Security Policy

SCM LATAM 2019

Security Policy

INDEX

1. Information security policies

1.1 Policy summary:

The information must be always protected, regardless the way it is shared, communicated or stored.

1.2 Introduction:

The information may be existing in different ways: printed or written in paper, stored electronically, transmitted by email or by electronic methods, showed in projections or in oral form in conversations.

The Safety of the information is the protection of the information against a wide range of threats, in order to ensure business continuity, minimize business risks and maximize the return of investments and opportunity of business.

1.3 Scope

- This Policy support the general policy of the information security management system (ISMS).
- This Policy is of consideration by the members of the organization.

1.4 Information security objectives

- Understand and treat the operational and strategy risks in security information to remain in acceptable levels for the organization.
- The protection of confidentiality of the information related with clients and the development plans.
- The preservation of the integrity of accounting records.
- The Web services of public access and the intern networks comply the specifications of availability required.
- Understand and give coverage to the needs of the interested parties.

1.5 Information security principles

- This organization affronts risks taking and tolerates those, who based in information available are understandable, controlled and treated if it is necessary. The Details of the adapted methodology for the risk evaluation and its treatment are available and described in the ISMS policy.
- All the personal will be informed and responsible for information security, as it is relevant to the performance of their work.
- Financing will be available for the operational management controls related to information security and management processes for its implementation and maintenance.
- It will be aware about possibilities of fraud related to the abusive use of information systems within the global management of information systems.
- Regular reports will be available with the security information status.
- Information security risk will be monitored, and relevant measures will be taken when there are changes that imply an unacceptable level of risk.
- The criteria for classification and risk acceptance are referenced in the ISM policy.

- Situations that may expose the organization to the violations of laws and legal norms will not be tolerated.

1.6 Responsibilities:

- The management team are the responsible for ensuring that information security is properly managed throughout the organization.
- The Manager is responsible for ensuring that the personnel in charge, protect the information in accordance with the rules established by the organization.
- The Security responsible will give advice to the management team, provides specialized support to the personnel of the organization and guarantees that reports about information security are available.
- All the members of the personnel have the responsibility of maintain the information security within the activities related to their work.

1.7 Key Indicators

- The information security incidents will not result in serious and unexpected costs, or in a serious disruption of commercial services and activities.
- Fraud losses will be detected and will remain within acceptable levels.
- The customers' acceptance of the products or services will not be adversely affected by aspects related to information security.

1.8 Related Policies

Here Below, it will be detailed those policies that will provide principles and guides in specific aspects of the information security.

- Information security management system (ISMS) Policy.
- Physical access control policy.
- Workplace hygiene policy.
- Unnotarized software policy.
- File download policy (external/internal network)
- Security copies policy.
- Information exchange with other organizations policy.
- Use of courier services policy.
- Retention of records policy.
- Network use services policy.
- Informatic and communication mobility uses policy.
- Teleworking policy.
- Cryptographic controls use policy.
- Legal provisions compliance policy.
- Software use licenses policy.
- Data and privacy protection policy.

At a lower level, the information security policy must be supported by other rules or procedures on specific topics that further enforce the application of information security controls and its normally structured to treat needs of determined groups of the organization or cover certain topics.

EXAMPLES OF THESE POLICY TOPICS INCLUDES:

- Access Control.
- Information Classification.
- Physical and environmental security.

AND MORE DIRECTED TO USERS:

- Information security management system (ISMS) Policy.
- Acceptable use of assets.
- Clean desk and clear screen.
- Information transfer.
- Mobile devices and teleworking.
- Software use and install restrictions.
- Backup Copy.
- Malware Protection.
- Technical Vulnerability management.
- Cryptographic controls.
- Security communications.
- The privacy and protection of identifiable personal information.

These policies/rules/procedures must be communicated to the employees and external interested parties. The need for universal security standards will vary depending on the organizations. When some of the information security rules or policies are distributed outside the organization, care should be taken not to disclose confidential information. Some organizations use other terms for these policy documents, such as: norms, guidelines, rules. All of these policies should support the identification of risks through the provision of controls in relation to a reference point that can be used to identify the deficiencies in the design and implementation of the systems, and the treatment of the risks through the possible identification of appropriate treatments for located vulnerabilities and threats.

