Security Policies

IT Global Consulting S.R.L.

In accordance with the requirements of standard ISO/IEC 27001:2022 “Information security management systems – Requirements”.

---

1. Security Policies

1.1 Purpose, Scope, Users

The purpose of this Policy is to define the objectives, direction, principles and basic rules for the management of information security at IT Global Consulting S.R.L. (hereinafter referred to as **ITGC**).

This Policy applies to the entire Information Security Management System (ISMS), as defined in the ISMS Scope document.

The users of this document are all ITGC employees as well as external parties.

---

2. Information Security Management

2.1 Objectives and Measures

The objective of this document is to define the principles and guidelines to be adopted, as well as the roles, functions and responsibilities for implementing an effective information protection system, which must be complied with by all persons working at and for ITGC.

The goals to be achieved are:

- Safeguard the company’s interests.
- Ensure the protection of company information and the continuity of business activities, making sure that the required level of protection is implemented according to the criticality of the information to be protected.
- Ensure a homogeneous behavioural model.
- Ensure traceability of authorization processes and activities carried out for legal, tax and operational purposes.

2.1.1 Guiding Principles

Data and information security is based on organizational, procedural and technical measures that proactively protect against unauthorized access, destruction, loss, alteration or disclosure of data, and against processing that is not permitted or not consistent with the intended purposes.

The IT function provides the IT tools used to process data: in compliance with legal requirements and security needs, IT resources and data are made available only to authorized persons, and solely for purposes strictly related to their role and operational needs.

The security Policy is aligned with current best standards for information protection and safeguards data according to the following requirements:

- **Integrity**: property of safeguarding the accuracy and completeness of assets.
- **Confidentiality**: property that information is made available or disclosed only to authorized individuals, entities or processes.
- **Availability**: property of being accessible and usable upon request by an authorized entity.

The following guiding principles apply:

1. All information security standards must be implemented and their adequacy and reliability periodically verified.
2. Access to systems, applications and information must take place through user authentication. Access must only be authorized to the extent necessary for the user's role.
3. Exceptions and changes must be authorized in advance and recorded.
4. The Owner of the information is responsible for access authorizations, ensuring that access is removed when it is no longer needed and periodically verifying its adequacy.
   The responsibility for administering access rights must be clearly defined and kept separate from that of the users who obtain authorization and are subject to periodic reviews.
5. Physical and logical access controls must be implemented for all systems/processes containing the company's information assets.
6. All systems and applications must be able to produce appropriate logs of activities carried out. Logs must be activated through dedicated procedures and related authorizations.
7. The nature of the controls implemented depends on the assessment of the criticality of systems, applications and company data. High criticality requires controls with a higher level of security. Criticality analysis is mandatory for each project.
8. All activities involving system/application/information management must be performed with the minimum level of privilege required to perform the activity. Development/Test and Production environments must be segregated.

9. All information, applications and systems must be restorable in the event of malfunction.
10. All information, applications and systems considered critical for the business must be restorable in the event of disaster.
    A configuration document for each environment must be prepared and kept up to date.
11. External network connections may only be established by authorized persons or companies.
    The content of transmissions must comply with company requirements based on the criticality level of the data.
12. All Suppliers who process information that is sensitive to the business must sign an agreement requiring them to keep confidential all information not relevant to them that is obtained while performing their activities.
    Applicable laws and regulations in the countries where activities are carried out must be respected.

2.2 Activities and Methodologies

Applying the security criteria and Guiding Principles requires activities of analysis of the company information assets and identification of the controls to be implemented.

A review of the Risk Assessment is carried out at least once per year. In the event of the addition of new services, a risk analysis report is prepared in advance, which defines the guidelines for the correct delivery of the service.

2.3 Risk Analysis

Risk Analysis aims to determine the exposure to risk of company resources (systems, applications and information assets) according to probability and significance parameters.

The chosen methodology must allow the risk to be assessed in terms of the vulnerability of the resource, the threats to which it may be exposed and the impact on the business.

2.4 Risk Management

Risk Management aims to define the strategy for managing the identified risks, identifying existing controls and those to be implemented.

The activities planned for the protection of information are divided into two types of intervention, called **protection domains**:

- **Prevention and control domain**, which includes identification of potential attacks on all information through a careful risk analysis and the implementation of appropriate countermeasures.

- **Emergency domain**, which includes all activities aimed at ensuring, in the event of disastrous events, the recovery of business processes within predefined times and of the information systems supporting them.

2.5 Roles and Responsibilities

To achieve the above goals, ITGC has identified internal organizational units or roles responsible for defining, implementing and maintaining information protection measures and other related regulatory obligations.

