
	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 1 of 16

Table of content

1. OBJECTIVE	2
2. SCOPE	2
3. RESPONSIBILITY	2
4. AUTHORITY	2
5. DEFINITION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM	3
6. SPECIFIC CONTENT OF THE POLICY	3
7. CHANGE CONTROL AND APPROVAL CYCLE	16

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
		Version: 12
	Capability: 7.4 Information Security	Page: 2 of 16

1. OBJECTIVE

To establish a set of rules, procedures, and guidelines that outline how the organization manages and protects its sensitive data and information assets.

2. SCOPE

The guidelines of this policy are mandatory for all Teleperformance MAR employees (Colombia, Perú Guyana, Nicaragua, and Trinidad & Tobago), including direct and indirect employees, contractors, subcontractors, and suppliers, who provide support to the organization both from physical facilities and from teleworking.

3. RESPONSIBILITY

- **Senior Management** is responsible for ensuring the necessary resources and support.
- The ISMS Team is responsible to perform annual reviews of the Information Security Management System (ISMS) including all the documented information and related activities.
- Service providers, such as vendors, suppliers, and contractors, shall comply with the organization's policies.
- The communication and public relations team is responsible for coordinating the communication of the policy with internal and external stakeholders.
- Operation unit leaders are responsible for considering this policy on all aspects of their critical business functions and services.

4. AUTHORITY

- Approval: Senior Management.
- Review and update: Leader of the Information Security management system (*ISMS*).

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.









	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 3 of 16

5. DEFINITION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

An Information Security Management System (ISMS) is a systematic approach to managing sensitive information so that it remains secure. It involves establishing policies, procedures, and processes to manage risks and ensure the confidentiality, integrity, and availability of information assets.


6. SPECIFIC CONTENT OF THE POLICY

Pillars of the policy:

-  Confidentiality: Protecting sensitive data and information from unauthorized access or disclosure, both internally and externally.
-  Integrity: Ensuring that data and information are accurate, complete, and reliable, and that they are not modified or tampered with in any way.
-  Availability: Ensuring that data and information is available to authorized users when needed, and that they are not subject to downtime or disruption.
-  Accountability: Ensuring that individuals are responsible and accountable for their actions in relation to information security, and that appropriate measures are taken in case of non-compliance.
-  Compliance: Ensuring that the organization complies with applicable laws, regulations, and standards related to information security, such as TP Global, SOC 1, SOC 2, GDPR, HIPAA, PCI DSS, ISO 27701, and ISO 27001.
-  Risk management: Ensuring that the organization identifies, assesses, and manages information security risks, and that appropriate controls and measures are in place to mitigate these risks.
-  Continuity: Ensuring that the organization can continue to operate and provide services in the event of a disruptive incident, such as environmental, political risk, loss of utilities, technology-Related outages, and cyber-attacks.
-  Awareness: Ensuring that all employees and stakeholders are aware of the organization's information security policies and procedures and are trained on how to identify and respond to security threats and incidents.

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 4 of 16

6.1. Information Security Policies

6.1.1. Management Direction for Information Security

- 6.1.1.1. Information Security has a set of policies approved by management. These will be made available to internal and external parties.
- 6.1.1.2. Information security policies are reviewed annually or when significant changes occur to ensure their relevance and effectiveness.

6.2. Organization of information security

6.2.1. Internal organization

- 6.2.1.1. All information security responsibilities shall be defined and assigned.
- 6.2.1.2. Conflicting duties and responsibilities shall be segregated to reduce opportunities for unauthorized modification, inadvertent, and/or misuse of the organization's assets.
- 6.2.1.3. Contacts with relevant authorities and Special Interest Groups shall be maintained.
- 6.2.1.4. Contacts shall be maintained with special interest groups such as security forums and other related professional associations.
- 6.2.1.5. Information security shall be included from the beginning of each project.

6.2.2. Mobile devices


- 6.2.2.1. The organization shall follow the local and global policy and security measures related to the use of mobile devices.

