Policy

Information Security

Public

Objective
Define, establish and protect the availability, integrity and confidentiality of all information related to our services.

Scope
Applies to all employees, consultants, visitors, who are involved in all Call Center Services S.A. de C.V. centers.

Department & Area
Information Technologies, Cybersecurity.

Responsible
IT Manager.

Elaborated by
Cybersecurity Analyst.

Document Control
Process Management Coordinator.

Reviewed by
Cybersecurity Analyst.

Approved by
IT Director.

Last Review	Effective Date	Version	ID
Oct20,2025	Oct23,2025	13	E_AIT-002_P

I. Policy

Introduction

At Call Center Services International we are committed to protecting information assets, ensuring their confidentiality, integrity and availability, in line with the **ISO/IEC 27001** standard. We implement an **Information Security Management System (ISMS)** that promotes continuous improvement, risk management and business continuity to ensure operational resilience.

Top Management explicitly endorses this system, ensuring legal, regulatory and contractual compliance, staff awareness and information protection throughout our operations, as well as a commitment to environmental protection through sustainable practices.

This policy is shared with vendors and contractors, fostering an aligned collaboration in data protection and the delivery of reliable and secure services.

NOTE: This policy is shared with clients and suppliers, promoting aligned collaboration in data protection and the delivery of reliable and secure services.

All information will be classified in the **Document Control and Records Procedure** in order to deliver information related to the internal operations of the Organization and its clients (internal / external), who are outside the scope of controlled access.

1. Information Security Responsible

Cybersecurity Team, in support with the Compliance Department and Information Technologies Department (IT), will have the responsibility of supervising, controlling, reviewing and applying the Information Security Policy. The rational use of CCSI resources should be conducted by the IT department including, but not limited to the following activities:

I. Ensure and implement at the Corporate level that employees are informed and comply with the policy.
II. Work altogether with the Operations Directors and Managers so that their personnel in charge can comply with the policy.
III. Provide follow-up when reviewing a report from any employee who becomes aware of any violation or suspected violation of this policy.
IV. Ensure that the information is classified according to the guidelines of **Document Control and Records Procedure.**
V. Validate that services provided are designed and implemented in compliance with the Information Security defined in this document.
VI. IT Department has primary responsibility and authority over all components of the IT infrastructure. All devices, applications, databases and other components must be aligned with the IT policies of the Organization.
VII. The Cybersecurity team shall review and manage all client practices that deviate from the guidelines of this policy, contacting and sharing the client's acceptance of responsibility before any implementation.
VIII. This policy must be reinforced to all collaborators every six months, through the GoCCSI Platform on a regular basis in order to ensure compliance with it.

NOTE: Business units or departments may establish additional procedures that are relevant to their operation. These procedures may provide more specific and / or restrictive details, as long as they do not conflict with this security policy.

2. Acceptable Use

The use of Corporate Email will be exclusive for issues directly related to the work assigned within the company, with total exclusion of personal issues or reasons unrelated to work, according to policy **Accounts and Digital Resources Access**.

All corporate emails must include the confidentiality notice in the signature of the body of the email according to **Corporate Image Policy**.

Information Technology tools and equipment provided by CCSI are for business proposal. For this reason, personal use of any computer, phone or software are not allowed based on with the stipulated on the **Password Policy**.

To ensure process traceability, establish guidelines for the appropriate use of official tools, and consult the protocols for information transfer, the provisions set forth in policy **Company Data** must be taken into account.

IT account and services will be provided by IT Department for only active employees in the Organization.

The Password Policy establishes the rules for the creation, distribution, safeguarding, termination and reclamation of the CCSI authenticity mechanisms based on the provisions of the **Password Policy**.

All the Technology Infrastructure has been implemented in such a way that it is not exposed to intrusion or random attacks. Always seeking to provide the appropriate maintenance to the infrastructure, with reference to the **Change Management Policy.**

All stationery, notebooks, cards, post-its, pens, pencils, markers and similar items are not allowed in the operations area unless properly authorized by the Client troughs **Non-Paper Authorization Waiver** and **Acceptance and Knowledge of Risk Format**. This is because we work in compliance with the **"Paperless and Clean Desk Policy"** environment as specified in **Corporate Policy** and **Company Data**, which establishes guidelines for information transfer and ensures process traceability.

Employees must use the company's internet access strictly for business-related purposes and in a responsible manner that ensures security and efficiency. Personal use should be minimal and must not interfere with work responsibilities. .

Accessing, transmitting, or downloading inappropriate, illegal, or high-risk content (such as gambling, adult material, or sites known for malware) is strictly prohibited. Guest networks are provided for convenience but must not be used to access restricted, high-risk, or non-business-related websites according to **Wireless Network Policy**.

3. Access Controls and Information Confidentiality

The Cybersecurity team will collaborate with Human Capital, Legal, and Information Technologies to ensure that access controls, legal compliance, and employee onboarding/offboarding processes are aligned with the security requirements established by the organization.