2.5.1 Chief Executive Officer

The Chief Executive Officer promotes the implementation and application of an adequate information protection system.

He delegates the implementation, control and enforcement of protection measures to the roles identified below.

2.5.2 ISSO (Information System Security Officer)

The ISSO is a role that works operationally with IT and HR at ITGC and has the following responsibilities:

Technical and Operational Compliance

- **Implementation of Controls**: key role in translating security policies into effective technical controls. This includes configuring firewalls, implementing access management systems, installing antivirus and antimalware software and configuring logging systems.
- **Continuous Monitoring**: supervises security systems (e.g. SIEM – Security Information and Event Management) to detect suspicious activities, anomalies or potential violations. Analyses system logs to identify attack patterns or non-compliant behaviours.
- **Patch and Vulnerability Management**: responsible for coordinating vulnerability scanning and ensuring that security patches are promptly applied to servers, workstations and applications, reducing the organization's "attack surface".

Security Incident Management

- **First Responder**: when a security incident occurs (e.g. ransomware attack, intrusion, data breach), the ISSO is the first to intervene, acting to contain damage, isolate compromised systems and collect forensic evidence.
- **Investigation and Analysis**: conducts technical investigations to understand root cause, impact and how the incident was carried out.
- **Support to the Response Team**: works closely with the ISMS Manager and other teams (e.g. IT, Legal) to implement corrective actions and restore services securely.

Systems and Network Security

- **System Hardening**: configures the security of servers, network devices and endpoints (e.g. laptops) to make them more resistant to attacks.
- **Privileged Account Management**: controls and monitors the use of administrative accounts, ensuring they are used only when strictly necessary.
- **Data Protection**: applies technical measures to protect data, such as encryption (data at rest and in transit) and Data Loss Prevention (DLP).

Technical Advisory and Training

- **Security in Development (DevSecOps)**: collaborates with software development teams to integrate security requirements in the early stages of projects (security by design).
- **Technical Training**: trains IT and technical staff on security best practices, correct use of security tools and incident response procedures.
- **Supplier Assessment**: provides technical input in the selection of IT service providers, assessing their security measures and compliance with company standards.

2.5.3 Users

Users are individuals who, with a specific authorization profile, process information subject to classification within the protection system.

Users are responsible for implementing both technical and organizational measures as required. To that end, users are supported by internal rules and the relevant company structures.

Each user has the following individual responsibilities:

- Safeguard all information created, used or acquired in the performance of their duties, during and after their employment at ITGC, including protection from unauthorized disclosure, modification, compromise and destruction.
- Comply with this Policy and any associated guidelines and procedures in all activities involving company information or related to it.
- Comply with all laws and regulations relating to information created, used or acquired in relation to their duties (e.g. copyright laws, software licenses, etc.).
- Use company IT and processing resources exclusively for business needs, in order to ensure an adequate level of security and system performance, and refrain from illegal, unethical, unauthorized or harmful use (e.g. chain e-mails, games, pornography, use of unauthorized software, etc.).

- Refrain from any unauthorized use of company information and of any other information residing on ITGC communication or processing resources.
- Use all security mechanisms provided to protect company information stored on communication resources and computers.
- Report any doubt or concern regarding information security to:
    - their Line Manager or delegate;
    - the ISSO.

Non-compliance with the above rules by employees may lead to disciplinary measures of varying severity, including possible legal action.

2.5.4 Suppliers and Consultants

Suppliers and consultants have the following responsibilities:

- Safeguard all company information created, used or acquired in the performance of their duties, during and after the period in which they work with ITGC, including protection from unauthorized disclosure, modification, compromise and destruction.
- Access processing resources only with specific authorization, using personal user IDs and access passwords.
- Maintain a secure and controlled (physical and logical) environment for all company information.
- Access company information only in accordance with granted authorizations.
- Use company IT and processing resources exclusively for business needs, in order to ensure an adequate level of security and system performance, and refrain from illegal, unethical, unauthorized or harmful use (e.g. chain e-mails, games, pornography, use of unauthorized software, etc.).
- Notify security managers of any known or suspected issues relating to the security of information processed.
- Comply with rules on physical access to company sites, particularly with respect to restricted areas.
- Store paper and/or digital documents containing confidential data according to the relevant Guidelines.
- Use specific written authorizations to bring data and software into or out of ITGC sites.
- Take all necessary measures to prevent the introduction and spread of malicious software (e.g. viruses, worms, etc.) that could damage ITGC’s information assets, as provided for in current Guidelines.

Internal self-assessments and audit activities are carried out based on the defined Risk Assessment or specific needs within the information protection plan.