6.2.3. Teleworking

- 6.2.3.1. The organization shall follow the local and global policies and procedures related to the organization's teleworking model.
- 6.2.3.2. Employees are responsible for protecting the organization's information and systems when working from home.

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 5 of 16

- 6.2.3.3. The organization will provide employees with regular training and appropriate awareness campaigns on information security in the context of teleworking.
- 6.2.3.4. Violations of this policy may result in disciplinary action, including termination of the contract.
- 6.2.3.5. Access to the organization's information and systems from a home environment shall be restricted to authorized personnel only.
- 6.2.3.6. External networks used to access the organization's information and systems shall be protected by appropriate technical controls, such as VPN, MFA, firewalls, and strong encryption.
- 6.2.3.7. The devices used to access the organization's information and systems from teleworking will be protected by EDR and antimalware, will be monitored, scanned for vulnerabilities, and regularly updated with the latest security patches.
- 6.2.3.8. The organization will regularly monitor and test its information security controls in the context of teleworking to ensure their effectiveness.
- 6.2.3.9. Information Security is responsible for implementing and enforcing this policy, as well as providing the resources and support necessary to maintain information security from teleworking.

6.3. Human resources security

6.3.1. Before employment


- 6.3.1.1. Background checks shall be performed on all candidates in accordance with relevant laws and regulations, business requirements, and the classification of information to which the employee would have access.
- 6.3.1.2. Contractual agreements with employees and third parties shall indicate their and the organization's responsibilities for information security.

6.3.2. During employment

- 6.3.2.1. All employees and contractors shall adhere to the organization's information security policies and procedures.

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 6 of 16

6.3.2.2. All employees and third parties shall receive regular appropriate training regarding the organization's information security policies and procedures.

6.3.2.3. There shall be a formal disciplinary process against employees who have committed an information security breach.

6.3.3. Termination and change of employment.

6.3.3.1. Information security responsibilities and duties that remain valid even after termination or change of employment.

6.4. Asset Management

6.4.1. Responsibility for assets

6.4.1.1. Assets associated with information and information processing shall be identified and maintained.

6.4.1.2. The inventory shall have the information of the owner of each asset.

6.4.1.3. Rules for the acceptable use of information and associated assets shall be maintained with information and information processing facilities.

6.4.1.4. All employees and third parties shall return the assets of the organization at the end of their employment, contract, or agreement.

6.4.2. Classification of information

6.4.2.1. Information shall be classified according to legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

6.4.2.2. The local and global procedure for labelling information shall be followed.

6.4.2.3. The organization shall comply with the documented procedures and policies related to information classification.


6.4.3. Media Management

6.4.3.1. Information classification procedures for asset manipulation shall be follow.

6.4.3.2. Information shall be securely deleted when it is no longer needed, using procedures documented by the organization.

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 7 of 16

6.4.3.3. Media shall be protected against unauthorized misuse, access or modification during transport or storage.

6.5. Access control

6.5.1. Organization's Access Control Requirements

6.5.1.1. An access control policy is in place and is reviewed periodically, depending on business and information security requirements.

6.5.1.2. Users will only be provisioned access to systems that they have been specifically authorized to use, based on the principle of least privilege.

6.5.2. User access management

6.5.2.1. There is a formal provisioning and de-provisioning process for registering and assigning access to users.

6.5.2.2. The formal provisioning and deprovisioning process will be applied to assign or revoke user access for all systems.

6.5.2.3. Privileged access will be restricted and controlled.


6.5.2.4. The assignment of secret authentication is controlled by the formal process.

6.5.2.5. Asset owners shall periodically review user access rights.

6.5.2.6. Access to employees and third parties shall be terminated and/or modified within 24 hours of receiving formal notice of termination of employment, contract, agreement, or role change.

6.5.3. User Responsibilities

6.5.3.1. It is the responsibility of users to comply with policies and best practices regarding secret user authentication.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 8 of 16

6.5.4. Access control to systems and applications

- 6.5.4.1. Access and functions to systems and applications shall be restricted in compliance with the access control policy.
- 6.5.4.2. A secure logon procedure shall be used where necessary in accordance with the access control policy.
- 6.5.4.3. The password management policy shall be applied to ensure quality passwords.
- 6.5.4.4. The use of programs capable of overriding system and application controls shall be restricted and controlled.
- 6.5.4.5. Access to the source code of programs and applications shall be restricted.

