Corporate Information Security Policy.

Summary

Corporate Information Security Policy.

1. Goal

7COMm Group's Information Security Policy aims to establish the Information Security principles and guidelines aimed at ensuring the confidentiality, integrity and availability of information, assets, systems and processing resources associated with the information owned and/or under its custody , and its compliance is mandatory for all who use the company's information, resources and/or other tangible or intangible assets.

Establishes rules, standards and best practices to ensure the protection of information made available for the performance of professional activities and compliance with current laws and regulations.

Ensure that the 7COMm Group has adequate Information Security standards, procedures and controls in place to mitigate Information Security risk and ensure compliance with all relevant Data Protection and Privacy laws, regulations and standards.

2. Recipients

This policy applies to all directors, administrators, employees, interns, apprentices, employees and visitors of the 7COMm Group and third parties involved, who act on behalf of the 7COMm Group, such as service providers, resellers and commercial partners who have access to the network or use the processing environment of the 7COMm Group and its customers
It also applies to all information assets and computer equipment, owned by the 7COMm Group or not, and which contain information relevant to the institution's business.

3. Responsibilities

3.1. Executive Board and Presidency

3.1.1. Analyze and support Information Security projects, helping to maintain the development of the area, always allied with the continuity of the business and strategic interests of the 7COMm Group.

3.1.2. Approve, observe and enforce this policy, which includes the basic principles, guide-

lines and responsibilities of the information security process.

3.1.3. Ensure the implementation of this Policy, ensuring compliance with its principles and guidelines in all its decisions.

3.2 .Area Managers and Leaders

3.2.1. Knowing, observing and enforcing this policy standards as well as its good practices, procedures involved and guiding employees in their day-to-day work.

3.2.2. Inform those responsible for Information Technology and/or Information Security by email, reporting channels or in person about any and all events, behavior or incidents that compromise information security.

3.3. Information Technology Sector

3.3.1. The Information Technology Sector is subordinated to IT Governance.

3.3.2. Program, execute and keep this policy, acting on its unfolding and the permanent and systematic dissemination of its content to interested parties.

3.3.3. Annually review and update the security policy, adapting it to the technological reality.

3.3.4. Register and deal with security incidents and changes in the environment through available computational resources, in compliance with current operational procedures.

3.4. Corporate Framework

3.4.1. Read, understand and fully comply with the terms of the General Information Security Policy, as well as other applicable security rules and procedures.

3.4.2. Notify the Information Technology Management of any event that violates this policy or may jeopardize the security of information or computing resources of the 7COMm Group.

3.4.3. Understand the role of information security in your daily activities and participate in awareness programs.

3.5. Service Providers, Resellers, Business Partners and Visitors

3.5.1. Understand, respect and follow the PSI made available by 7COMm Group from the moment you have access to the network or use the processing environment of 7COMm Group and its customers.

4. Guidelines

4.1. Corporate Network Access

7COMm Group provides its authorized users with access accounts that allow the use of information assets, information systems and computational resources, such as the corporate network.

4.1.1. It is hereby established that the IAM access management standard, NOR SEG 001/21, is complementary to this policy as it contains details of the process.

4.1.2. Every access account is personal to the user to which it was delegated and non-transferable.

4.1.3. The user is fully responsible for its use, answering for any violation or irregular/illicit act, even if exercised by another individual and/or organization in possession of his access account.

4.1.4. To ensure information security, 7COMm Group practices blocking access to network and e-mail accounts in the following situations: emergency requests, attacks or cybernetic risk and shutdown

4.1.5. The use of notebooks, computers, tablets that are private on the corporate network that are not following BYOD (Bring Your Own Device) rules is prohibited.

4.1.6. Personal equipment of visitors, suppliers and service providers must connect to the visitor network (WIFI – Guest).

4.1.7. Installation of any equipment on the network without proper authorization from the information technology management is prohibited.

