InformationSystems Security Policy

Corporate policy of Information Security

At MSLA ID information is a crucial asset for the delivery of its services and the efficient decision-making, which is why there is an explicit commitment to protection of their most significant properties as part of a strategy to the continuity of the business, the management of risks and the consolidation of a culture of security.

Aware of its current needs, MSLA implements a management model of information security as the tool that allows you to identify and minimize the risks to which it is exposed the information, aid for the reduction of operating costs and financial, establishes a culture of security and ensures compliance with the legal requirements, contractual, regulatory and business in force.

The risk analysis process of information assets is the support for the development of the Information Security Policies and controls targets selected for the expected levels of protection in MSLA; this process will be led on a permanent basis by the Information Security Officer.

This policy will be regularly reviewed as part of the management review process, or when changes in the business, its structure, objectives or any condition affecting the policy, to ensure that it remains adequate and adjusted to the requirements identified.

General policies of Information Security

MSLA has established the following policies of General Safety Information, which represent the vision of the company in terms of the protection of their information assets:

1. There will be a security committee of the information, which will be responsible for the maintenance, revision and improvement of Information Security Management System of MSLA.

2. The information assets of MSLA, will be identified and classified to establish the necessary mechanisms of protection.

3. MSLA define and implement controls to protect the information against violations of authenticity, unauthorized access, loss of integrity and to ensure the availability required by customers and users of the services offered by the entity.

4. All staff members and/or partners will be responsible for protecting the information towhich access and processed, to prevent its loss, alteration, destruction or abuse .

5. Audits will be carried out and quarterly checks on the management model of Information Security of MSLA.

6. Is permitted only the use of licensed software that has been lawfully acquired by the Company.

7. It is the responsibility of all staff and partners of MSLA report security incidents, suspicious events and the misuse of resources that identify.

8. The violations of the Security Policies and controls of the information will be reported, registered and monitored.

9. MSLA will have a Business Continuity Plan to ensure the continuity of operations before the occurrence of unanticipated events or natural disasters.

Additionally MSLA account with specific policies and a set of standards and procedures that support the corporate policy.

Confidentiality Agreements

All officials of MSLA and/or third parties must accept the confidentiality agreements defined by the company, which reflect the commitments for the protection and proper use of the information in accordance with the criteria laid down in it.

In the case of partners, the respective contracts should include a clause of confidentiality, similarly when you allow access to the information and/or resources of MSLA to people or external entities.

These agreements must be accepted by each of them as part of the recruitment process, which is why such a clause and/or confidentiality agreement makes it an integral part of each of the contracts.

Risks associated with third parties

MSLA identifies the potential risks that can generate the access, processing, communication or management of the information and the infrastructure for processing by third parties, with the purpose of establishing the necessary control mechanisms to ensure that safety is maintained.

The controls that are established as necessary on the basis of the analysis of risks should be reported to and accepted by the third through the signing of agreements, prior to the delivery of the required access.

Proper use of the assets

Access to the physical documents and digital will be determined by the rules related to the access and restrictions to public documents, to the jurisdiction of the area or specific unit andthe permissions and access levels for staff and partners identified by the heads of area.

For the consultation of uploaded documents in the Document Management software will be established access privileges to the officials and/or partners in accordance with the development of their functions and powers. These privileges will be established by the head or director of the area, who shall report to the group responsible for the administration of the software the listing with officials and their privileges.

All staff and third parties that manipulate information in the development of its functions should sign a "agreement of confidentiality of information", where individually to undertakenot to disclose, use or exploit the confidential information to which they have access, respecting the levels set for the classification of the information; and that any breach of the provisions of this paragraph shall be considered as a "security incident".

Internet Access

The Internet is a working tool that allows you to navigate in many other related sites or not with the activities of the business of MSLA, for which the appropriate use of this resource must be controlled, check and monitor, considering, for all cases, the following guidelines:

A. is not allowed:

- Access to pages related to pornography, drugs, alcohol, webproxys, hacking, and/or any other page that would go against the moral ethics, existing laws or policies established herein.

- The access and the use of instant messaging or interactive services such as Facebook, Whatsapp, MSN Messenger, Yahoo!, Skype and other similar, which aim to create communities to exchange information, or for different purposes in the activities of the business of MSLA.

- The unauthorized exchange of property information of MSLA, its customers and/or its officials, with third parties.