6.6. Cryptography

6.6.1. Cryptographic controls


- 6.6.1.1. There is a policy on the use of cryptographic controls for the protection of information.
- 6.6.1.2. The policy on the use of cryptographic keys throughout their entire life cycle shall be applied.

6.7. Physical and environmental security

6.7.1. Safe areas

- 6.7.1.1. Security perimeters shall be defined to protect areas that may contain sensitive, critical information, as well as processing facilities.
- 6.7.1.2. Secure areas shall be protected by adequate access controls that only authorized personnel are allowed entry.
- 6.7.1.3. Physical security shall be applied to the design of offices, rooms, and facilities.
- 6.7.1.4. Facilities shall have physical protection against natural disasters, malicious attacks, or accidents.
- 6.7.1.5. Established procedures for working in safe areas shall be applied.

TELEPERFORMANCE PUBLIC
information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 9 of 16

6.7.1.6. Delivery, cargo, and other access points shall be protected from unauthorized access. If possible, these areas shall be isolated from processing centers.

6.7.2. Equipment

6.7.2.1. Equipment shall be located to reduce risks of environmental threats and hazards, as well as opportunities for unauthorized access.

6.7.2.2. Equipment shall be protected from power failures and other power interruptions.

6.7.2.3. Power and telecommunications wiring shall be protected against interception, interference, or damage.

6.7.2.4. Equipment shall be maintained to ensure its continued availability and integrity.

6.7.2.5. Equipment can only leave the premises when prior authorization is obtained.

6.7.2.6. For information assets, the risks associated with being outside the premises shall be considered.

6.7.2.7. When necessary, all computers containing storage media shall be validated. To ensure that all confidential information has been properly disposed.

6.7.2.8. Users shall not leave their computers unattended without adequate protection.

6.7.2.9. Organization's clean desktop policy shall be followed.


6.8. Security of operations

6.8.1. Operational procedures and responsibilities

6.8.1.1. Operational procedures and responsibilities shall be available to those who require it.

6.8.1.2. Changes that may affect information security shall be monitored and documented.

6.8.1.3. The use of resources shall be monitored, and projections shall be made to adjust these to ensure the appropriate performance of the systems.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 10 of 16

6.8.1.4. Development, testing, and production environments shall be segregated to mitigate the risks of unauthorized changes, incidents, and failures.

6.8.2. Malware protection

6.8.2.1. Appropriate controls and tools shall be in place for detection, prevention, and recovery against malware-type threats.

6.8.3. Backup

6.8.3.1. Regular backups shall be available based on the criticality of the information and restore tests shall be performed to ensure the integrity of these copies.

6.8.4. Logging and monitoring

6.8.4.1. The organization shall have an event log centralized solution where security events, activities, exceptions, errors, user information, and other events can be found.

6.8.4.2. Installations and event logs shall be protected from tampering and unauthorized access.

6.8.4.3. Logs about privileged user activities shall be maintained, protected, and reviewed regularly.


6.8.4.4. An NTP server configuration shall be in place to ensure synchronization at the domain level.

6.8.5. Operating software control

6.8.5.1. When necessary, restrictions shall be applied to control the installation and execution of software on systems.

6.8.6. Technical vulnerability management

6.8.6.1. Regular vulnerability scans shall be performed. The results shall be reported in a timely manner to the responsible areas and these vulnerabilities shall be mitigated within the deadlines established in the organization's policies and applicable regulatory frameworks.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 11 of 16

6.8.6.2. The organization shall implement the necessary controls to restrict unauthorized software installation.

6.8.6.3. Software installations approvals shall be properly documented on the organization's ticketing system.

6.8.7. Information systems audit considerations

6.8.7.1. Technical tests that could produce interruptions in service shall be planned and agreed to minimize this risk.

6.9. Communications security

6.9.1. Network Security Management

6.9.1.1. Networks shall be managed and controlled to protect information, systems, and applications.

6.9.1.2. Security mechanisms, service levels and other requirements shall be identified and included in network service provision agreements.