4.1.8. Do not write down or record access passwords anywhere, except in the tools officially provided by 7COMm Group

4.2. Access Passwords

Every access password is personal to the user, which was delegated and non-transferable. In this way, the user is fully responsible for its use, answering for any violation or irregular/illicit act, even if exercised by another individual and/or organization in possession of his access password.

Users should take precautionary measures to ensure secure access to information assets and services, including:

4.2.1. Passwords are valid for 90 (ninety) days. After this period, the systems will automatically request to change the password.

4.2.1. Passwords associated with accounts with non-administrative privilege will be composed using a minimum amount of eight (8) digits, combining uppercase and lowercase letters, numbers and special characters; the new password cannot be the same as any of the last 10 passwords used.

4.2.2. After 05 (five) access attempts with invalid passwords, the user account will be blocked, remaining in this way for at least 30 (thirty) minutes;

4.2.3. Upon joining the corporate framework of the 7COMm Group, all users and third party users receive a “username” and “temporary password” to start their activities. The temporary password must be changed at the first access, being composed within the standards mentioned in this policy.

4.2.4. Any unauthorized use or attempted unauthorized use of credentials and passwords to access information assets/services or computational resources will be treated as an information security incident, with an analysis of the infringement by the area responsible for Information Security and application of the sanctions and punishments provided for in the Information Security Policy, according to the seriousness of the violation. If the employee’s account is involved in a possible incident, the account may be blocked immediately.

4.2.5. Access Password Recommendations: when creating a new password, users must

pay attention to the following recommendations:

4.2.5.1. Do not use any part of your credential in the composition of the password;

4.2.5.2. Do not use any of your names, surnames, names of family members, work colleagues or information about you that is easily obtainable, such as, for example, car license plate, date of birth, or address;

4.2.5.3. Do not use repetition or sequence of characters, numbers or letters;

4.2.5.4. Any part or variation of the 7COMm Group name;

4.2.5.5. Any variation of the items described above such as duplication or reverse writing.

4.3. Use of Files, Directories and Data Storage

4.3.1. All requests for access to data must be processed in accordance with the 7COMm Group's current management and access procedure and deadlines specified by the relevant legislation.

4.3.2. This policy addresses basic rules for the protected and adequate use of the 7COMm Group's data, details and more technical and specific rules will be dealt with in the information management standard.

4.3.3. Concessions, revisions and exclusions must be based on concepts of authority, authenticity and minimum access privileges, with each one having access only to the information that is necessary for the development of their professional activities.

4.3.4. The manager of each system/platform is the one who must authorize access to data, in addition to carrying out periodic reviews.
4.3.5. If IT identifies an information security risk, it can question the access request and propose a change suggestion.

4.3.6. Information Security may audit access to information and its proper use at any time, apply appropriate Level 1 sanctions, guide and make corrections necessary to comply with the rules of the current information security policy. In the event of any infringement, the management of those involved must be informed via email.

4.3.7. Whenever there is a need to transfer a user or third party user to another department or function and there is a need to review existing accesses, the former manager must register a call to block previously granted accesses.

4.3.8. Data owned by 7COMm Group, or not, must be stored exclusively on its servers and corporate cloud platform and on file servers. Printed data must be properly filed in secure locations.

4.3.9. Access to files and directories is carried out through sharing on the network, respecting the rules for managing access by profile through network accounts, however, it is the responsibility of area managers to open a call with IT to request, review and revoke access.

4.3.10. It is prohibited to use external media such as: Pendrives, External HDs and CDs for private copies of work data.

4.3.11. The secrecy of information is the responsibility of all recipients, and the unauthorized use of information from the 7COMm Group is prohibited.

4.3.12. Confidentiality and privacy of information must be a priority as instructed in the secrecy and privacy policy referenced in item 4.5 of this document.

4.4. Asset Management

This policy aims to establish guidelines for the acceptable use, understood as safe, of the information assets of the 7COMm Group, by its authorized users.