- The download, use, exchange and/or installation of games, music, movies, protectors and funds of screen, free software, information and/or products which in any way infringe the intellectual property of their authors, or that contain executable files and/or tools that are directed against the integrity, availability and/orconfidentiality of the technological infrastructure (hacking), among others. The download, use, exchange and/or installation of audio-visual information (videos and pictures) using public sites on the Internet must be authorized by the Head of the unit concerned and the direction of technology, or to whom they delegate explicitly to this function, associating the procedures and controls required for monitoring and ensuring the proper use of the resource.

B. MSLA must perform permanent monitoring of times of navigation and pages visited on the part of officials and/or third parties. We can also inspect, record and assess the activities carried out during the navigation, according to the national legislation in force.

C. Each user is responsible for providing adequate use of this resource and at no time can be used to perform illegal practices or bad intentions that are directed against third parties, the legislation in force and the guidelines for information security, amongothers.

D. Officials and third parties, as well as the employees cannot assume on behalf ofMSLA, personal positions in opinion polls, forums or other similar means.

E. The use of the Internet are not considered within the previous restrictions, is always allowed and when you perform in an ethical manner, reasonable, responsible, not abusive and without affecting the productivity or the protection of the MSLA Information International.

Email

The officials and authorized third parties to whom MSLA assigned an email account must follow the following guidelines:

A. The email account must be used for the performance of the functions assigned within MSLA, it may be used for personal use, always and when you perform in an ethical manner, reasonable, responsible, not abusive and without affecting productivity.

B. The messages and information contained in the mailboxes are the property of the MSLA and each user, as responsible for your mailbox, you must maintain only the messages related to the development of its functions.

C. The size of the mailboxes is determined by the VP of systems according to the needs of each user and with authorization from the head of the relevant unit.

D. The size for sending and receiving messages, its contents and other inherent characteristics of these shall be defined and implemented by the VP of systems.

E. is not allowed:

- Chains send mail, messages with religious content, political, racist, sexist, pornographic, non-corporate advertising or any other type of messages that violate the dignity and the productivity of the people or the normal performance of the e- mail service onthe Company, malicious messages that can affect the internal systems or of third, messages that go against the law, the morals and the good customs and messagesthat incite to perform illegal practices or promote illegal activities.

- Use the email address of MSLA as the point of contact in interactive communities of social contact, such as *Facebook, Whatsapp, Skype* among others, or any other site that does not have to do with the working activities.

- The sending of files that contain executable extensions, under any circumstances.

- The sending of music files and videos. In case you require to make a shipment of files of this type should be authorized by the respective direction and the VP of systems.

F. Sending corporate information must be made exclusively from the email account that MSLA provides. Similarly, the generic email accounts should not be used for personal use.

G. Massive deployment of corporate advertising messages must be approved by the General Management and authorization of the VP of systems. In addition, third party should include a message that tells the recipient as to be removed from the distribution list. If a unit should, by any circumstance, perform mass mailing , so frequent, this must be sent through an email account in the name of the respective dependence and/or service enabled for that purpose and not through email accounts assigned to a particular user.

H. Any information of MSLA generated with the different computer programs (e.g. Office, Project, Access, Wordpad, etc.), which requires to be sent outside of the entity, andthat by their characteristics of confidentiality and integrity should be protected, must be in a format not editable, using the security features that provide the tools provided by theVP of systems. The information may be sent in the original format under the responsibility of the user and only when the receiver is required to make modifications to this information.

I. All the messages sent must respect the standard format and corporate image defined by MSLA and should retain in all cases the corporate legal message confidentiality.

Technological Resources

The proper use of technological resources allocated by MSLA to its officials and/or third parties is regulated under the following guidelines:

A. The installation of any software or hardware in the computer equipment of MSLA is the responsibility of the VP of systems and therefore are the only ones authorized to perform this work. Likewise, the installation media for software must be those provided by MSLA through this address.

B. Users should not make changes to the workstations associated with the configuration of your computer, such as network connections, local users of the machine, wallpaper and screen saver corporate, among others. These changes can be made only by the VP of systems.

C. The VP of systems must define and update on a regular basis, the list of authorized software and applications that are allowed to be installed on the users' workstations. Likewise, perform the control and verification of compliance with the licensing of the respective software and associated applications.

D. Only officials and third parties authorized by the VP of systems, upon written request by the unit that requires it, can connect to the wireless network of MSLA.

E. The connection to external wireless networks for users with mobile computers that are out of the office and that require to establish a connection to the technological infrastructure of MSLA, must use a connection under the schemes and security tools authorized and established by the VP of systems.