2.6 Self-Assessment and Audit Activities

Self-assessment and audit activities aim to:

- Ensure ongoing verification of the internal control system and the expected level of operational security, including at outsourcers, and promote measures to improve effectiveness.
- Monitor how IT systems are used by internal and external users to verify compliance with regulations and identify anomalous situations of potential risk.
- Systematically verify the robustness of the protection system by performing penetration tests on systems, networks and applications.
- Promptly inform the ISSO and IT Manager about any issues and/or criticalities of general relevance.

Audit activities may be requested by the ISSO and/or commissioned to specialized external companies.

2.7 Information Handling

All information concerning ITGC is considered the property of the company.

For this reason, it must be protected against unauthorized disclosure, modification, compromise and destruction.

These protections are implemented according to the **need-to-know** principle: classified information must be shared only with those who have a legitimate business need to access it.

The criteria for determining the classification level of information derive directly from:

- The risk of damage to competitiveness in case of erroneous or malicious disclosure to parties outside the company.
- Laws/regulations on trade and industrial secrets.
- Laws/regulations on personal data protection.

Systems, applications and the company's information assets must therefore be classified according to parameters of **criticality**, identifying the value of information for the business. The criticality level expresses the required degree of protection.

In line with the guideline MAN-ISMS-001 "Information Classification", the following information criticality levels and related handling rules are defined: **Public, Internal Use, Restricted, Secret / Confidential**.

Depending on the degree of confidentiality and exposure to risk, minimum measures must be adopted to protect information and may be strengthened based on the specific risk analyses carried out.

Confidential company information in paper form must be protected in the same way as information on electronic media; the confidentiality level must be clearly indicated on each page of the document containing it.

---

3. Information Security Elements in Personnel Management

The following information security requirements must be applied in the management of staff performing work activities.

3.1 Work Rules and Staff Recruitment

In order to reduce the risk of human error, theft, fraud or misuse of company information, it is necessary that:

- Job descriptions define roles and responsibilities regarding information security management.
- Employment conditions define the employee's responsibilities as regards information security.

3.1.1 External Personnel

All non-employees (consultants, interns, employees of third-party companies) working on behalf of ITGC must be informed of company policies, standards and procedures regarding security.

Any violation of security policies and standards may result in termination of the contractual relationship and potential damages, between the external personnel and/or its company and ITGC.

3.1.2 User Training

Users must receive appropriate information on policies, standards, guidelines and procedures relating to information security issues.

3.1.3 Incident or Malfunction Reporting

Users must receive appropriate information on policies, standards, guidelines and procedures relating to information security issues.

- Incidents must be reported to the appropriate personnel and then managed according to known procedures, through a proven system and within short timeframes.

- Any weakness, or suspected weakness, in security controls must be reported. Reports must cover all types of incidents, including: denial of service, data inaccuracies, confidentiality breaches, intrusions on systems or workstations, spamming and chain letters, etc.
- All software malfunctions must be reported.
- Violations of security rules may lead to disciplinary sanctions commensurate with the seriousness of the violation.

3.2 Physical Security

The following rules apply to the management and implementation of physical and environmental security.

3.2.1 Secure Areas

Physically protected areas must have a clearly defined perimeter, possibly through the use of barriers.

Secure areas must have controlled access. Only authorized personnel may enter using the dedicated app, and access is recorded.

Additional security measures must be provided for sites requiring specific security levels.

3.2.2 Equipment Security

All computers and communication devices are located in protected areas.

Information requiring special protection is segregated from other information to increase overall security.

The risks related to the following factors must be assessed: fire, smoke, water, dust, vibration, chemicals, power outages and radiation. Following this assessment, appropriate countermeasures must be identified.

Computers and communication devices necessary for business continuity are protected against voltage fluctuations or power outages by uninterruptible power supplies.

Power and telecommunication lines are protected to prevent interception or damage.

Equipment must be properly maintained by authorized personnel, in accordance with the vendor’s instructions.

Security controls must also be applied to equipment used outside company sites (particularly mobile phones and smartphones).

Data must be erased before devices are disposed of or reused.

Paper documents and removable digital media must be stored in appropriate secure locations.

Workstations must be locked when not in use.

Equipment, data and software must not be taken off-site without prior written authorization.

---

4. Operating Procedures

4.1 Operating Procedures and Responsibilities

Security procedures are operational instructions that build on and extend the indications in this Security Policy.

Documented procedures must be in place for configuring and managing communication devices.

Any changes to technological infrastructures (hardware and software) must be controlled and documented.

Responsibilities and procedures for incident management must be defined to ensure an effective and prompt response.

Separation of duties is required to minimize risks due to abuse or negligence.

Development/Test environments must be separated from the Production environment. In particular, authentication procedures must be clearly distinct.

