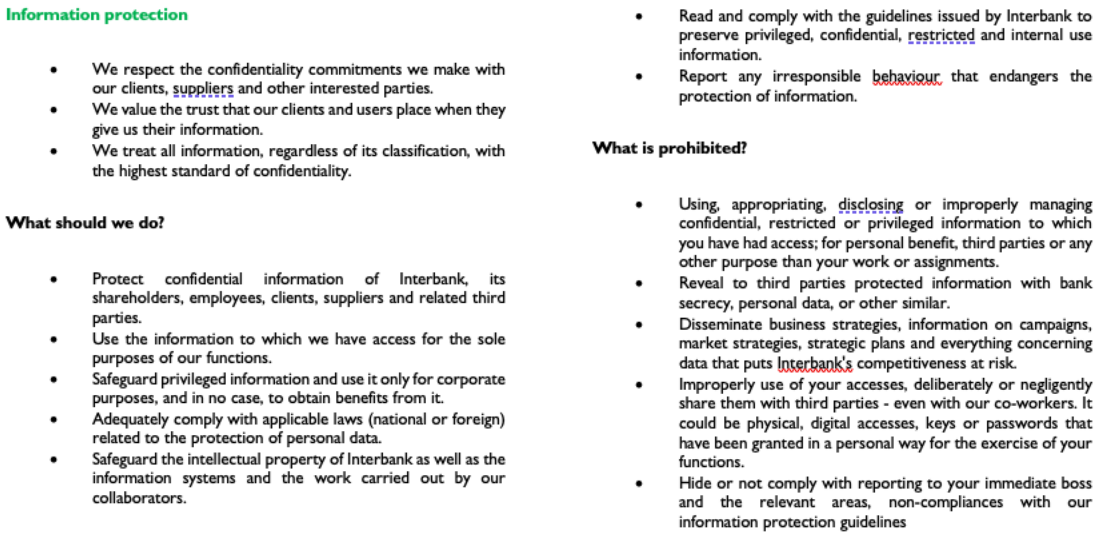
Interbank's Information Security Policy compiles the requirements established by the Personal Data Protection Law and the special regulations overseen by the Superintendency of Banking and Insurance (SBS: acronym for its name in Spanish) for financial operations as well as international standards of PCI.

Complementing this, we have developed an Information Security Guide to provide security guidelines for employees, suppliers, and partners (in general, third parties). The guide describes the organizational aspects of the information security management system, human resource security, asset management, access controls, encryption mechanisms, physical and

environmental protection of assets, the safety of operations, security in communications and infrastructure, acquisition, development and maintenance of systems, response to security incidents, among other topics.

Code of Ethics for employees

Similarly, in numeral 9.5 of our Code of Ethics for collaborators, the basic guidelines regarding the protection of information are emphasized, indicating the following:



Information protection

- We respect the confidentiality commitments we make with our clients, suppliers and other interested parties.
- We value the trust that our clients and users place when they give us their information.
- We treat all information, regardless of its classification, with the highest standard of confidentiality.

What should we do?

- Protect confidential information of Interbank, its shareholders, employees, clients, suppliers and related third parties.
- Use the information to which we have access for the sole purposes of our functions.
- Safeguard privileged information and use it only for corporate purposes, and in no case, to obtain benefits from it.
- Adequately comply with applicable laws (national or foreign) related to the protection of personal data.
- Safeguard the intellectual property of Interbank as well as the information systems and the work carried out by our collaborators.
- Read and comply with the guidelines issued by Interbank to preserve privileged, confidential, restricted and internal use information.
- Report any irresponsible behaviour that endangers the protection of information.

What is prohibited?

- Using, appropriating, disclosing or improperly managing confidential, restricted or privileged information to which you have had access; for personal benefit, third parties or any other purpose than your work or assignments.
- Reveal to third parties protected information with bank secrecy, personal data, or other similar.
- Disseminate business strategies, information on campaigns, market strategies, strategic plans and everything concerning data that puts Interbank's competitiveness at risk.
- Improperly use of your accesses, deliberately or negligently share them with third parties - even with our co-workers. It could be physical, digital accesses, keys or passwords that have been granted in a personal way for the exercise of your functions.
- Hide or not comply with reporting to your immediate boss and the relevant areas, non-compliances with our information protection guidelines

Contractual aspects with Suppliers

To guarantee the correct treatment of the information by our suppliers or partners, as well as compliance with the obligations derived from the Personal Data Protection Law, special regulations for financial operations and the international standards of PCI, we incorporate confidentiality clauses, information security and personal data protection into their contracts.

Likewise, in number 6 of our Interbank Supplier Code of Ethics and Conduct, we specifically reiterate the obligation of confidentiality from our suppliers and partners with the handled information, indicating the following: *"the supplier respects the confidential nature of the information to which its employees may have access, especially that related to Interbank´s business strategy and its*

clients, including information protected by bank secrecy, bank reserve and processing of personal data."