Policy information security

Version:	4
Approval date:	02/03/2022
Responsible process:	Technology
Approved by:	Steering Committee

Information security policy

Celsia S.A. E.S.P.
www.celsia.com

1. Declaration

Establish all those organizational, technical, physical and legal measures necessary to protect information assets against unauthorized access, disclosure, duplication, system interruption, modification, destruction, loss, theft, or misuse, which may occur intentionally or accidental.

Through this policy, CELSIA Information Security objectives are disseminated, which are achieved with the application of their respective controls to manage an acceptable level of risk.

Technology is responsible for carrying out the awareness, communication, training and socialization actionsof the Information Security policy.

Compliance with the Information Security Policy is mandatory. If collaborators, consultants, contractors, third parties violate these policies, the organization reserves the right to take the corresponding measures.

The principles of the policy are part of CELSIA's culture, which is why a commitment on the part of CELSIA Steering Committee is ensured for the dissemination, consolidation and compliance with this policy.

2. Reach

This Policy is applicable to all collaborators, consultants, contractors, third parties, who use information assetsthat are property of CELSIA.

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

3. Policy guidelines

Organization for the Security

Technology through the Cybersecurity Leader is responsible for defining, coordinating and controlling the necessary management to mitigate the risks associated with information security in CELSIA and will report to the Technology Risk Committee, said committee must have the presence of key and clearly defined personnel, in order to comply with and support Information Security activities.

Classification and control of information assets

Information must be inventoried and security risks and exposures identified; In order to avoid financial, operational and/ or image losses for the organization, the information must be classified as secret, restrictedor general.

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

Acceptable use of information assets and resources

All collaborators, consultants, contractors, and third parties that use information assets owned by Celsia are responsible for complying with and accepting with integrity the Acceptable Use guidelines to give a rational and the resources allocated efficiently.

Information Security Risk Treatment and Management

Technology, through the Cybersecurity leader, is responsible for analyzing information security risks, based on business objectives and in accordance with 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 theorganization's risk appetite.

In projects or new acquisitions, information assets, risks, threats, vulnerabilities, and the management level must be identifiedto establish an information security plan.

Information Security in Human Resources

Human Talent must ensure that employees understand their responsibilities and are suitable for the roles for which they arebeing considered, are aware of their information security responsibilities and comply with them.

Human Talent must protect the interests of the organization as part of the process of change or termination of the contract.

Physical and Environmental Security

The data processing center and TIC, equipment room must be in areas physically protected against unauthorized access,damage or interference and must comply with physical security guidelines.

Information access control

Technology, in accordance with the classification of information assets, must implement the applicable security measures,depending on the case, in order to avoid adulteration, loss, leakage, consultation, use or unauthorized or fraudulent access.

Access control of data and sensitive information must be based on the principle of least privilege, which implies that accesswill not be granted unless it is explicitly allowed.

Cryptographic Controls

Technology must implement cryptographic controls to protect the confidentiality, authenticity and/ or integrity of the information.

Management of information security incidents

All collaborators, consultants, contractors, third parties must write down and communicate any weak point that they have observed or that they suspect exists in the systems or services through the Help Desk and Services.

TIC service continuity management

Technology must implement disaster recovery procedures to ensure the continuity of operations and the availability ofcritical TIC services.

Management of Telecommunications and TIC Infrastructure

Technology must provide the correct and safe operation of information processing facilities and communication media, through an effective and efficient Management of Telecommunications and TIC Infrastructure.

Acquisition, Development and Maintenance of systems

Technology must provide security measures in information systems from the requirements phase, and must be incorporated in 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 the systems must comply with commonly accepted safety standards and current regulations.

Compliance and legal regulations

Any service solution or technological infrastructure must guarantee that its selection is in accordance with the contractual conditions, legislation and external and internal regulation, for due compliance with the legal regimes to which the organization is subject.

Exceptions

Exceptions to any compliance with the Information Security Policy must be approved by Technology or the Leader of Human Talent and Organizational Solutions or the Leader of CELSIA. All exceptions to the policy must be formally documented, logged, and reviewed.

Non-compliance with the Information Security policy

Violations of the Information Security policy or its guidelines by collaborators will trigger treatment measures for Security incidents generated and could be subject to disciplinary actions by Human Talent.

4. Definitions

For the purposes of this document, the following concepts are defined:

- ***Asset:*** *Anything that has value to the company.*
- ***Threat:*** *potential cause of an undesired incident, which may cause damage to a system or company.*
- ***Confidentiality:*** *property that determines that information is not available or*

disclosed to unauthorized individuals, entities or processes.

- ***Technology Risk Committee:*** The *Technology Risk Committee must establish management and control criteria that allow the most appropriate mechanisms to protect CELSIA's information to be implemented, applying the principles of confidentiality, integrity and availability of the same and of the computer or other resources that support it, in accordance with the strategic planning of the company.*
- ***Disaster****: interruption of the ability to access information and process it through computers or other means necessary for the normal operation of a business.*
- ***Availability:*** *property that the information is accessible and usable by request of an authorized entity.*
- ***Security guidelines:*** *are approved products, procedures and metrics, which define in detail how security policies will be implemented for a particular environment, taking into account the strengths and weaknesses of the available security features. They must be reflected in a document that describes the implementation of a guide for a specific component of hardware, software or infrastructure.*
- ***Risk assessment:*** *process of comparing estimated risk against risk criteria given, to determine the significance of the risk.*
- ***Integrity:*** *property of safeguarding the accuracy and completeness of the assets.*
- ***Security Organization:*** *It is a function that seeks to define and establish a balance between the responsibilities and requirements of the roles associated with information security management.*
- ***Policies:*** *all intentions and directives formally expressed by management.*
- ***Processes:*** *a business process is defined as each set of activities that receive one or more inputs to create a product of value for the customer or for the company itself (concept of quality internal customer). Typically, a business activity has multiple business processes that serve to develop the activity itself.*
- ***Procedures:*** *Procedures are the operational steps that officials must take to achieve certain objectives.*
- ***Risk:*** *combination of the probability of an event and its consequences.*
- ***Information security:*** *preservation of the confidentiality, integrity and availability of the information, it may also involve other properties such as: authenticity, traceability (accountability), non-repudiation and reliability.*
- ***ICT:*** *refers to information and communication technologies*
- ***Vulnerability:*** *weakness of an asset or group of assets, which can be exploited by one or more threats.*

5. Attachments

- *TEC-N-2 Information Security Policy Guidelines.*

Change control

Version	Date	Justification of the version
1	06/12/2014	Creation of the document
2	10/30/2017	Change of document format.
3	06/18/2019	Simplification of the policy by excluding the guidelines documenting them as an annex. Inclusion of words from the Celsian culture such as: team, leader, among others.
4	03/02/2022	Change in the policy documentation format. Reference standards that were used as basis for politics. The domain of cryptographic controls is included.