Using an external service for managing processing and telecommunication systems must be accompanied by a security impact assessment and the adoption of appropriate security measures.

4.1.1 Protection Against Malicious Software

Antivirus systems and appropriate prevention and user awareness measures must be adopted.

4.1.2 Network Management

The following security measures are required for network protection:

- Procedures and responsibilities must be defined for the management of network devices.
- Controls must be defined for protecting data over public networks and for protecting connections.
- Activities of host and network management must be coordinated.

4.1.3 IT Device Security Management

A procedure must be in place for managing and controlling removable devices.

The disposal of computers and removable devices must be controlled.

System documentation must be protected from unauthorized access.

4.1.4 Exchange of Information and Software

When exchanging data and software between different organizations, appropriate agreements must be made, particularly regarding security measures.

When transporting computers, appropriate precautions must be taken to prevent loss, damage or misuse.

Special security controls must be applied to electronic data exchange in order to prevent interception or modification.

Adequate measures must be taken to prevent risks associated with the use of e-mail.

4.2 Logical Access Management

Access to IT resources must always be controlled according to the confidentiality and criticality of information for business operations. Each user authorized to access data and IT resources is subject to an authentication process that, at a minimum, requires entering a user ID and password defined in accordance with established rules.

4.2.1 User Access

Access to ITGC's information assets must be managed and controlled based on business needs and security requirements.

ICT staff managing logical access to systems must comply with the rules set out in this paragraph.

Data Owners, together with their ICT contacts, must:

- Define and maintain authority levels for user access in their area of responsibility.
- Verify user authorizations for access to information/applications, including external access.
- Manage changes to access profiles when a user changes job, leaves the company or no longer needs access for any reason.

The main rules relating to access to company information systems are:

- Access to systems must be personal and organized by user groups according to documented business requirements.
- Assignment and management of access and passwords must follow a defined process.
- System access rights must be verified and controlled regularly (every 3–6 months depending on privileges).
- Users must only have access to services for which they are authorized.

- Networks must be segmented into logical domains consistent with the company structure. Access between domains must be controlled.
- Each user must have a unique identifier.

4.2.2 Access to Telecommunication Networks

Access to internal and external networks must be controlled, in order to ensure that users accessing networks and network services do not compromise system security, by:

- Using appropriate authentication mechanisms for users and communication devices.
- Controlling user access to network services.

4.3 System Development and Management

Security must be an integral element in the development and management of information systems.

During system development and management, the following activities must be carried out:

- Verification of compliance with security rules.
- Use of change control procedures for system configuration.
- Controls on development procedures for software produced by third parties (e.g. licenses, quality plans, audit activities, etc.).

When developing new applications and managing existing systems, reference must be made to data classification (see section 2.7 “Information Handling”), on the basis of which appropriate data protection levels must be defined (e.g. use of encryption).

4.4 Acceptable Use of Company Assets

This Policy defines the rules and expectations for proper and responsible use of all company assets, including, by way of example but not limited to, hardware, software, IT systems, networks, mobile devices, vehicles, tools and facilities. The objective is to ensure information security, protection of company assets, legal compliance and operational efficiency.

This Policy applies to all employees, collaborators, interns and any other person who has access to or uses company assets, regardless of their position or type of relationship with the company.

General Principles

- **Primary Use for Business Purposes**: Company assets are provided primarily to facilitate the performance of work duties and to support the company’s business objectives.

- **Limited and Responsible Personal Use**: Limited and reasonable personal use is tolerated, provided it does not interfere with work responsibilities, does not compromise security, does not incur significant costs for the company and is not illegal or contrary to company values.
- **No Expectation of Privacy for Business Use**: The company reserves the right to monitor the use of its assets and systems for legitimate purposes such as security, performance management, legal compliance and troubleshooting. There is no expectation of privacy for data or communications generated or stored on company assets.
- **Individual Responsibility**: Every user is responsible for the protection and proper use of the company assets entrusted to them.

Acceptable Use (Examples)

- Performing authorized work activities.
- Internal and external communications related to work.
- Accessing company resources and applications needed to perform job responsibilities.
- Minimal and reasonable personal use such as brief personal communications, occasional online purchases not related to work, or web browsing, provided it does not hinder work, does not violate this or other company policies and does not cause costs or risks for the company.

