INFORMATION SECURITY POLICY

1. OBJECTIVE

In order to fulfill its mission of providing relocation services, corporate services and migratory assistance to natural persons, companies, officials and their families at the national and international levels, through highly qualified professionals, who, with a humane approach, ensure that the relocation of a transferee and his or her family is carried out efficiently and effectively, LARM has developed an Information Security Management System that enables it to ensure the preservation of confidentiality, integrity and availability of company and stakeholder information. To achieve the proposed purposes LARM commits to:

- The satisfaction of the applicable requirements related to the security of the information of the Company and the interested parties.
- The integration of information security into the Company's risk management culture.
- Ensure that Information Security requirements are integrated into the contractual processes (employees and third parties) that are carried out by the Company.
- Comply with applicable legal regulations and other contractual requirements that the Company has with third parties related to the security of information.
- Continuous improvement and expected performance in all Company processes.

The Information Security Management System Policy, with its respective rules, standards, procedures and other documents that are generated and supported by this system, are mandatory for employees and in general, any natural or legal person accessing any information asset. The implementation of actions that violate confidentiality, availability, integrity and privacy of the information will result in a disciplinary action that may extend to the termination of the employment contract and the possible establishment of a judicial process under national or international laws that apply.

The Information Security Management System Policy is part of the Management Review procedure and is expressly disseminated to all Company staff and stakeholders.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

2. SCOPE

This Information Security Policy will be applied to all administrative, management, logistical and control aspects set by the company, which must be fulfilled by the managers, officials, contractors, third parties who provide their services, employees of third-party suppliers who are regulated by contractual terms, and in general all those persons who have some kind of relationship with the manipulation of information in LARM COLOMBIA S.A

3. SPECIFIC POLICIES FOR THE PROCESSING OF PERSONAL DATA.

3.1 SOFTWARE INSTALLATION

Purpose: To minimize the risk of exposure and infection by malware, while avoiding possible sanctions for the use of unlicensed software.

Policy

Workers must not install software on the company's devices without authorization. Requests for software installation must be approved by management and the installation process must be carried out by the company's qualified personnel. Any software that is installed must have a commercial license, be free license (open source, free trial), or, failing that, the license must come from the technology department.

3.2 USE OF EXTERNAL STORAGE DEVICES

Purpose: To minimize the risk of exposure of company information or malware infection contained in external storage devices (External Hard Drives, USBs, CDs, Diskettes, Cell Phones, Media Players, etc.).

Policy

The use of personal storage devices within the company's technological infrastructure is prohibited. If any of these devices are required, they must be borrowed from the corresponding area managers. Once the required work is completed with the device, all the information contained in it must be deleted, cleaned with antivirus software and returned to the maintainer.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

3.3. USE OF THE BUSINESS INTERNET AND MONITORING POLICY

Purpose: The purpose of this policy is to define the standards for monitoring and limiting Internet browsing from any device in the enterprise network. These standards are designed to ensure that employees use the Internet safely and responsibly.

Policy

Management is empowered to monitor all incoming and outgoing communications within the organization's network. This includes knowing the source IP, date, time, protocol, server or destination address and the data reported.

Management may block Internet sites deemed inappropriate for the business environment. Access to websites and websites with explicit sexual content, gambling or betting sites, websites related to illicit substances, dating sites and social networks is considered a disciplinary offence under any circumstances, fraud sites, SPAM content or in relation to offences under Colombian law, content that is racist or in any way offensive and discriminatory, violent content, and any content not related to the development of the purposes of the company without prior authorization.

Likewise, the use of business infrastructure to carry out computer attacks or similar is totally prohibited. In addition, the use of the Internet during unauthorized hours to access multimedia content not associated with the employee's work is prohibited. Any attempt to evade the technical controls imposed will in itself be considered a disciplinary offence.

3.4 USE OF E-MAIL AND PERSONAL COMMUNICATIONS

Purpose: To prevent damage to the image or the name of the organization due to improper management of communication services.

Policy

The various means of communication available to workers must not be used for the distribution of messages with offensive, racist, discriminatory, pornographic, sexual content, policy, etc. Employees who receive communications with this content must remove it immediately and report the incident if it is of internal origin.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

Using business emails for personal communications is prohibited. Especially if it is for the distribution of chain messages, spam or in some commercial way.

Employees should not expect any privacy in content they store or ship as part of the company's communication services. Failure to comply with the above-mentioned conditions is considered a disciplinary offence and is liable to punishment.

3.5 BACKUP COPIES

Purpose: To avoid loss of company information.

Policy

The backup copies of the information will be taken automatically every day, to the databases with accounting, administrative and operational information of the company. Backups shall be stored in digital media and shall be guarded for an unlimited period.

The officials responsible for managing the storage and backup of the information shall provide the necessary resources to ensure the proper processing of the information.

The owners or persons responsible for the assets of technological information and computer resources must define the strategies for the correct and adequate generation, retention, and rotation of the backup copies of the information.

The owners or persons responsible for the assets of technological information and computer resources must ensure compliance with the procedures for supporting the information.