F. Only authorized personnel can perform remote administration activities of devices, computers or servers in the infrastructure of information processing of MSLA; the connections established for this purpose, must use the schemas, security and management tools defined by the VP of systems.

G. Synchronization of mobile devices such as PDAs, smartphones, cell phones or other electronic devices on which you can perform exchanges of information with any resource of the Organization, must be explicitly authorized by the respective dependence, in conjunction with the VP of systems and may be carried out only on devices provided by the organization for that purpose.

Physical Access Control

All areas intended for the processing or storage of sensitive information as well as those that are the equipment and other infrastructure to support the information and communication systems are considered to be areas of restricted access. They must therefore have measures of physical access control at the perimeter such that they can be audited, as well as with operational security procedures to protect the information, the software and the hardware of intentional or accidental damage.

Similarly, the tallying centers, wiring and technical rooms of the offices should have mechanisms to ensure compliance with the environmental requirements (temperature, humidity,etc.), specified by the manufacturers of the computers that host and that can respond appropriately to incidents such as fires and floods.

Protection and location of the equipment

The computers that are part of the technological infrastructure of MSLA such as, servers, communications equipment and electronic security, centers of wiring, UPS, electricalsubstations, air conditioners, plants calls, as well as workstations and storage devices and/or mobile communication containing and/or provide services to support the critical information of the units, should be located and adequately protected to prevent the loss, damage, theft or unauthorized access of the same. Similarly, we must adopt the necessary controls to keep equipment away from sites that may be at risk of potential threats such as fire, explosives, water, dust, vibration, electromagnetic interference and vandalism, among others.

The officials and third parties, including their employees or partners, that have access to the computers that make up the technological infrastructure of MSLA cannot smoke, drink or eat any type of food near the equipment.

MSLA through appropriate mechanisms will monitor the environmental conditions of the areas where they are the equipment (Counting Centers).

Segregation of Duties

Every task in which the officials have access to the technological infrastructure and information systems, must have a clear definition of the roles and responsibilities, as well asthe level of access and the relevant privileges, in order to reduce and prevent the unauthorized use or modification of the information assets of the Organization.

In concordance:

- All systems of critical availability or average of the company, must implement the access rules in such a way that there is segregation of duties between those who manage, operate, maintain, audit and, in general, have the possibility of accessing information systems, as well as between who granted the privilege and who uses it.

- The Executable modules should never be transferred directly from the libraries of evidence to the libraries of production without that previously are compiled by the area allocated for that purpose, that at no time shall be the area of development or production.

- The level of super user of the systems must have a dual control, in such a way that there is an oversight to the activities performed by the system administrator.

- Must be clearly segregated the support functions, planners and operators.

Protection against malicious software

MSLA establishes that all computing resources must be protected using tools and security software such as antivirus, antispam, Anti-Spyware and other applications that provide protection against malicious code and prevention of the entry of the same to the company network, where they have the appropriate controls to detect, prevent and recover potential failures caused by malicious and mobile code. It will be the responsibility of the VP of systems toauthorize the use of the tools and ensure that these and the security software are not disabled under any circumstances, as well as its continuous updating.

Likewise, MSLA defines the following guidelines:

is not allowed:

- The uninstallation and/or disabling of security software and tools previously backed by MSLA.
- Write, generate, compile, copy, propagate, run or attempt to enter any programming code designed for auto replicated, harm or affect the performance of any device or technological infrastructure.
- Use storage media physical or virtual non-corporate.
- The use of mobile code. It may be used only if it operates in accordance with the policies and safety standards defined and duly authorized by the VP of systems.

Backup Copies

MSLA must ensure that the information with a certain level of classification, defined together by the VP of systems and units responsible for the same, contained in the technological platform of the company, as servers, network devices for storage of information, workstations, configuration files for network devices and security, among others, should be regularly protected through mechanisms and adequate controls to ensure their identification, protection, integrity and availability. In addition, it shall establish a plan for the restoration of backups that will be tested at regular intervals in order to ensure that they are reliable in case of emergency and retained for a period of time.

The VP of systems shall establish procedures explicit of guard and retrieval of information that include specifications on the transfer, frequency, identification and defined in conjunction with the units retention periods for the same. Additionally, you must have the resources necessary to enable the identification related to the storage media, the information contained in them and the physical location of the same to allow a rapid and efficient access to the media containing the information protected.

The magnetic media that contain critical information must be stored in a different location to the facilities where is ready. The external site where you protect those copies, must have appropriate security controls, comply with maximum measures of physical protection and safety appropriate.