This identification and risk treatment are part of the defined processes in the principles section within the security policy or, as referenced in the example, they are usually part of the ISM policy itself, as noted below.

THE EXECUTIVE DIRECTION OF THE COMPANY IS RESPONSIBLE FOR APPROVING AN INFORMATION SECURITY POLICY.

1. The information will be protected against any unauthorized access.
2. The information confidentiality, especially the related with personal employee and customer data.
3. The information integrity will be maintained related to the information classification (especially the information of “internal use”)
4. The information availability that complies with the relevant times for the critical business processes development.

5. The compliment according to the current legislation and laws regulations, especially with the Data protection and digital signature.
6. Business continuity plans will be maintained, tested and updated annually.
7. Safety training is accomplished and updated sufficiently for all employees.
8. All events that are related to information security, real or supposed, will be communicated and investigated to the security officer.

Additionally, Support procedures are available for the designed responsible and include the specific way to accomplish the general guidelines indicated in the policies.

Compliance of this policy, as well as the information security policy and any procedure or documentation included within the ISMS documentation repository, is mandatory and concerns all the staff of the organization.

The visits and external personnel who access to the facilities are not exempt from the compliance of the obligations indicated in the ISMS documentation, and the internal personnel will observe their compliance.

In any case of doubt, clarification or for more information about the use of this policy and the application of its content, please consult by phone or e-mail the responsible in charge of the ISMS formally designated in the corporate organization chart.

2. Access Management

2.1 General Objective

The control of access policy is stablished to control the information of access of the facilities of information processing (Datacenter) and the supply processes which must be controlled by security requirements. Trough the different areas, Operations, Software, Support and Security, it will allow the administration of the user lifecycle, from the automatic user account is created, management of roles and necessary permissions to the account deactivation in systems; Based on the requirements reported by the Human Resources Department and from the direct Manager.

The user will be provided with the appropriate access to information systems and technologic resources, validating the authentication, authorization and audit.

2.2 Specific Objectives

- Identify the security requirements of each of the applications.
- Identify all related information with the applications.
- Define the access profile of standard users.
- Manage access rights in network environment, and all the available network connections.

2.3 Scope

This policy will be applied to all SCM LATAM workers, that have access rights to information that may affect assets and all their relationships with third parties that involves access to their data, resources or management and control of their information systems.

2.4 Access control

2.4.1 Rules for access control

The rules for access control, will be documented trough of the different procedures of technology resources.

2.4.2 Entity Management

The access of the authorized users may be ensured and prevent the unauthorized access to the information systems. For the user credential assignation to the different systems will be used a form with the system name, username, temporal password and the rights to the services and systems.

2.4.3 Users Responsibility

All the company workers and third parties who have a user in a technology platform, should know and must fulfill this specific use of the policy, where guidelines on rights and duties regarding the proper use of the systems, unattended user protection policies, clean desk and clear screen.

2.4.4 Access control to the network

The unsafe connections to the network services may affect all the organization, for this reason the access to the network services will be controlled internal and external. This is necessary to guarantee the correct network services and access for the users and do not compromise their safety.

The rules of access to the network through the ports, would be based on the premise – “everything is restricted, unless this is expressly allowed”.

2.4.5 Service network use Policy

Procedures were developed for the activation and deactivation of access rights to networks, which will include:

- Access control to the network services external and internal.
- Identify the networks and network services to which access is allowed.
- Perform rules and procedures for authorization of access between networks.
- Establish controls and administration procedures to protect access

2.4.6 Identification of the devices in the network

SCM LATAM will control and identify the equipment connected to the network using domain controllers, manual IP assignment and captive portal for the WIFI connection.

2.4.7 Protection of the ports of configuration and remote diagnostics

Ports that allow remote maintenance and support network equipment, servers and end-user equipment will be restricted to network administrators or servers. The final users should allow to take the remote control of their equipment for the Support Area, the user will not have files with sensitive information in the desktop, not disregard the equipment while control of the equipment is by a third party.

2.5 Access control to the operating system

2.5.1 Safe start registers

The access to the operating system will be protected, by a safe start session, which will contemplate the following conditions:

- Do not display system information, until the startup process is complete.
- Validate the access data, once all the input data has been correctly approved.
- Limit the number of failed connection attempts by auditing unsuccessful attempts.
- Don't show the digits of the password.