All new operational or administrative personnel, must sign a **Onboarding Package** and **Information Security Policy Acknowledgement** upon completion of their Induction Course, by means of which they undertake to adhere to and comply with the standards and criteria established by CCSI.

All new administrative and operations personnel must sign out the **Confidentiality Notice**, in addition to **Onboarding Package**.

All equipment and user systems will be managed and controlled through the **Access Control Procedure**, **Physical Access Control Procedure** and **Accounts and Digital Resources Access Policy.**

In the event that a provider requests access to the data center, it must be registered through our **Data Center Access Log**. Access must be provided by the activity responsible in accordance to the **Physical Access Control Policy**.

4. Electronics devices

All photography and video camera equipment (handheld or not) is strictly prohibited at CCSI, unless is authorized by Senior Direction of **CCSI by Photo-Video Permission** establishes in **Organization Chart** and requested through **Electronic Storage Device Follow Up.**

All external equipment, such as laptops and/or mobile devices; must be authorized requested as outlined in the **BYOD Bring Your Own Device policy** and **PIT-052_P BYOD Approval Procedure** using **BYOD Service Request (https://goccsi.net).** These records must be auditable and available on **GoCCSI database of approved and rejected devices.**

In the event that the Client's need warrants the use of devices other than those provided by CCSI, it must be authorized by the Client through **Acceptance and Awareness of Risk Format** and by the Operations Director through **BYOD Service Request**

The authorized user must sign **Responsive Letter of User Acceptance for the use of their own device.**

Internet access must be requested in accordance with **Acceptance and Awareness of Risk.**

Mobile devices electrical charging is strictly prohibited within the area of operations, with the exception of previously authorized laptops.

All equipment belonging to the Organization such as laptops, mobile telephony, headset, among others, must have a responsive letter signed by each person responsible of the equipment. Please refer to **IT Responsive Letter.**

All electronic devices with storage capacity are strictly prohibited inside areas like: Operations, Administrative, Training; according to **Corporate Policy**. Devices such as: MP3 players, sound recorders, portable USB memories, electronic pens, portable media devices, smartwatch and similar equipment. These can only be used in common areas and/or rest. During the working day they must be sheltered in their lockers or areas assigned for this purpose.

It is prohibited connect in the CCSI computer equipment any type of electronic storage device.

Information Technologies department are allowed to use and connect only electronic storage devices property of CCSI and only for work related purposes.

CCSI domain or Client / Account domain mail configuration will not be installed on mobile devices unless it is approved by the Client and the service request is created as indicated in **BYOD Approval Process**.

5. Hardware and Software Security Controls

CCSI will maintain an update nightly backup of all the information stored in the Organization's server systems. This includes, but is not limited to, files, spreadsheets, databases used by the Organization, any information required by the authorities, as well as information that needs to be recovered in the event of a disaster. Please refer to the **Backup and Restore Procedure.**

All required changes to IT equipment or software must be approved by IT. Please refer to the **IT Service Level Agreement.**

6. Incidents

All incidents must be reported, handled, managed, and resolved by adhering to the Incident Reporting Procedures. For all IT incidents please refer to **Incident Management Procedure.**

7. Penalties

The Information Security Policy will penalize in accordance with the following:

a) **Administrative Personnel**: Will be penalized according to the **Disciplinary Cycle and RIT Internal Employee Handbook.**
b) **Operational Personnel**: Will be penalized according to the **Disciplinary Cycle and RIT Internal Employee Handbook.**
c) **Professional Training Personnel (Interns)**: Will be penalized according to the **Disciplinary Cycle and RIT Internal Employee Handbook.**
d) **Visitors:** Will be addressed with a verbal warning.
e) **Contractors**: Will be addressed with a verbal warning in case of recurrence, the notice of contract termination will be given.
f) **Vendors:** It will be addressed with a verbal warning in case of recurrence, the notice of contract termination will be given.

Those employees who are reasonably suspected of having compromised the security of the information will be subject to the termination of the contract with the Organization.

Any employee who interferes with or refuses to cooperate with a corporate investigation of a violation of this policy will be subject to disciplinary action, up to and including termination of contract with the Company according to **Disciplinary Cycle**.

In the event that any Supervisor or Manager makes inappropriate use of IT resources, the sanctions mentioned in the **RIT - Internal Employee Handbook** will be applied. If the employee repeats the contract termination may apply according to **Disciplinary Cycle**.

All video and photography material that is published on **Public Websites**, as well as **Emails** without prior authorization, will be held accountable to the owner of the website or publication profile and will be subject to investigation, sanction and / or if the case merits it, contract termination with the Organization.

CCSI will collaborate with the police forces in their investigation efforts in the event of any violation of any state or federal law related to information security. In the event that CCSI suspects a violation of any law, CCSI may request the police forces to investigate the case.