Unacceptable Use (Examples)

Any use of company assets that is:

- **Illegal**: activities that violate laws or regulations (e.g. unauthorized download or sharing of copyrighted material, unauthorized access to third-party systems, fraudulent activities).
- **Unethical or Immoral**: obscene, offensive, discriminatory, sexually explicit, violent or threatening content.
- **Harmful to the Company or Third Parties**: distribution of viruses, malware or other cyber threats; unauthorized disclosure of confidential or proprietary information; activities that damage the company's reputation.
- **Excessive Personal Use**: usage that interferes with job performance, consumes significant resources (e.g. bandwidth) or causes unacceptable costs to the company.
- **Non-Work Games and Entertainment**: installation or use of games, excessive streaming of video or music, or participation in chat rooms / non-professional forums during working hours or in ways that consume company resources.

- **Security Violations**: attempts to bypass security controls, install unauthorized software, change system configurations without permission, share passwords or credentials.
- **Political or Personal Commercial Activities**: use of company assets for political activities not authorized by the company or to promote personal commercial interests.

Information Security

All data and information created, processed or stored on company assets are considered the property of the company, unless otherwise stated.

All company information security policies must be respected, including data protection, password management and security incident reporting.

Company assets, particularly portable devices, must be adequately protected from loss, theft and unauthorized access (e.g. through strong passwords, encryption, not leaving them unattended).

---

5. Business Continuity

5.1 Business Continuity Management

Critical business processes essential for the company's survival must be safeguarded through specific emergency plans that include all activities required to restore the information system, in order to minimize financial loss in the event of a disaster of any kind: flooding, fire, terrorist attack, etc.

As indicated in the Policy "Guidelines for the Protection of Company Information", the emergency domain protection plan consists of two components:

- **Disaster Recovery Plan**, which identifies IT resources related to critical business processes and their recovery procedures.
- **Business Continuity Plan**, which provides for:
    - identification of critical business processes and assessment of the impact of different types of disasters on those processes;
    - appropriate risk analysis;
    - definition of plans to maintain or restore business processes within set timeframes in case of disruptions or failures;
    - implementation methods and identification of those responsible for executing all actions, with related priorities;
    - regular updating and testing to ensure effectiveness.

Management plays a key role in properly defining emergency plans and involving staff in the functional and organizational tests required by the plans.

5.2 Compliance

The design, development, use and management of information systems must comply with laws and company regulations.

To this end:

- For each information system, legal and contractual requirements must be defined and documented.
- Appropriate measures must be taken to comply with contractual obligations regarding copyright.
- Records required for legal proceedings must meet legal requirements.
- Appropriate measures must be taken to avoid loss, falsification or destruction of data/documents with legal value.
- Appropriate measures must be taken to protect personal data.
- Necessary precautions must be taken to prevent unlawful use of processing and communication resources.

5.3 Sanctions and Control Activities

Anyone who:

- fails to adopt the precautions set out in this Security Policy;
- does not comply with security instructions given by the relevant roles;
- openly violates the protection measures set out in the information protection system;

is subject to sanctions, imposed by the relevant company structures, proportionate to the seriousness of the violation.

ITGC verifies, in lawful ways and within the limits of applicable regulations, that users comply with the principles defined by the security Policy and procedures, informing employees that responsibility for violations rests directly with the individual.

Where appropriate, specific offences under the Criminal Code relating to cybercrime will also be prosecuted.

In case of substantiated suspicions or credible reports, in consultation with the competent bodies, control measures may be taken to protect the integrity of the information assets or the company’s image.

---

6. Specific Provisions

6.1 Additional Specific Provisions for ITGC

6.1.1 Staff Responsibilities Regarding Security

Every ITGC employee, at any level, must know, comply with and enforce the security policies and is required to actively report incidents or improper behaviours that clearly violate information security rules.

Examples of behaviours contrary to security and data privacy include:

- Unauthorized access to the company information system.
- Unauthorized access to offices or other employees' workstations.
- Intercepting or blocking communications relating to the information system or between systems.
- Reproducing or removing documentation of any kind without explicit authorization from the holder of the rights or an authorized delegate.
- Accessing or disclosing personal/sensitive and confidential data without formal authorization.
- Destroying, damaging or rendering unusable, in whole or in part, IT systems, programs, information or data.
- Duplicating or removing installed programs for which the company or any Client is licensee or owner.
- Introducing, installing or using software that has not been legally acquired.
- Using the data network and IT equipment for purposes other than those for which the company has provided them.

Additional security responsibilities include the obligation to notify the entities managing system access of staff departures and changes in role, duties or organizational unit, for both employees and external collaborators.

Employees and consultants must sign **non-disclosure agreements (NDAs)** regarding any information that the company deems confidential or secret and that they may learn in the course of their work.

These agreements must explicitly prohibit disclosure of such information outside the company and must be signed at hiring (or, mainly for external personnel, before the individual is granted access to confidential information).