Every user must observe the following provisions regarding the use of equipment owned by the 7COMm Group:

4.4.1. The 7COMm Group provides its users with equipment exclusively for carrying out their professional activities.

The equipment made available with the specific purpose of allowing users to carry out their professional activities are the property of the 7COMm Group, and use for private purposes is expressly prohibited;

4.4.2. The alteration and/or maintenance of any equipment owned by the 7COMm Group is

a specific attribution of the internal infrastructure department of the 7COMm Group which, at its sole discretion, may be formally delegated to another person in charge. Other users are expressly prohibited from performing any type of maintenance or modification on the equipment;

4.4.3. Group 7COMm equipment must be used with care to ensure its preservation and proper functioning.

4.4.4. Desktop computers (desktops) or mobile computers (notebooks) must be blocked at the end of the working day or whenever the user is absent.

4.4.5. For the release or loan of assets of the 7COMm Group, it is necessary to sign the Equipment Lending Agreement - Notebook and Peripherals and/or Term of Receipt and Responsibility - Notebook and Peripherals, and this will only occur after the documents are signed.

4.4.6. At the end of the provision of services and/or contractual relationship, the equipment made available for the performance of professional activities must be returned in an adequate state of conservation when the user disconnects or terminates the relationship with the 7COMm Group.

4.4.7. At its sole discretion, the 7COMm Group may allow the use of private equipment for the performance of professional activities, which must undergo a technical evaluation by the information technology department, ensuring that it is within the minimum safety standards.

4.4.8. Connecting network, Wi-Fi or telephony devices to the 7COMm Group network is not permitted without authorization from the information technology sector. This safety equipment has a standardized installation and non-compliance with this standard is considered serious.

4.4.9. The 7COMm Group may, at its sole discretion, provide its users with mobile devices or devices with removable storage capacity to carry out professional activities, subject to compliance with the guidelines as per the general data storage standard.

4.4.10. It will not be admissible, under any circumstances, the reuse of pages already printed and containing information classified as confidential, which must be discarded in accordance with the procedures adopted by the 7COMm Group.

4.4.11. The 7COMm Group may, at its sole discretion, provide digital certificates to users who perform specific professional activities, each recipient being responsible for proper and acceptable use, and the guidelines of the digital identification standard must be observed.

4.4.12. Use of printing and reprographic equipment (photocopiers) must be made exclusively for the printing/reproduction of documents that are of interest to the 7COMm Group or that are related to the performance of the user's professional activities.

4.4.13. In cases of unauthorized access, loss, theft or theft of computing devices belonging to the 7COMm Group, the responsible user must immediately report the incident to the information technology department.

4.5. Privacy and confidentiality of information

4.5.1. All employees who have access to information from the 7COMm Group or under the company's custody - strategic, personal, sensitive or not - may not use it for personal purposes or disclose it to unauthorized persons. Restrictions include the use of data in lectures, presentations, publications or any other disclosure to the external public without prior approval of the company's management.

4.5.2. To ensure data integrity and reliability, 7COMm Group relies on the use of virtualization technologies integrated with cloud storage, keeping its environment safe in case of disasters.

4.5.3. The 7COMm Group processes personal data for specific purposes and in accordance with the legal bases provided for in the GDPL.

4.5.4. Personal data is information relating to a living individual who is or can be identified from the data or the data together with other information that is or is likely to be in the possession of the 7COMm Group. All recipients of this Policy who process data must be aware of and follow the guidelines of the Privacy Policy of the 7COMm Group, ensuring the confidentiality and privacy of data in accordance with current legislation.

4.6. Backup e Restore

4.6.1. To ensure data integrity and reliability, 7COMm Group relies on the use of virtualization technologies integrated with cloud storage, keeping its environment safe in case of disasters.

4.6.2. The information technology sector periodically performs restore tests to ensure availability in case of disaster. Technical details are detailed in the backup management standard that complements this policy.

4.6.3. Restores can be requested via call and will have their SLA followed according to the service management policy.

4.6.4. The Backup Policy does not cover the backup of information stored on workstations (Desktop/Notebook), therefore it is necessary for users to store information only on servers or resources offered by the 7COMm Group.