6.9.1.3. Information services, users and information systems shall be segregated into separate networks.


6.9.2. Transfer of information

6.9.2.1. The security of the information shall be protected during the transfer, applying the practices established in the formal procedure of transfer of information.

6.9.2.2. Where necessary, agreements shall reflect the general conditions for the secure transfer of information between the organization and third parties.

6.9.2.3. Only secure channels shall be used for the transmission of information by electronic messaging.

6.9.2.4. Where necessary, the organization shall have confidentiality or non-disclosure agreements in place for the protection of information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 12 of 16


6.10. System acquisition, development, and maintenance

6.10.1. Security requirements for information systems

- 6.10.1.1. Information security requirements shall be included in new systems and/or improvements to existing systems.
- 6.10.1.2. All information transmitted over public networks shall be adequately protected against fraudulent activity, contract disputes, unauthorized disclosure, and modification.
- 6.10.1.3. All information shall be adequately protected to prevent incomplete transmission, incorrect routing, alteration, disclosure, duplication, or reproduction.

6.10.2. Security in development and support processes

- 6.10.2.1. For internal developments, the secure development policy applicable to computer programs and systems shall be followed.
- 6.10.2.2. Changes related to the development life cycle shall be monitored.
- 6.10.2.3. Be sure to complete the necessary tests, which ensure that there are no adverse effects or impact on the operations or safety of the organization.
- 6.10.2.4. Modifications to software packages shall be avoided and necessary changes shall be controlled.
- 6.10.2.5. Documenting and maintaining good practices and safe development principles in systems engineering shall be applied.
- 6.10.2.6. Security shall be properly established and protected in development environments and system integration throughout their lifecycle.
- 6.10.2.7. When necessary, third-party activities in system development shall be monitored.
- 6.10.2.8. Functionality and security testing shall be performed during development.
- 6.10.2.9. The established criteria for the acceptance of tests to new systems, updates and new versions shall be used.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 13 of 16

6.10.3. Test data

6.10.3.1. Test data shall be protected and controlled based on the related policy and controls.

6.11. Supplier Relations

6.11.1. Information security in supplier relationships

6.11.1.1. Information security requirements shall be agreed upon and documented to mitigate the risks associated with third-party access to the organization's assets.

6.11.1.2. Information security requirements shall be agreed upon and documented, so that third parties can access, process, store, communicate, or provide IT infrastructure components for the organization.

6.11.1.3. Information security risks associated with communications technology and supply chain services for products and/or services.

6.11.2. Management of the provision of services to suppliers

6.11.2.1. Third parties who provide services for the organization shall be regularly monitored, reviewed, and audited.

6.11.2.2. Changes shall be reviewed in the provision of services by third parties, including maintaining and improving existing information security policies and performing periodic risk reassessment.

6.12. Information Security Incident Management

6.12.1. Incident management and information security improvements


6.12.1.1. The incident response plan shall be followed where responsibilities and procedures are defined, to ensure optimal response to security incidents.

6.12.1.2. Timely notification of incidents shall be made, in accordance with the incident response plan and contractual requirements.

6.12.1.3. Employees and third parties have the responsibility to notify about any information or suspected information security weakness related to systems and/or services.

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 14 of 16

6.12.1.4. All information security events shall be reviewed before defining whether they can be classified as information security incidents.

6.12.1.5. Information security incidents shall be addressed in accordance with the applicable incident response plan and policies.

6.12.1.6. The principle of continuous improvement shall be applied based on previous incidents, to reduce the impact and probability of occurrence in future incidents.

6.12.1.7. Be sure to follow documented processes for the identification, collection, acquisition, and retention of information that could serve as evidence in relation to potential incidents.

6.13. Information security aspects of business continuity management

6.13.1. Continuity of information security

6.13.1.1. The necessary requirements shall be in place for the continuity of information security during potentially disruptive events.