2.5.2 Password Management

The assignment of passwords should be controlled through a formal management process in charge of the support area. The recommendations are:

- Do not write them on easily accessible papers, or in unencrypted files.
- Do not send it in e-mail.
- Never store passwords, on any paper or easily accessible places.
- Passwords must be kept confidential.
- Do not share passwords with other users.
- Change your password if you think someone else knows it and if you have tried to misuse it.
- Create strong passwords not easy to guess.
- Never record your password on a function key or in a predefined character command.
- Change your password regularly.
- Do not use the option to store passwords on the Internet.
- Do not use password with phone numbers, family name or similar.
- Do not use password with variables (name1, name2, name3 or similar)

2.5.3 Access control to the information

The Access control to the information through an application, will be carried out through the roles that administer the privileges of the users within the information system. The control of access to physical or digital information will be carried out considering the levels of classification and the management of information exchange.

2.6 Mobile computing and remote working

Account the advantages of the mobile computation and remote work, as well as the level of exposure to threats that put at risk the security of the institutional information, then guidelines are established to regulate the use of mobile computing and remote work:

2.6.1 Computing and mobile communications

Mobile devices and communication devices are understood as all those that allow access and storage of organization information, from different locations to the facilities.

The use of computer equipment and mobile storage devices is restricted only for those provided by the organization and should contemplate the following guidelines:

- Use of username and password to access to system.
- Encryption of the information.
- Use of antivirus software.
- Restriction of administrative privileges for users.
- Use of licensed software.
- Periodic backups.
- Use of security mechanisms that protect information in case of loss or theft of devices.
- Always stay close to the device.
- Do not leave equipment unattended.
- Not attracting attention, about carrying mobile equipment.
- Do not identify the device with organizational badges.
- Do not place technical contact data on the device.
- Keep the classified information encrypted.
- Do not connect to public Wi-Fi networks.
- Keep off Bluetooth or any other wireless technology that exists or will exist.
- Immediately inform the organization about the loss or theft of the device, who will proceed to block the user.

For mobile communication devices (cell phone) of the company the above-mentioned controls and those detailed below will be applied:

- Activate the cell phone password, to access the cell phone directory, text messages, incoming, outgoing and missed calls. Voice, image and video files.
- Don’t speak about confidential topics near persons who don’t requires to know the information.

2.6.2 Remote working

The remote work will only be authorized by the Manager in charge of the organizational unit where the user who request the permission belongs. Such authorization will only be granted by the Safety Area once the safety conditions of the work environment are verified.

3. Risk evaluation process

3.1. Objective

Describe the methodology and criteria to be applied to carry out the process of hazard identification and risk assessment, in order to facilitate decisions to control possible consequences.

3.2. Process Activities

Even when a large part of the monitoring and evaluation attention is focused on the vertical elements of the consultative service project framework (Resources, Activities, Products, Objectives, Goals), the project team must also monitor the assumptions (which they form the horizontal logic). These assumptions correspond to the risks that could prevent success. The risk of the project is the possibility that something goes wrong, or at least that does not work out as planned. The risks are different in each project and they change as the project progresses. The specific risks of the project, as they might appear in the assumption's column in the logical frameworks, may include the following:

-Does the government's policy / priority support the strategy and objectives of the project? - Are there new investments / developments in the project area that can impact the project objectives? -Did the changes in the sociocultural context affect the project? -

Are there changes in the political or security situation? - Is the economic situation stable (exchange rates, banking systems, devaluation risks)? - How do relationships with key actors seem to be? - Is it possible for the project to lose key employees? - Is the availability of suppliers and skills reliable?

The goal of risk management is to "control" those risks and that identification, analysis and response to them be useful for decision making. Risk management attempts to maximize the probability and generation of positive events and minimize the probability and consequences of adverse events. In practice, project risk management focuses on the following questions:

- **Are we aware of what is happening in the context of the project?**
  At SCM we try to make our links with our clients as close as possible, in order to understand the reality of each other's needs, then go beyond the original requests, and understand possible risks factors to mitigate under the context in which the project or service hours are executed.
- **Are we reconsidering the critical assumptions and risks that could affect the project's ability to act?**
  Using the protocols and latest security techniques, we take care of the day to be under the latest security standards in terms of information protection, which is why critical situations and possible risks that can directly affect the work with our clients, they are evidenced and exposed (if they exist) to the clients, so that they are aware of the possible risks.