4.7. Remote Access

The 7COMm Group provides VPN access to users and third party users providing remote services to ensure a secure connection to its corporate network.

4.7.1. Only equipment validated and configured by the IT team can access the VPN.

4.7.2. Only the 7COMm Group's internal Infrastructure team is authorized to perform remote access to desktops, notebooks, devices and servers for maintenance and monitoring purposes. If any need arises, the employee's manager must open a ticket subject to the service SLA deadlines.

4.7.3. Remote user and third-party user access to 7COMm Group's information assets/services or computing resources can only be granted after the confidentiality agreement between the parties is in effect and must be monitored by the 7COMm Group's internal infrastructure. The granting of access must be limited to the estimated time necessary for the activity of the third party or service provider. Minimum privileges access will be granted for the execution of activities.

4.7.4. The third party user, as well as the company where he works, will be solely responsible for all actions performed with his remote access credentials, including any unauthorized activity carried out by other parties in possession of his remote access credentials.

4.7.5. During the monitoring of remote access to its information assets/services or computational resources, 7COMm Group reserves the right, without any notice or notice, to intercept, register, record, read, copy and disclose by, or to, authorized persons for official purposes,

including criminal investigations, all information transmitted, whether originating from its internal network and destined for external networks or otherwise.

4.8. Physical Access Control

Access to the controlled environment must be carried out through a unique, personal, identifiable credential and cannot be given to another person;

This topic aims to formalize the guidelines for physical access to the 7COMm Group Data Center. Access control to the other premises will be done according to the specificity of each area to be visited, where the criteria established by those responsible for them will be observed.
The following guidelines for controlled access environments must be adhered to:

4.8.1. Access to the Data Center is only allowed to the IT Infrastructure, Information Security team or other supervised persons.

4.8.2. In internal or external audits, auditors must always enter the Data Center accompanied by at least one member of the 7COMm Group team.

4.8.3. In the case of third-party services to be carried out within the Data Center, monitoring and approval by the IT and Information Security area is required.

4.8.4. All access to the Data Center must be registered in its own access control system and will be allowed through the use of an approach card.

4.8.5. Data Center access records must be stored in a safe place and must be kept in history for at least 1 (one) year.

4.8.6. In controlled access environments, the use of cameras is prohibited, whether attached to the smartphone or not, except in situations inherent to the work routine and/or under IT authorization.

4.9. Regarding the acceptable use of the corporate Internet

This aims to formalize the general guidelines for the use of the Internet, E-mail, Social Networks and instant messaging tools on the premises of the 7COMm Group.

4.9.1 - The Internet must be used by users and third-party users for work-related activities and made available according to the needs corresponding to the functional profile of each user, with the aim of meeting the needs of the respective areas;

4.9.2. In cases where access is necessary for other purposes, the internet may be made available with the due authorization of the immediate manager, this access being controlled and monitored;

4.9.3. Internet access for people not affiliated with the 7COMm Group may be made available in a separate technological environment (visitor network), controlled and monitored, either via mobile (wi-fi) or fixed means;

4.9.4. Granting access to the guest network must be associated with awareness of the internal rules for using the network.

4.9.5. The 7COMm Group seeks to prioritize compliance with current laws, to ensure compliance the 7COMm Group adopts some monitoring and blocking measures, acting preventively, improving security, aligning its business objectives;

The following items are subject to monitoring, blocking and penalties if performed with 7COMm Group assets:

1. Excessive browsing on sites that are not strategic to the 7COMm Group's business

2. Navigation on sites that allow or encourage downloads and/or distribution of pirated sites,

3. Browsing inappropriate websites.

4. Browsing websites that promote gambling.

5. Disclosure or propagation of defamation, prejudice or fraudulent behavior.

Access to social networks (ex.: facebook, linkedin, etc.) or to sites that have audio and/or video (ex.: radios, online TVs, youtube, etc.) are controlled and made available only to areas that need to use these resources in their work activities. Requests for the release of these sites must be made by opening a call, which must be authorized by the immediate manager and filed for audit purposes;

4.9.6. Software with peer-to-peer (P2P) characteristics, such as Emule, Kazaa, Morpheus, Torrent and the like, are not allowed, so they must be restricted by the Information Security technical area and monitored user access, with the aim of ensure security and proper use of the Internet;

4.9.7. It is prohibited to provide or disclose on the internet (registration sites, discussion groups, social networks, among others) information of the 7COMm Group that is classified as internal, reserved or confidential.