3.6 KEY HANDLING

Purpose: The purpose of this policy is to establish a standard for the generation of secure passwords, the protection of such passwords and their frequency of change.

Policy

All system level passwords (root, administrator, windows users, etc., databases) must be changed at least every 6 months.

All user level passwords (mail, personal accounts) must be changed at least every 3 months.

All passwords used must follow the conditions described below: Contain at least three of the following characters: Lowercase, Shift, Numbers, Special characters (e.g. #$%&/("!!. ;), the length of the password must be at least 8 characters, the password must not be composed only of dictionary words, traditional passwords such as password, 123456, qwerty, asdfg, etc.

As a basis for the correct handling of keys and passwords, a series of recommendations are presented for the correct handling of them:

- Always use different passwords for the company's services and your personal accounts unrelated to the work environment.
- Do not share your passwords with any third parties, even if they belong to the organization.
- Passwords should never be written in plain text (never files called.txt keys and on the desktop).
- Do not reveal passwords by unprotected media such as mail, instant messaging, SMS, etc.
- Avoid using the option of remembering password in browsers and internal programs.

3.7 ACTIVITY REGISTER AND SUPERVISION

Purpose: To record events and generate evidence.

Policy

There will be regular and careful reviews of recorded event logs of user activities, exceptions, failures, and information security events. Information records shall be protected against manipulation and unauthorised access.

The activities of the system administrator and the network shall be recorded.
Estos registros serán protegidos y regularmente revisados.

Clocks from all relevant computer systems will be synchronized to a single reference time source.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

3.8 PHYSICAL AND ENVIRONMENTAL SECURITY

Purpose: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.

Policy

Computer equipment should be located and protected to reduce the risks of environmental threats and risks and opportunities for unauthorized access. Equipment shall be protected against power failure and other interruptions caused by failures in the support of utilities. Cabling that transports data, energy and telecommunications or the support of information services must be protected against interception, interference or damage. Computer equipment must be properly maintained to ensure its continued availability and integrity.

Equipment, information or software shall not be removed from the premises of the company without prior authorisation. Security shall be applied to assets outside the premises, taking into account the different risks of working outside the premises of the organisation.

All items of equipment containing the storage media shall be verified to ensure that sensitive data and licensed software have been safely deleted or overwritten before disposal or reuse..

Users should ensure that equipment not under surveillance is adequately protected.

Workstations must be clean of paper, removable storage media and when a computer is unattended the screen must be locked.

Where appropriate, papers and media should be secured in special lockers, especially during off-duty hours.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

3.9 REQUIREMENTS FOR ACCESS CONTROL

Purpose: To limit access to information and information processing facilities.

Policy

Workers are required to monitor and ensure compliance with the following security measures:

- *Access to secure areas where confidential and restricted information is processed or stored is limited to authorized persons only.*
- *Access to secure areas requires access control schemes, such as cards, keys or padlocks.*
- *The person in charge of a secure area must ensure that cameras, videos, mobile phones with cameras do not enter, unless they have an express authorization.*
- *Forms are used to record the entry and exit of staff.*
- *Physical access is restricted to devices such as: wireless access points, network gateway and network terminals located in secure areas.*

3.10 REQUIREMENTS FOR ACCESS CONTROL

Purpose: To limit access to information and information processing facilities.

Policy

Workers are required to monitor and ensure compliance with the following security measures:

- *Access to secure areas where confidential and restricted information is processed or stored is limited to authorized persons only.*
- *Access to secure areas requires access control schemes, such as cards, keys or padlocks.*
- *The person in charge of a secure area must ensure that cameras, videos, mobile phones with cameras do not enter, unless they have an express authorization.*
- *Forms are used to record the entry and exit of staff.*
- *Physical access is restricted to devices such as: wireless access points, network gateway and network terminals that are located in secure areas.*

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

3.11 REQUIREMENTS FOR ACCESS CONTROL

Purpose: To limit access to information and information processing facilities.

Policy

Workers are required to monitor and ensure compliance with the following security measures:

• Access to secure areas where confidential and restricted information is processed or stored is limited to authorized persons only.
• Access to secure areas requires access control schemes, such as cards, keys or padlocks.
• The person in charge of a secure area must ensure that cameras, videos, mobile phones with cameras do not enter, unless they have an express authorization.
• Forms are used to record the entry and exit of staff.
• Physical access is restricted to devices such as: wireless access points, network gateway and network terminals that are located in secure areas.

3.12 ACCESS TO SENSITIVE EMPLOYEE DATA.

Purpose: To ensure that sensitive data related to health, religious, political, sexual, and other worker data can only be known by competent and relevant personnel by virtue of their functions, taking into account the Restricted Access principle.

Policy

The purposes for which sensitive data are processed in the company are limited and specified in the respective authorizations granted by the owner of the information.

In general, the processing of sensitive data in the company will be limited only to the areas of Human Management and Directorate General, taking into account the particular purposes authorized by the owner.