Security must be taken into account during recruitment by selecting staff also based on criteria assessing reliability and loyalty, and by including information security clauses in employment contracts.

Before hiring, and within the limits allowed by labour law, it is advisable to carry out checks such as: reference checks; verification of academic and professional qualifications; checking for pending criminal proceedings or prior convictions, etc.

6.1.2 Use of the Communication and Processing Infrastructure

The company's IT infrastructure must be used appropriately, avoiding personal or improper use and misuse of shared resources. This infrastructure includes the data network, services available on central and distributed systems and individual workstations.

6.1.3 Use of the Company Intranet

Proper use of the network requires compliance with all rules defined in this document and with current technological and operational standards. Access to the network by entities external to the company is regulated by security controls defined by the ISSO in agreement with the IT Manager, according to technological best practices and the reliability level of interconnections, in order to safeguard common company resources.

Partners and suppliers are required to accept and sign any confidentiality agreements for accessing the company intranet.

Access to the network by internal staff and external collaborators must always comply with all current and future security rules.

It is strictly forbidden to install or use network monitoring or control software for any type of network control and/or monitoring, even for security purposes, without prior authorization from the ISSO and IT Manager.

It is likewise forbidden to use pirated software tools that scan network resources, send large volumes of data to other machines, spy on information in transit, or perform any actions contrary to the general security principles set out herein.

6.1.4 Management of IT Equipment: Workstations

No workstation component may be removed or added without specific authorization. Logical access to the workstation must be protected by a password usable only by its assignee.

Confidential personal or critical data must not be stored on the local hard disk unless protected by appropriate mechanisms (e.g. encryption). Managers must periodically verify compliance with software rules.

Copying personal/sensitive data to external media must be justified and authorized by the Data Controller or the Data Processor appointed by the company.

6.1.5 Resource Sharing

Each user may share resources (files, printers or peripherals) on their personal system with other users. Only specific, clearly identified resources should be shared; sharing entire drives, particularly the operating system drive, must be avoided.

A password must be set to protect shared disk areas or resources.

6.1.6 Antivirus

Each person must ensure that their workstation is protected against computer viruses by:

- Verifying the presence of antivirus software.
- Ensuring that the antivirus version is current.
- Requesting updates through existing company tools/procedures.

The antivirus installed by the company cannot be removed or replaced with another product.

Virus scans must be run periodically (once a week) and whenever files are received from outside, downloaded from the Internet or where their origin is uncertain.

6.1.7 Use of Modems / USB Data Sticks for Data Connections

The use of dial-up data connections via modem or USB sticks/SIMs for data connections from the workstation is allowed only for staff authorized for work reasons and may be activated only when the PC is **not** simultaneously connected to the company network.

6.1.8 Use of Wireless Devices

The use of wireless devices is allowed only and exclusively through the company Wireless infrastructure (access points). Only devices explicitly enabled may use this service.

6.1.9 Intrusions

The company considers unauthorized access to other users' workstations to be a serious misconduct, whether performed via physical access to machines or over the network.

Users may not access, or attempt to access, network resources and directories shared by other users without prior authorization from the owners.

6.1.10 Internet Access

Internet access is granted to enable work activities. Collaborators authorized to access the Internet must only use the services for which they are enabled and must not share their credentials or use those of other employees.

Browsing must be conducted ethically and only to improve personal productivity:

- When requested, users must provide their identity.
- Collaborators must respect copyright rules, including for freeware and shareware downloaded from the Internet, when properly authorized.
- Available programs may contain viruses: applicable antivirus standards must be followed.

- Material that is inappropriate, offensive or discriminatory (religious, political, sexual, racial, etc.) must not be made available, shared or forwarded; in any case, users must not access such material.
- Confidential or personal information must not be made available to third parties.

6.1.11 E-mail

E-mail is a tool provided for business purposes and must not be used for personal purposes. The e-mail address is personal and may not be disclosed to third parties who do not work with the company, without the address owner's knowledge. Likewise, it is not permitted to give others access to one's e-mail account or to use another employee's account.

Security measures for message transmission must match the value of the information. Confidential information or personal/sensitive data may be transmitted only if properly protected (encryption).

Exchange of messages that conflict with professional ethics or the company's interests is not tolerated.

Chain letters or spamming (sending unsolicited e-mail, e.g. advertising) are not allowed. By using their address correctly, users can prevent the company from being targeted by such attacks.

The company will not disseminate "requests for help" of any kind, unless formally requested by the competent authorities. Users who receive such messages, even from known senders, must immediately stop the chain and report the fact to their managers.

6.1.12 Access Control

Access to IT resources must always be controlled according to business requirements and information criticality. Each user authorized to access data and IT resources is subject to an authentication process (for recognition by the workstation) that requires entering a user ID and password, confirmed by Multi-Factor Authentication (MFA) via app.