4.9.8. Any information that is accessed, transmitted, received or produced on the internet within the company may be audited without prior notice. 7COMm Group reserves the right to monitor and carry out constant audits of access to websites visited by users and third-party users within legal compliance.

4.9.9. The recipients of this PSI will respond for any acts or infractions caused by recklessness or malpractice that may compromise the security of information through the use of the internet.

4.10. Use of Corporate Email

The 7COMm Group provides the email service exclusively for the performance of its professional activities to users and authorized third party users;

4.10.1. It is not allowed for work purposes, the use of any e-mail service, other than the one officially provided by 7COMm Group;

4.10.2. It is not allowed to use the e-mail service on a personal basis or for purposes that are not in the interest of the 7COMm Group;

4.10.3. It is not allowed to send information classified as INTERNAL USE or CONFIDENTIAL to electronic addresses that are not part of the corporate domain of 7COMm Group, except when expressly authorized;

4.10.4. During monitoring, 7COMm Group reserves the right, without any notice or warning, to monitor, intercept, record, read, block, redirect, retransmit, copy and disclose by, or to, authorized persons for official purposes, including criminal investigations, all messages sent or received by users through its email service without prior notice;

4.11. Messenger

4.11.1. 7COMm Group makes Microsoft Teams available to its entire organization and adopts this application as standard. It is expressly prohibited to use any other messaging service other than the 7COMm Group standard for communication or data sharing. Except when at the express request of a customer;

4.12. Secure Development

These guidelines aim to ensure that information security is an integral part of the entire life cycle of information systems, establishing guidelines and requirements for the development and maintenance of information systems, providing regulations for secure software development within the Group 7COMm.

As for data storage, storage media that do not have access to read and write restricted by password should not be used, in addition, they should preferably be stored encrypted.

4.12.1. As for database access:

1. Access to a database should not be made available to applications using a user login with root permissions.

2. Access to a database should not be made available to applications using a user login with permissions to execute commands in Data Definition Language (DDL).

3. Applications must not be given access to a database using a user login with permissions beyond those strictly necessary for their operation.

4. The above rules can be changed according to the needs of each client and must be duly justified.

4.12.2. Regarding the use of passwords:

1. The creation of passwords that do not follow the standards established in the access management rules of the 7COMm Group must not be allowed.

2. Password storage in source code should not be used.

3. The homologation and production environments cannot have the same passwords as the development and test environments.

4.12.3. Regarding user authorization and authentication

1. Passwords should not be stored in plaintext without using a secure hashing and salting algorithm.

2. Authentication via AD or LDAP should be used whenever possible.

4.12.4. Authentication in Web Systems:

1. Since HTTP is a stateless protocol, which uses cookies to maintain user sessions, it is necessary to guarantee both the security of the exchange of credentials and the security of the other pages accessed by users of web systems. The HTTPS protocol aims to contribute to guaranteeing this security.

2. Thus, HTTPS must be used on all screens of the systems.

4.12.5. Attacks and Defense:

1. SQL Injection attacks must be prevented.

2. SQLs should not be created by concatenating textual parameters from non-safe sources, such as parameters filled in by the user or even stored in the database.

3. Access permissions to the database for the application user must be restricted.

4. Whenever possible, parameters should be passed in SQL commands (DML or DDL) using prepared statements. Queries that cannot be parameterized must be given special treatment, such as escapes or hexadecimal encoding.