Management of removable media

The use of removable storage media (example: CDs, DVDs, USBs, flash memories, external hard drives, Ipods, cell phones, tape) on the infrastructure for processing the information of MSLA, will be authorized for those staff members whose profile of the position and functions requires it.

The VP of Systems is responsible for implementing the controls necessary to ensure that in the information systems of the MSLA only authorized officials can make use of the removable storage media.

Likewise, the official undertakes to ensure the device is physically and logically so as not to put at risk the information of MSLA it contains.

Exchange of information

MSLA will sign confidentiality agreements with employees, customers and third parties who for different reasons require knowing or exchange restricted information or company-confidential. In these agreements shall be specified the responsibilities for the exchange of information for each of the parties and must sign before allowing access or use of such information.

Any official of MSLA is responsible for protecting the confidentiality and integrity of the information and special care should be taken in the use of different means for the exchange of information that could generate a disclosure or unauthorized modification.

The owners of the information that is required to exchange are responsible for defining the levels and profiles of authorization for access, modification and deletion of the same and the custodians of this information are responsible for implementing controls to ensure compliance with the criteria of confidentiality, integrity, availability and required.

Logical Access Control

Access to platforms, applications, services and in general any information resource of MSLA must be allocated according to the prior identification of security requirements and business thatwill be defined by the different units of the company, as well as legal rules or laws applicable to the protection of access to the information present in the information systems.

Those responsible for the management of the technological infrastructure of MSLA assigned access to platforms, users and network segments according to formal processes of authorization which must be reviewed periodically by the General Management of MSLA.

The authorization for access to information systems must be defined and approved by the unit that owns the information, or whom it define, and should be granted in accordance with the level of classification of the information identified, according to which we should determine the controls and access privileges that can be granted to officials and third parties and implemented by the VP of systems.

Any internal or external user that requires remote access to the network and to the infrastructure of information processing of MSLA, either from the Internet, access by telephone or by other means, must always be authenticated and their connections shall use data encryption.

User Password Management

All the resources of information critical of the MSLA are assigned the access privileges of users based on roles and profiles that each member of staff required for the development of its functions, as defined and approved by the business areas and managed by the VP of systems.

Any official or third party that requires access to the information systems of the MSLA should be duly authorized and must have access to these systems by making use of at least one user (ID) and password (password) assigned by the Organization. The officer should be responsible for the proper use of the access credentials assigned.

Desktop and clean screen

In order to avoid losses, damages or unauthorized access to information, all officials of MSLA must maintain the restricted information or confidential under key when their jobs are neglected or in-hours. This includes: printed documents, CDs, USB storage devices and removable media in general. Additionally, it is required that the sensitive information that is sent to the printers is collection immediately.

All users are responsible for blocking the meeting of your workstation at the time it waswithdrawn from the job, which you will be able to unlock only with the password for the user. When they finish their activities, you must close all applications and leave the equipment off.

All workstations must use the wallpaper and screen saver corporate, which will be activated automatically after five (5) minutes of inactivity and you can unlock only with the password for the user.

Segregation of networks

The technological platform of MSLA that supports Information systems should be separated into segments of physical and logical network and independent of network segments of users, connections to networks with third parties and the Internet access service. The division of these segments must be carried out by means of devices Internal and perimeter security routingand if so required. The VP of systems is the area responsible for establishing the security perimeter necessary to protect those segments, according to the level of criticality of the flowof the information transmitted.

MSLA establishes mechanisms for the automatic identification of computers on the network, such as means for authenticating connections, from specific network segments to the platforms where they operate the information systems of the Organization.

It is the responsibility of the administrators of technological resources to ensure that the physical and logical ports of diagnostic and configuration of platforms that support information systems should always be restricted and monitored in order to prevent unauthorized access.

Identification of security requirements

The inclusion of a new product of hardware, software, application, internal or external development, changes and/or updates to existing systems in MSLA, must be accompanied by the identification, analysis, documentation and approval of the safety requirements of the information, work that should be the responsibility of the VP of units and systems owners of the system in question.

The safety requirements of the identified information, obligations arising from the laws of intellectual property and copyright should be set out in the contractual agreements that are made between MSLA and any supplier of products and/or services associated with the infrastructure of information processing. It is the responsibility of the VP of systems ensure the definition and implementation of the safety requirements of the information and in conjunction with the General Management to establish these aspects with the specific contractual obligations.