Version: 2

Approved on: 6/12/2014

Process responsible: Technology

Information Security Policy

- **Information Security Policy**

Information Security Policy

Establish all the organizational, technical, physical and legal measures required to protect information assets from unauthorized access, disclosure, duplication, interruption of systems, alteration, destruction, loss, theft, or misuse that may occur intentionally or accidentally.

This policy disseminates Celsia's information security objectives, which are achieved by applying their respective controls to manage an acceptable level of risk.

The Technology department is responsible for carrying out awareness-raising, communications, training and dissemination actions for the Information Security Policy.

Compliance with the Information Security Policy is mandatory. If employees, consultants, contractors and third parties violate these policies, the Organization reserves the right to take the applicable measures.

The policy's principles are part of Celsia's culture. Therefore, a commitment from Celsia's Steering Committee is ensured to disseminate, consolidate and comply with this policy.

Guidelines of the Information Security Policy

This policy is applicable to all employees, consultants, contractors and third parties that use information assets owned by Celsia.

This policy must be reviewed at least once a year or when required.

Security Organization

Through the Cybersecurity Leader, the Technology department is responsible for defining, coordinating and controlling the actions required to mitigate the risks associated with Celsia's information security and it will report to the Technology Risk Committee. This committee must have clearly established key staff in order to enforce and support the information security activities.

Classification and Control of Information Assets

Information must be inventoried, and the security risks and exposures must be identified to prevent financial or operating losses and/or loss of image for the Organization. Information must be classified as secret, restricted or general.

Secret and restricted information must be supported by a confidentiality or non-disclosure agreement when shared with third parties.

Acceptable Use of Assets and Resources

All employees, consultants, contractors and third parties that use information assets owned by Celsia are responsible for complying with and integrally adhering to the Acceptable Use Guidelines in order to rationally and efficiently use the assigned resources.

Information Security Risk Treatment and Management

Through the Cybersecurity Leader, the Technology department is responsible for analyzing the information security risks based on the business objectives and the Risk Management Policy, and *with the approval of the Technology Risk Committee.*

The leaders of each process are responsible for prioritizing and treating information security risks in accordance with the Organization’s risk appetite.

Projects or new acquisitions must identify the information assets, risks, threats, vulnerabilities and the management level in order to establish an information security plan.

Information Security in Human Resources

Human Resources must ensure that employees understand their responsibilities and are suitable for the roles for which they are considered; that they are aware of their information security responsibilities; and that they meet them.

Human Resources must protect the Organization’s interests as part of the process of changing or terminating the contract.

Physical Security and Environment

The Data Processing Center and ICT equipment room must be in areas that are physically protected against unauthorized access, damage or interference, and they must comply with physical security guidelines.

Information Access Control

In accordance with the classification of information assets, the Technology department must implement the applicable security measures to prevent unauthorized or fraudulent falsification, loss, leaks, consultation, use or access.

Control of access to sensitive data and information must be based on the principle of least privilege. This means that access will not be granted unless explicitly permitted.

Management of Information Security Incidents

All employees, consultants, contractors and third parties must note and report any weak point they have observed or that they suspect exists in the systems or services through the Services Help Desk.

Continuity Management of ICT Services

The Technology department must implement disaster recovery procedures to ensure the continuity of operations and availability of the critical ICT services.

Management of Telecommunications and ICT Infrastructure

The Technology department must ensure correct and safe operation of information and communication media processing facilities, through effective and efficient telecommunications and ICT infrastructure management.

IT Acquisition, Development and Maintenance

The Technology department must provide security measures in information systems from the *requirements phase, and these must be incorporated into the design, development, implementation and maintenance stages.*

The information systems acquired or developed by Celsia must meet minimum security requirements in accordance with good information security practices and this security policy. The design and operation of systems must adhere to commonly accepted security standards and current regulations.

Legal Regulations and Compliance

All technology infrastructure or services solutions must ensure that they are selected in accordance with external and internal, legal and regulatory contract terms, so that they comply with the legal systems that govern the Organization.

Exceptions

Exceptions from any compliance with the Information Security Policy must be approved by the Technology department, Administrative Human Resources Leader, Technology Leader or Celsia CEO. All exceptions to the policy must be formally documented, recorded and reviewed.

Breach of the Information Security Policy

Breaches of the Information Security Policy or its guidelines by employees will result in treatment measures for the information security incidents generated and could be subject to disciplinary action by Human Resources.

DEFINITIONS

For the purposes of this document, the concepts below are defined as follows:

- **Asset:** Any item that has value for the company.
- **Threat**: Potential cause of an unwanted incident that may cause damage to a system or to the company.
- **Confidentiality:** Feature that determines that the information is neither available nor to be disclosed to unauthorized individuals, entities or processes.
- **Technology Risk Committee**: The Technology Risk Committee must establish management and control criteria to implement the most appropriate mechanisms to protect Celsia's information, applying principles of confidentiality, integrity and availability of the information and of IT or other resources to support it in accordance with the Company's strategic planning.
- **Disaster:** Interruption of the capacity to access and process information through computers or other means necessary for normal business operation.
- **Availability:** This means that the information is available and usable when requested by an authorized entity.

- **Security guidelines:** These are approved products, procedures and measures that clearly define how the security policies will be implemented in a specific environment, taking into account the strengths and weaknesses of the available security features. These must be demonstrated in a document that describes the implementation of a guide for a specific hardware, software or infrastructure component.

- **Risk assessment:** The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

- **Integrity:** Safeguarding the accuracy and complete status of assets.

- **Security organization:** This is a function that seeks to define and establish a balance between the responsibilities and requirements of roles associated with information security management.

- **Policies:** Any intention or guideline that is formally expressed by Management.

- **Processes:** A business process is defined as each group of activities that receives one or more entries to create a value product for the client or for the Company itself (internal client quality concept). Typically, a business activity has multiple business processes in order to develop an activity.

- **Procedures:** Procedures are the operational steps that officers must take to achieve certain objectives.

- **Risk:** A combination of the probability of an incident and its consequences.

- **Information security:** Preservation of the confidentiality, integrity and availability of information. This may also involve other properties such as: authenticity, accountability, non-repudiation and reliability.

- **ICT:** Refers to information and communications technology.

- **Vulnerability:** Weakness in an asset or group of assets that could be exploited by one or more threats.

APPENDICES AND REFERENCES

- *ISO 27000.*
- *Information Security Guidelines and Appendices.*

TRACK CHANGES

VERSION	DATE	JUSTIFICATION OF THIS VERSION
1	6/12/2014	Document creation
2	10/30/2017	Change of document format
3	6/18/2019	Simplification of the policy, excluding the guidelines, documenting them as an appendix. Inclusion of words of the Celsia culture, such as: team, leader, etc.