5. You must prevent HTML and Javascript injection attacks.

6. Cross-site scripting (XSS) attacks must be prevented.

7. Breaking Authentication and Session Management attacks must be prevented.

8. Systems in the Product area must be submitted to penetration testing tools.

4.12.6. As for the tests

1. Security tests must be performed on each version of the software that modifies its structure (login screens, unauthenticated services, new forms with user interaction, etc.) when applicable, to be defined by the technical responsible for the application.

2. It must be ensured, through automated tests, that the services and confidential data are protected and available only to the users who hold the information.

3. A testing policy, whether automated or not, should be designed to ensure non-vulnerability to the main known attacks on systems.

4. Test scenarios aimed at guaranteeing the non-functional requirements of the software must be defined, preferably carried out by a test team different from the software development team, in order to avoid vices.

Test scenarios must be defined, mainly in the security aspects, for cases of system architecture updates (application servers, databases, browser versions, operating system versions, etc.).

4.12.7. Access to the source repository and business rules

1. For each project there is a specific area in our repositories and access to both sources and business rules is allowed only to collaborators who are somehow involved with the project.

2. Access is controlled via username and password defined in the corporate Active Directory under the responsibility of the security and infrastructure area.

3. Access to the repositories is allowed, by formal request from the responsible team leader, when a user starts the project.

4. Accesses are withdrawn immediately when the user leaves the company, goes on leave, leaves the project or is reallocated.

5. At the end of the project all accesses are withdrawn;

6. In addition to daily maintenance, there is a quarterly assessment with the leaders and it is verified whether users should still continue with existing accesses, if not, accesses are withdrawn.

5. Sanctions

Upon becoming aware of this Policy, all recipients are responsible for complying with its provisions and ensuring that third parties in their relationship are informed about its content. Violations, even if by omission, or unsuccessful attempt of this Policy, its rules and published procedures may result in penalties such as those described below:

Level 1 - Actions of people that may generate everyday and low-severity incidents will be treated with informative and corrective measures, such as:

- Verbal warning;

- Formal notification.

Nível 2 – Actions that may cause serious incidents, but with low damage, may generate administrative punishments, such as:

- Unpaid suspension;

- Cancellation of signed main contract.

Level 3 – Actions that may cause serious incidents and high losses, may lead to legal infractions, such as, but not limited to:

- Application of labor sanctions provided for in current legislation, including dismissal or just cause;

- Civil or criminal proceedings;

- Reimbursement of damages caused to 7COMm Group.

The existence of recurrent and continuous violations makes the incidences serious.

For violations that are related to criminal activities or that may cause damage, the offender will be held responsible for the damages, with the application of appropriate legal measures.

6. Thecnical Glossary

- **BYOD:**

BYOD is an acronym for Bring Your Own Device, in Portuguese “bring your own device.

- **Encryption:**

Encryption in cybersecurity is the conversion of data from a readable format into an encoded format.

- **Data Center:**

It is an environment designed to house servers and other corporate assets such as data storage systems (storages) and network assets (switches, routers) with security and control. The main objective of a Data Center is to guarantee the availability of equipment that stores corporate information and that hosts corporate systems that are crucial to the Institution’s business.

- **Homologation:**

The homologation environment is an environment where the customer must test the system’s functionalities that will later be put into production or, in cases of problems, will be redone, if approval by this customer does not occur.

- **GDPL:**

General Data Protection Law.

- **Backup:**

The term backup means “backup copy”, and corresponds to the creation and storage of copies of important digital files, so that it is possible to restore them in case of loss of the original files.

- **Restore:**

Restore is the action of recovering data stored on a given device during the backup routine, ensuring that all recorded information is intact.

- **Server:**

Server is a computer that centralizes services, offering them to other computers that are in your network. Such services may be of a different nature, such as e-mail, website, file storage, among others.

- **SLA:**

The meaning of the acronym SLA is “Service Level Agreement”, in Portuguese, “Service Level Agreement”, “Service Level Agreement” or “Service Level Guarantee”.

- **VPN:**

VPN stands for “Virtual Private Network”, i.e. “Virtual Private Network”. As the name implies, it is a user’s private network that provides more security when browsing, as it has better encryption, protecting your data.