MFA must also be applied to all Cloud services.

MFA has also been extended to the SaaS Cloud service "Fatture in Cloud" (see application standards defined in documents POL-IT-001_Procedura_Utilizzo_Dispositivi_Aziendali and POL-IT-002_Regolamento_Aziendale_utilizzo_SIA).

To ensure that access to personal data is limited to authorized staff only, the following procedures are in place:

- Staff responsible for managing and accessing personal data within the organization have been identified and appointed, and each has been assigned specific roles and clearly defined responsibilities, ensuring they only access resources necessary to perform their duties.

- A secure authentication mechanism (multi-factor authentication) has been implemented to ensure that only authorized personnel can access the system.
- Role and privilege assignments are regularly reviewed and updated, where necessary, in response to changes in staff responsibilities or business needs.
- Access activities are logged and analyzed to identify any security breaches or unauthorized use of personal data.
- Staff have been trained on the importance of personal data protection and on proper use of the authorization system, and made aware of their responsibilities and legal obligations relating to processing personal data.
- Access to company data is protected by conditional access rules through centralized security policies. These rules exclude unsupported operating systems and legacy protocols, and favour advanced authentication systems.

6.1.13 User ID

The assignee must use their user ID strictly personally (may not share or disclose it to third parties), operate within their granted authorizations and use resources only to perform their job or for other purposes authorized by the company. Use of user IDs and passwords by third parties due to improper sharing by the owner constitutes a security violation.

User IDs are defined according to company standards, are personal for all IT applications and must be revoked when the user no longer needs access to the system due to a change in duties or leaving the company; under no circumstances may they be reused by others after handover.

User IDs are strictly personal and may not be reassigned to another user except for group IDs or technological reasons.

The validity of each user ID and its associated authorizations must be reviewed by the security administrator of the specific application at least annually (compliance check).

If a user changes Legal Entity within the Group, a new user ID must not be requested; the user will continue to use the existing ID, but must request the disabling of applications/services that, due to the new role, they should no longer access.

6.1.14 Group User ID

Any group user IDs assigned must have an associated responsible person, who is accountable for their use and monitors activities performed with that user ID. If that person changes role or leaves the company, the group user ID(s) may be reassigned to a new responsible person or blocked.

6.1.15 Passwords

A password is defined and known only to the user and must be managed confidentially; it is strictly personal and must not be disclosed to others for any reason.

Passwords must meet security requirements and, where technically possible, must be subject to rules regarding content and lifetime (mandatory change every 4 months); they must be automatically revoked after 6 months of inactivity and blocked after 5 failed access attempts.

Password reactivation must be requested in writing from the relevant entities, with prior authorization from a Business Unit Security Manager.

Password selection and protection rules include:

- Minimum length of 8 characters.
- Must not be equal to, or contain, the user ID.
- Must contain numbers and alphanumeric characters.
- Must not be trivial and/or easily guessed.
- Must differ from the last 10 previously used passwords.
- Must be changed if there is any suspicion it is known to others.
- Must not be written on devices or sticky notes.
- Must not be visible on the screen when entered.

6.1.16 Communication

Security policies and procedures, as well as any alerts or information on security, must be communicated as effectively as possible to reach the largest number of interested personnel.

ITGC uses all available means, IT and otherwise, to communicate and receive communications regarding information security and protection of the telecommunication infrastructure. In this context, the preferred and only company-recognized channels are:

- Intranet portals.
- E-mail messages from the ISSO.
- Official internal publications.
- Communications attached to pay slips.

Any security-related communication disseminated via channels other than those above is to be considered unreliable and an open violation of security policies.

6.1.17 Connection and Data Transfer

To ensure the security and confidentiality of data during transfer both within and outside the organization, internal and external communication channels used to transfer sensitive or confidential data have been identified and their security and confidentiality requirements have been assessed, based on the types of data transferred and associated risks.

Encryption technologies used to protect data in transit include SSL/TLS (version 1.3) for web communications, SFTP for file transfer and VPN protocols for remote communications.

Where appropriate, encryption technologies used on communication channels use the AES-256 algorithm.

Multi-factor authentication is used to further strengthen access to communication channels.

Use and performance of encrypted communication channels are regularly monitored to identify anomalies or security breaches and to implement any updates needed to ensure compliance with security standards.

6.1.18 Cookie Management

Application session cookies do not contain sensitive information such as passwords or other confidential data. They are primarily used to uniquely identify the user session and maintain application state during navigation.

Cookies are configured to expire when the browser session ends, ensuring sensitive data is not retained longer than necessary.

