1. Policy Statement

ALGI is committed to ensuring data protection and compliance with ISO 17021:2015 Conformity Assessment – Requirements for bodies providing audit and certification of management systems, ISO 9001:2015 Quality Management Systems, ISO/IEC 27001 Information security management, SA8000 advisories, BSCI protocols, and applicable international Personal Data Protection Dispositions with regards to data collection and processing. ALGI releasese the **General IT Policy** as a conceptual umbrella and conduct parameter for all ALGI employees and relevant stakeholders.

ALGI has in place data protection, confidentiality and disclosure procedures to which all ALGI personnel abide by. Such dispositions cover all aspects of information within the organization. In order to guarantee the effectiveness of the programs and controls implemented to safeguard information (such as the IT01 Information Security Management Procedure), **ALGI requieres that all employees respect all the provisions set forth in the** ALGI IT General Policy.

2. Objective

To guarantee that ALGI has effectively communicated the mechanisms globally implemented to safeguard personal data protection and information security.

To provide ALGI members with the required directives they shall abide by, in order to comply with ALGI global requirements on personal data protection and information security.

3. Scope

This policy applies to all ALGI employees and external contractors (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to ALGI business activities worldwide, and to all information handled by ALGI relating to other organisations with whom it deals. It also covers all IT documentation and communications operated by ALGI or on its behalf.

4. General Provisions

ALGI has in place data protection, confidentiality and disclosure procedures to which all ALGI personnel abide by. Such dispositions cover all aspects of information within the organization, including (but not limited to):

- Staff/client/service user information
- Personal information
- Organisational information
- Information and personal data gathered in the auditing process

- If applicable, personal data gathered by means of an external stakeholder complaint/concern/certification appeal.

In order to guarantee the effectiveness of the programs and controls put forward to safeguard information (especially regarding procedure IT01 Information Security Management), **ALGI requieres that all employees respect the following provisions:**

- Information shall not be shared with or disclosed to any external or internal individual that requieres so without having a previous formally and written consent by Top Management.
- Information will only be relesead if a deemed authority formally requieres so and all interested parties are informed and have formally approved.
- Information shall not be duplicated.
- Information must be kept, centralized and controlled by the ALGI Suite Software and it shall be not locally stored in personal devices or any unauthorized device.
- Commercial and sales department is independent from Operations.
- Impartiality Risk Assessment with focus on data protection risk based approach is performed periodically.
- All ALGI services and Activities shall be registered in our webApp worldwide accessible management system software; ALGI Suite.
- ALGI recognizes strictly the Corporation's official email domain in its communications.

4.1. Specific provisions regarding software usage

4.1.1. ALGI Suite and ALGI Email Account Access Control

Individual's Access to the ALGI Suite and Email account (hereafter referred to as 'ALGI IT System) is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the ALGI IT systems.

Individuals must not:

4.1.1.1. Allow anyone else to use their user ID/token and password on any ALGI IT system or Email account.
4.1.1.2. Leave their user accounts logged in at an unattended and unlocked computer.
4.1.1.3. Use someone else's user ID and password to access ALGI IT systems.
4.1.1.4. Leave their password unprotected (for example by having it written down).
4.1.1.5. Perform any unauthorised changes to ALGI IT systems or information.
4.1.1.6. Attempt to access data that they are not authorized to use or access.
4.1.1.7. Exceed the limits of their authorization or specific business need to interrogate the system or data.
4.1.1.8. Connect any non-ALGI authorised device to the ALGI network or IT systems.

4.1.1.9. Store ALGI data on any non-authorised ALGI equipment.

4.1.1.10. Give or transfer ALGI data or software to any person or organisation, outside ALGI without the authorization of ALGI. Supervisors, country managers or regional managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

4.1.1.11. Every document generated by ALGI IT system has a control code that permits validate the genuinity of the document. Thus, you might never alter sensible documents such as TORs, recepts, audit plans, etc.

4.1.1.12. Cooperate with IT designated staff whenever they ask ALGI employee to change user's passowrds (ALGI International personnel's password would requiere update every three months, for the rest of the regions every month).

4.1.1.13. IOS and windows are the prefered operating system.

4.1.1.14. Webapplications are optimized to be worked on Chrome internet browser.

4.1.2. ALGI Internet and email Conditions of Use (During working ours and outside working ours)

Use of ALGI internet and email is intended for business matters only. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to ALGI in any way, not in breach of any term and condition of employment and does not place the individual or ALGI in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

4.1.2.1. Use the internet or email for the purposes of harassment or abuse.

4.1.2.2. Use profanity, obscenities, or derogatory remarks in communications.

4.1.2.3. Access, download, send or receive any data (including images), which ALGI considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.

4.1.2.4. Use the internet or email to make personal gains or conduct a personal business.

4.1.2.5. Use the internet or email to gamble.

4.1.2.6. Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

4.1.2.7. Place any information on the Internet that relates to ALGI, alter any information about it, or express any opinion about or in behalf of ALGI, unless they are specifically authorised to do this.

4.1.2.8. Send unprotected sensitive or confidential information externally.

4.1.2.9. Forward ALGI mail to personal (non-ALGI) email accounts (for example personal hotmail account).

4.1.2.10. Make official commitments through the internet or email on behalf of ALGI unless authorised to do so.

4.1.2.11. Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list), even to personal devices, without appropriate approval.
4.1.2.12. Incur in any way of infringing any copyright, database rights, trademarks or other intellectual property.
4.1.2.13. Download any software from the internet without prior approval of the IT Department.
4.1.2.14. Connect ALGI devices to the internet using non-standard connections.
4.1.2.15. Open ALGI accounts/Profiles and participate on social networks on behalf of ALGI without explicit permission.
4.1.2.16. In general, take advange of ALGI hardware, software or IT human resources for deviated purposes other than ALGI Business.
4.1.2.17. Forget to use the official distribution lists as specified by ALGI HQ for external communications.
4.1.2.18. Use other employee's digital signature without written consent of the employee and the formal authorization by a relevant manager.

4.1.3. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, ALGI enforces a clear desk and screen policy as follows:

4.1.3.1. Personal or confidential business information must be protected using security features provided for example secure print on printers.
4.1.3.2. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
4.1.3.3. Care must be taken to not leave confidential material on printers or photocopiers.
4.1.3.4. All business-related printed matter must be disposed of using confidential waste bins or shredders.
4.1.3.5. Weekly perform information backup on ALGI authorized storage device.

4.1.4. Working Off-site

It is accepted that laptops and mobile devices will be taken off-site.
The following controls must be applied:

4.1.4.1. Equipment and media taken off-site must not be left unattended in public places and not left in sight in any means of transportation (car, plane, train, bus).
4.1.4.2. Laptops must be carried as hand luggage when travelling.
4.1.4.3. Information should be protected against loss or compromise when working remotely (for example at home or in public places).
4.1.4.4. Mobile Storage Devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.

4.1.4.5. All ALGI equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and cameras, must be returned to ALGI at termination of contract. All ALGI data or intellectual property developed or gained during the period of employment remains the property of ALGI and must not be retained beyond termination or reused for any other purpose.

5. Final Remarks

All data that is created and stored on ALGI computers is the property of ALGI. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. ALGI has the right (under certain conditions) to monitor activity on its system, including internet and email use, in order to ensure system security and effective operation, and to protect against misuse.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with ALGI disciplinary procedures.