- **Are we identifying alternative strategies, contingencies or emergency plans?**
  The identification of these strategies is based on the result of this document, for the taking of action in the event of service failures, such as: connection errors on servers, backups / restore from the database, among others.
- **Are we allocating enough funds to address project risks?**
  Since many of our information services are outsourced, using Amazon Web Services (AWS), we allocate enough funds to minimize as much as possible the uptime our services have.
- **Have changes in the environment, such as new systems or new leadership, created new risks that need to be addressed?**
  Each new client is a new challenge to attend, from the implementations that are made based on the services provided. From load balancers provided by AWS, and instances secured by trust protocols, they make our services market leaders.
  Developing a risk management strategy at the project level helps to ensure that the process is carried out effectively. Some key elements of the project risk management process are:

3.3. Risk Identification (Identify and document all risks that may affect the project)
3.4. Analysis of qualitative risks (determinate the effect of the identified risks on the project´s objectives).
3.5. Analysis of quantitative risks (Assign numerical probabilities to the risks and their impact on the projects objectives).
3.6. Planification of a quick response (decide which actions are required to reduce or remove treats, especially the highly likely and with high impact).
3.7. Monitoring and Control of the risks (respond to risks as they arise and ensure the appropriate risk management procedures are applied)

Once identified, the risks must be addressed with a combination of the following strategies:

- **Avoid the risk** Do not do any part of the scope that implies a high impact and / or a high probability of risk, if it is still possible to achieve the project objectives. Examples: Limit geographic reach if a certain region is problematic or reduce the number of units delivered, such as latrines, if construction materials are missing for the project.
- **Transfer the risk:** Transfer the risk to third parties (or share it) on some aspect of the project through a contract, insurance or other means. Example: in insecure sites, logistics contracts are outsourced to private providers with more knowledge and experience of the region.
- **Mitigate risk:** Take specific actions to reduce the probability and / or impact of a potential risk. Example: institute a security system that prevents unauthorized access to the storage areas of project construction materials.
- **Accept the risk**: If an assessed risk is reasonable, an organization may choose not to take immediate action and undertake to monitor the situation to see if the probability and impact remain acceptable. Example: A community may know that it faces a seasonal risk of landslides but prefers to accept the probability and consequences of the accident rather than trying to avoid it, transfer it or mitigate it.

4. Training in Information Security

   Information is one of the main assets of our organization. The defense of this asset is an essential task of all SCM employees to ensure continuity and business development, as well as a legal requirement (protection of intellectual property, data protection personal, services for the information society), and transfers with confidence to customers or users.

   The greater the value of the information, the greater the risks associated with its loss, deterioration, improper or malicious manipulation.

   Our Information Security Management Systems (ISMS) are the most effective means of minimizing risks, by ensuring that assets and their risks are identified and valued, considering the impact to the organization, and controls and procedures more effective and consistent with the business strategy are adopted.

   Effective information security management ensures:

   - Confidentiality, ensuring that only those who are authorized can access the information of our customers.
   - Integrity, ensuring that the information and its process methods are accurate and complete.
   - Availability, ensuring that authorized users have access to the information and its associated assets when required.

   4.1. Certification

   We are in the process of certifying the System of Management where Security of Information of AENOR, according to UNE-ISO / IEC27001: 2014, which would contribute to promoting the information protection activities in our organization, improving our image and generating trust with our clients.

5. Physical and environmental security

   5.1 Objectives

   In coordination with technological measures, this section focuses on the need to identify and establish physical control measures to adequately protect information assets to avoid incidents that affect the physical integrity of unwanted information or interference.

   5.2 Objective 1 - Safe Areas

   Avoid unauthorized physical access, damage and interference against the information processing facilities and information of the organization.

   5.2.1. Physical Security Perimeter

   Control oriented to provide protection against unauthorized entry. The perimeter, parameters and controls or defenses must be determined in a risk analysis or assessment.

   5.2.2. Physical Access Controls

   Those areas that are considered safe must be protected by entry controls that allow only authorized personnel.

   5.2.3. Workplace, offices and facilities Security.

   Facilities, they must be designed to avoid as much as possible the risk that the confidential information is accessible to visitors.