6.13.1.2. Processes, procedures, and controls shall be established, documented, implemented, and maintained to ensure continuity of information security during potentially disruptive events.

6.13.1.3. Established controls, procedures and policies shall be validated periodically to ensure the effectiveness of information security continuity during potentially disruptive events.

6.13.2. Redundancies

6.13.2.1. Adequate redundancy in information processing facilities shall be considered to meet availability requirements.


6.14. Compliance

6.14.1. Compliance with legal and contractual requirements

6.14.1.1. All applicable legislative, regulatory, and contractual requirements for the organization shall be met.

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.

	POLICY INFORMATION SECURITY	Code: SI-PC-01
	Capability: 7.4 Information Security	Version: 12
		Page: 15 of 16

6.14.1.2. Appropriate procedures shall be applied to ensure compliance with applicable legislative, regulatory, contractual, intellectual property rights and software usage requirements for the organization.

6.14.1.3. Records shall be adequately protected against loss, destruction, falsification, Unauthorized access, and unauthorized release, in compliance with legislative, regulatory, and contractual requirements.

6.14.1.4. Adequate controls shall be in place to protect the information in accordance with applicable legislative, regulatory, and contractual requirements.

6.14.1.5. Where necessary, cryptographic controls shall be used in accordance with applicable legislative, regulatory, and contractual requirements.

6.14.2. Information Security Reviews

6.14.2.1. Annual reviews of information security shall be conducted and its implementation in the organization, to ensure compliance with controls, policies, procedures, and objectives.

6.14.2.2. Compliance with information security policies and any other applicable regulatory framework in the organization shall be reviewed annually.

6.14.2.3. Information systems shall be reviewed annually to verify compliance with information security policies and any other regulatory framework applicable in the organization.

7. CHANGE CONTROL AND APPROVAL CYCLE

DATE	VERSION	DESCRIPTION	APPROVAL CYCLE
08/05/2012	1	First version of the ISMS policy definition and objectives	Created: Ana Gomez Reviewed: Ivan Fernando Diaz Approved: Carlos Carrizosa
19/03/2014	2	ISMS Policy and Objectives Review 2013/2014	Updated: Ana Gomez Reviewed: Ivan Fernando Diaz Approved: Omar Ladino
07/04/2015	3	Document review and update	Updated: Ana Gomez Reviewed: Ivan Fernando Diaz Approved: Omar Ladino
09/02/2016	4	Document review and update	Updated: Ana Gomez Reviewed: Ivan Fernando Diaz Approved: Omar Ladino
14/08/2017	5	Document review and update	Updated: Ana Gomez Reviewed: Ivan Fernando Diaz Approved: Omar Ladino
30/08/2018	6	Revision and updating of the document (logo)	Updated: Ana Gomez Reviewed: Ivan Fernando Diaz Approved: Omar Ladino
29/04/19	7	Expansion of the scope of the policy and integration with Management Systems.	Updated: Gustavo Olaya Reviewed: Ivan Diaz- Ana Gomez Approved: Carlos Carrizosa
28/10/2020	8	Minor revisions and corrections to the text	Updated: Luis Gonzalez Reviewed: Alvaro Guerrero Approved: Carlos Carrizosa
13/09/2021	9	Minor revisions and corrections to the text	Updated: Luis Gonzalez Reviewed: Alvaro Guerrero Approved: Carlos Carrizosa
27/09/2022	10	Expansion and improvement of the content of the policy.	Updated: Jose Montañez Reviewed: Luis Gonzalez Approved: Claudio Esteves
18/01/2023	11	The scope in relation to teleworking is expanded.	Updated: Jose Montañez Reviewed: Luis Gonzalez Approved: Claudio Esteves
26/04/2023	12	Minor revisions and corrections to the text and translation of the Policy from Spanish to English.	Updated: Luis Gonzalez-Liliana Villar Reviewed: Javier Albiol Fernandez Approved: Claudio Esteves

TELEPERFORMANCE PUBLIC

information may be shared internally and to third parties without additional authorization from the owner of the information.