All persistent cookies are set with a specific expiration date (7 days).

The retention Policy ensures that cookies are used only for legitimate purposes and are deleted or updated when no longer needed, in accordance with the General Data Protection Regulation (GDPR) in the European Union.

6.1.19 Device Configuration Management

The principle of minimum functionality is applied by identifying and assessing the functionalities actually necessary for each system and application, based on operational and business needs.

System and application configurations are set to enable only the functionalities essential for correct operation and to meet operational objectives, removing or disabling unnecessary or unused functionalities.

Individual users, service accounts and processes are granted only the privileges and permissions strictly necessary to perform their activities, using roles and security groups to simplify authorization management and ensure users have the rights they need.

Configuration changes may include firewall settings, access policies, file permissions, network configurations, administrator passwords, etc.

All employees and consultants are provided with a company laptop configured with advanced security systems, including antivirus, encryption, firewall and centralized access and security policy management. All systems are subject to continuous vulnerability

assessment using XDR (extended detection and response) software and are kept up to date with the latest patches.

6.1.20 Backup Management

All company data is managed on cloud platforms (Microsoft) within OneDrive and SharePoint environments. For data stored on these platforms, versioning and recovery of deleted files within 30 days (Recycle Bin) are available.

Employees are strongly encouraged to save critical and work-related data on company cloud storage platforms that are already covered by the company backup perimeter.

Personal data on company devices is not covered by this backup Policy, unless otherwise specified or used for internal investigations.

Employees are responsible for ensuring that local data needed for work is regularly synchronized with company resources subject to backup.

6.1.21 Encryption

All company data is managed on cloud platforms (Microsoft) within OneDrive and SharePoint environments.

Download, upload and synchronization of data are protected using industry-standard encryption protocols:

- **SSL/TLS (Secure Sockets Layer / Transport Layer Security)**: ensures that the connection between the browser (or OneDrive/SharePoint application) and Microsoft servers is secure and that no one can intercept or read data in transit. Microsoft uses 2048-bit keys for TLS connections.
- Data transfers between Microsoft data centers (e.g. for geo-replication for disaster recovery) take place on private networks protected by additional layers of encryption.

Encryption of Data at Rest

Data stored in Microsoft data centers is encrypted. Microsoft uses several technologies:

- **BitLocker**: used for disk-level encryption, protecting the entire storage volume where data resides.
- **Per-file encryption**: each file (or even parts of a file, “chunks”) is encrypted individually using a unique encryption key, typically with AES-256. This provides a very high level of security. Keys are themselves encrypted and securely managed by Microsoft in a dedicated Key Store.
- **Transparent Data Encryption (TDE)**: used for Azure SQL databases storing SharePoint metadata, ensuring protection of such information as well.

6.1.22 Clean Desk and Screen Policy

When the authorized person is not at their workstation, all paper documents and data storage media identified as sensitive must be removed from the desk and from other locations (printers, fax machines, copiers, etc.) to prevent unauthorized access.

Such documents and media must be stored securely in accordance with the information classification Policy.

When the authorized person is not at their workstation, all sensitive information must be removed from the screen and access to all systems they are authorized to use must be blocked.

For short absences (up to 30 minutes), the clear screen Policy is implemented by logging out of all systems and locking the screen with a password.

6.2 Office Access

The ITGC office in Assago consists of offices on the fifth floor of an office complex.

Employees who do not work directly at Client sites or who need to work at the office, even temporarily, work at this location.

6.2.1 Right of Access

ITGC employees are entitled to access the offices using the company badge.

Third-party access to the offices is only allowed after:

- identification of the third party;
- authorization to enter from the Administration Manager;
- registration of access (name, role, date and time of entry, date and time of exit).

6.2.2 Entrance Controls

Access to the offices is overseen by the HR Office.

People who are not employees of IT Global Consulting S.R.L. must obtain access rights as follows:

- identification of the third party;
- authorization to enter from the Administration Manager;
- registration of access (name, role, date and time of entry, date and time of exit).

Guests may enter and remain in the offices only in the presence of a designated employee, who must accompany them for the entire duration of their stay.

6.2.3 Prohibited Activities

The following activities are **NOT** allowed in ITGC offices:

- Making any kind of photographic, audio or video recording without explicit authorization.
- Connecting any electronic device to the power supply without specific authorization.
- Touching or working in any way on any installed equipment without specific authorization.
- Connecting any device to the data network (wireless or wired) without specific authorization.
- Storing flammable materials or equipment.
- Using any type of heating equipment.
- Smoking.

6.2.4 Periodic Checks

The ISMS Manager checks every two weeks that the area complies with all safety and security requirements.