   Masking techniques must be considerate for data referring to customer names or activities.

Example: a data processing center where many telephone lines are open at any time or situations such as user training or software testing.

5.2.4. Protection Against external and environmental threats

In a world of growing instability and terrorist threats and an unpredictable climate, physical protection against external factors must be considered, designed and applied. Although current laws require us to have protection and emergency plans, we should go further and, if necessary, seek specialized advice.

We could also think that external and environmental threats are covered by the development of "Business Continuity Plans" and "Disaster Recovery", however, protection measures against this should be considered floods, fires and earthquakes to mitigate its effects.

5.3 Objective 2 – Hardware Security

Prevent loss, damage, theft or compromise of assets as well as the interruption of the activities of the organization.

Damage to the equipment can cause interruptions in the activity of an organization or violate the confidentiality of the information caused by theft of assets.

Let's look at the controls that we should review in our risk assessment for information security.

5.3.1 Location and Protection of equipment

Controls to protect the equipment from environmental damage and unauthorized access.

- Avoid unnecessary access
- Protect sensitive area equipment such as data centers or server rooms.
- Protection controls in equipment storage locations if they contain information.
- Protective measures against electrical damage (regulated power supplies, separate and backed power lines etc.)
- Environmental control to comply with the manufacturer's specifications regarding humidity conditions, temperature protection against dust or materials that could damage the equipment.
- Radiation protection measures.
- Guidelines for eating, drinking and smoking should be established near the equipment to avoid damage or simply prevent employees from being in contact with the equipment if they are not working on them.

5.3.2 Support elements

It involves establishing control measures for the supply necessary to keep the facilities and equipment operational.

Often this section is overlooked in small and medium-sized businesses like us, but we should have a checking account to ensure our coverage of power supply and communications failures.

The controls are focused on:

- Comply with the manufacturer's specifications of the equipment when supplies (electricity, gas, etc.)
- Comply with the legal requirements.

- Establish some supply failure detection process.
- Maintain possible alternatives to supply failures (uninterruptible power supplies, alternative routes in communications etc.)

We must be imaginative because it is not always within our reach to be able to duplicate the communications of the electricity and electricity suppliers etc. We sometimes go through to reinforce systems such as Telecommuting, CLOUD supports or agreements with larger companies as important clients of trust with more and more infrastructure in case of disasters that we cannot assume.

5.3.3 Wiring Security

Controls for protection of power and communications wiring that affects information systems. Avoid the possible damage of the infrastructures as well as the possible interferences that corrupt the data or the supply to our clients.

5.3.4 Equipment Maintenance

Ensure that the equipment is properly maintained to ensure that it does not deteriorate and is always available. For this we consider:

- The manufacturer's recommendations.
- Only authorized personnel should maintain critical equipment and records must be maintained.
- Sensitive information should be removed from the equipment when necessary.
- Comply with all the requirements of the insurance policies.

5.3.5 Withdrawal of assets

When it comes to the withdrawal of an information asset, be it equipment, software or other information devices, we should control.

- The identification and authorization of personnel authorized to remove equipment or assets outside the organization.
- We set time limits.
- We keep track of retired equipment and its return as well as personnel identification.

5.3.6 Equipment and out of facilities assets security

We keep a record of the custody of the assets that leave the organization and carry out the risk assessments for facilities where they will be used.

5.3.7 Safety in the reuse and elimination of equipment.

For the equipment that will be reused we guarantee:

- The information they contained was destroyed or overwritten correctly before reuse.
- The information has been completely removed considering that the standard formatting does not perform this task properly.
- Damaged equipment must be subject to a risk assessment before having them available for repair.

5.3.8 Equipment unattended for the user

Users should not leave sessions open while the equipment is not in use. In addition to the screen lock procedures, the application and network session must be closed when connections are not used. This should apply to both mobile devices and fixed equipment.

5.3.9 Clean desktop and clear screen policy

The screens should not display information when the equipment is not in use and the desks must be free of papers when they are not in use or unattended. Depending on the classification where documents in paper and organization culture, paper and extractable media must be secured according to the policy when they are not in use.

Risk assessments should consider the use of technologies that allow copies of information such as: printers, photocopiers, scanners and cameras (especially in phones). The printers can be set up so that only the creator can access the copies once a code has been entered in the machine to prevent unauthorized access.