The company in a particular way and in the respective manuals of functions according to the position, will determine those particular charges that may have access to sensitive data, without that access means a violation of the restricted access security policy. Likewise, they apply the security mechanisms previously identified as restricted access to personal data.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

3.11. INFORMATION SECURITY AROUND HUMAN RESOURCES

In the processing of personal data, before, during and after the employment relationship, will be governed by the following rules:

- **LARM COLOMBIA S.A.S.** will inform the persons interested in participating in a selection process, the rules applicable to the processing of personal data provided by the interested party during the respective selection process, as well as of those data obtained during the performance of the same.

- The processing of the data provided by those interested in the vacancies of LARM COLOMBIA S.A.S. and those obtained from the selection process, will be only the one informed in the authorization to the applicant.

- The company will carry out security studies prior to hiring new staff for the company.

- Once an applicant has been selected to fill a position at LARM COLOMBIA S.A.S., the respective employment contract, confidentiality agreement and will be assigned when the position requires it, a user with a defined profile directly related to the position to be held, which will allow access to personal information processed by the company, when the position so requires.

- Selected the candidate for the position, the company will store the personal data of the worker in a folder identified with the name of each person. Only the Area of Human and Administrative Management will have access to this folder and in order to manage the employment relationship between the company and the employee.

- When LARM COLOMBIA S.A.S., requires contracting external services for the processing of data during the contractual relationship with the workers, the transfer of personal data to a third party may be required to be called Data Controller, In this case, the company will follow the guidelines for the selection of Managers in the transmission of personal data contained in this policy.

- Upon termination of the employment contract, the company will enter into a confidentiality agreement with the former employee to safeguard the confidentiality of the personal information handled by the former employee; as well as request the delivery of forms of profiles and passwords that have been assigned to you during the execution of the employment contract.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

3.12 CONFIDENTIALITY WITH THIRD PARTIES

Purpose: To establish confidentiality requirements in relationships with suppliers, contractors, in particular employees and third parties in general.

Policy

For the development of contractual, commercial and labour relations, third parties should be required to accept confidentiality agreements defined by the organization.

Such agreements should establish a commitment to safeguard the information, ensure its correct use, prevent the unauthorized use of such information and keep it confidential. In turn, the information that is protected under the agreement and its temporality should be stipulated.

Agreements should be included in contracts concluded between the organisation and third parties as an integral part of the contract or signed as a separate agreement.

Acceptance of the confidentiality conditions is essential to grant the third party access to the protected information.

3.13 SELECTION OF DATA CONTROLLERS FOR THE TRANSMISSION OF PERSONAL DATA

Purpose: To ensure that at events where personal data is transferred, the data controller is chosen taking into account the prerogatives that are dealt with in the regulations on the protection of personal data.

Policy

LARM COLOMBIA S.A.S. as responsible for the processing of personal data, when making Transmission of personal data, it is imperative compliance by the company, follow the following guidelines:

• Determine the scope of the treatment to be allowed to the Manager.

• To assess the competence and ability of the Data Controller to carry out the processing that will be entrusted to him

•To review the Data Controller's own manual of personal data processing policies.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

• *Examine the security measures implemented by the Data Controller for the processing of personal data, and their compatibility with the standards determined by LARM COLOMBIA S.A.S.*

• *Sign a contract for the transmission of personal data.*

• *Conduct audits to measure the level of protection*

3.14 INFORMATION SECURITY REVIEWS

Purpose: To ensure that IT security is implemented and applied in accordance with the organization's policies and procedures. Politics

Policy

Information systems are regularly reviewed through Audits to ensure compliance with the entity's information security policies and standards.

4. PROCESS FOR HANDLING INCIDENTS

Whenever an incident occurs with the security of the information processed by **LARM COLOMBIA S.A.S.**, the following procedure must be carried out:

1). **Incident Report:** Once the security incident has occurred, the first person who has knowledge of it must immediately notify the address of what happened, and prepare a detailed report on the facts of the incident within 24 hours of its occurrence.

2). **Communication of the Incident to the SIC:** Any information security incident must be reported to the Superintendence of Industry and Commerce, specifically to the National Database Registry -RNBD-. The reporting of incidents is an obligation of the Supply & Accountant Manager who must do so once they have been notified of the occurrence of the incident by any area of the company.

3). **Meeting of the Information Security Committee:** The area or person in charge of information security and management will call an extraordinary meeting in which the following items will be evaluated, among others:

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

a. **Issue of the technical concept:** Evaluated the Facts of the case a technical concept must be given that determines all the contingencies arising in the specific case.
b. **Identification of the flaw:** As a result of the technical concept, the flaw that gave rise to the information security incident must be fully identified.
c. **Taking of Action:** The committee shall take the necessary measures and corrective measures to avoid future incidents.

5. MODIFICATION OF POLICIES

LARM COLOMBIA S.A.S. reserves the right to amend this Information Security Policy at any time, communicating in a timely manner to all those persons who are related or involved in the manipulation of the company's information for its correct implementation.

6. DURATION

This Policy applies from 5 January 2022.

LARM Colombia
Carrera 14 # 99-33 Of. 403
Bogotá- Colombia
(571)2570488 | (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com