6. Information Systems Acquisition, Development and Maintenance.

6.1 Objective

Address the requirements for improvement or automation of processes through the development or acquisition of information systems for the Superintendence of Companies.

6.2 Scope

Applied to the requirements of the users that meet the needs of the different processes that the entity advances and that need to be automated, once they are approved by the Enterprise architecture group.

6.3 Definitions

- **Development:** Process of creation and maintenance of programs and information systems.
- **Tools used for development:** Tool Used to Write the Programming Code (development) of Information Systems.
- **Implementation**: The implementation of computer systems is one of the stages of system development, it is to put the information system into operation once it has been developed and tested.
- **Maintenance:** These are the modifications that are made in the information system (software) after delivery to the user. These modifications could be made to improve performance, correct defects, adapt the information system to a new environment, software or hardware, or other desirable properties.
- **Final user:** Official who requires functionality by updating or acquiring an information system.

6.4 Policies

The request or requirement made must be recorded in a complete, clear and with all the background, using the tool that the Directorate of Information and Development defines. This can be the only point of attention DID, help desk, System Center, memorandum or e-mail addressed to the Directorate of Information Technology and Development or to the Innovation and Development Group. The Directorate of Information and Development must ensure:

- In the development or acquisition of information systems, all the necessary requirements for its proper functioning are defined.
- There is integration of the information systems that the organization has.
- All the necessary tests are executed before the start-up (production) of any solution that is implemented.
- Information systems are documented, and the corresponding updates are made when they are modified. Any acquisition, development or modification of information systems should include the provision and / or updating of the corresponding documentation of the system or module:
    - Functional specifications
    - Security specifications
    - Installation and configuration manual
    - Administration, operation and maintenance manual
    - User manual.

- The information systems inventory documents are updated with the modifications and acquisitions that are generated.
- Information security is an integral part of the applications life cycle.
- There are the work environments required in the development of information systems or implementation of information systems that are acquired. (development environments, testing, production, training).
- Tools (source program, object programs, licenses and manuals), of the information systems to be inventoried, have the guarantees and licenses as a result of the acquisition or development.
- In the testing phase of information systems developed or acquired, depersonalized data (no production data) should be used.
- If production data are used, these must be submitted to an official responsible for the same, who must agree on the confidentiality of the data received for evidence. Once the tests are finished, they must be erased safely.
- In compliance with the legal requirements of privacy and information security, the test data must not contain information that allows the identification of the natural or legal person to which the information belongs.
-

- In the development or acquisition of information systems, the source and object programs must be delivered and received from the officials responsible for their control.
- There should be an area or official responsible for the delivery of source programs that are going to be modified and of their reception once they are put into production. Receive the source and object programs resulting from the acquisition of a new information system.
- Personnel outside the development-testing environment must not have, for any reason, access to source programs, utilities, command lines that may put the information systems of the Superintendence of Companies at risk.
- The following guidelines should be considered to control access to program source codes:
  - IT support personnel must have restricted access to the source program libraries.
  - An audit log of all access to the source program libraries must be maintained.
  - Old versions of source programs should be archived with a clear indication of the precise dates and times they were in operation, along with all support software, task control, data definitions and procedures.
  - The maintenance and copying of program source codes must be subject to strict change control procedures.

- **Stages in the development of information systems:** Analysis and approval of information system requirements the fundamental part of the development, acquisition, implementation or maintenance of information systems for the clearing of requirements. The coordination of Innovation, Development and Architecture of Applications must advise officials who require improvements in their information processes.
- **Acquisition or development, and proof of the required information systems**: Once the requirements document has been defined and approved, the process of acquiring or developing the requirements must begin.
- **Delivery and implementation of the required information systems** Once the required functionality or information system has been developed and / or acquired, tested and approved, it must be put into production, prior approval in the committee of changes.
- **Monitoring and control of the development, acquisition or maintenance of the required information systems** Once the information system has been implemented it has been put into production, the following activities should be carried out:
  - Verification of service level agreements.
  - Preparation of supervision reports.
  - Review of process indicators.
  - Update of the information systems catalog.
  - Notifications and announcements to the entity about the start-up of the information system developed, acquired or maintained.

Security Policy

SCM LATAM 2019