IT Security Policy (Externals and Third Parties)

CIRCULATION	
For the application: All PUBLIC	**For more information: All company**

All document modifications must be tracked and reported below:

Version	Author	Date	Object
V.1.0	Christian Koschmieder	28/08/2024	Creation

Version	validator	Role	Date	Object
V1.0	Christian Koschmieder	CISO	28/08/2024	Validation
V1.0	Alberto Mendez	CEO	28/08/2024	Validation
V 2.0	Christian Koschmieder	CISO	17/09/2024	Modification
V 2.0	Alberto Mendez	CEO	17/09/2024	Validation

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OBJECTIVE

The main objective of this External Annex to Plexigrid IT Security Policy (hereinafter referred as “Policy”) is to define the basic principles and rules for information security management for Externals. This Policy outlines the guidelines and procedures for Externals to ensure the confidentiality, integrity, and availability of our organization's information and systems.

The final objective is to ensure that Plexigrid guarantees the security of the information and minimizes the risks derived from an impact caused by ineffective information management.

1.2 SPECIFIC OBJECTIVES

- Have adequate platforms that protect the processing, storage, and communication mechanisms where the services provided by Plexigrid are contained and supported.

- Educate Externals to achieve an information security culture reflected in the acceptance and application of security guidelines.
- Educate Externals to achieve competent and committed, with a culture of information security reflected in the acceptance and application of security guidelines.
- Implement an information security risk management methodology as a tool to act proactively in situations that may affect the continuity, confidentiality, and integrity of information in Plexigrid.

1.3 DOCUMENT SCOPE

This Policy establishes the criteria and behaviours that must followed to preserve the security of information in Plexigrid by Externals and third parties.

1.4 POLICY SCOPE

This Policy applies to all Externals.
External is understood as any non-employee who have access to Plexigrid organization's information and systems, including Contractors, Vendors, Partners, Consultants, Temporary workers and Interns.
If the External is provided with Plexigrid's computer equipment and a Plexigrid e-mail account, the Plexigrid IT Security Policy will be applicable to him/her, with the exception, regarding labour law, of the disciplinary system for non-compliance.
All Externals must meet these minimum requirements without prejudice to having more restrictive policies and improving security to the extent possible. Additionally, projects in other countries must adapt and develop this policy and must inform the Plexigrid Steering Committee of its adequacy, in execution of the monitoring processes of the incident management system.

The scope of this Policy covers all Plexigrid information and services regardless of the way it is processed, who accesses it, the medium that contains it or the place where it is located, whether it is printed or stored information.

The Policy must be mentioned on the Plexigrid corporate website, www.plexigrid.com. But should not be published or shared without the CISO allowance and knowledge.

This Policy must follow an update process subject to relevant organizational changes: growth of the staff, changes in the computing infrastructure, development of new services, among others.

All Externals must acknowledge that they have read, understood, and will comply with this Policy before being granted access to Plexigrid’s systems and information through signing the last page of the Policy Non-employees

Once signed, Admin department will take care of the signed document.

For those Externals who provided services to Plexigrid prior to the approval of this Policy, they must sign it as soon as possible and send to Admin department.

1.5 INFORMATION POLICY PRINCIPLES

This Policy responds to the recommendations of the best Information Security practices contained in the International Standard ISO/IEC 27001, as well as compliance with current legislation on the protection of personal data and regulations that, in the field of Information Security, it may affect Plexigrid.

Plexigrid establishes the following basic principles as fundamental information security guidelines that must always be kept in mind in any activity related to information processing:

- Strategic scope: Information security must have the commitment and support of all Plexigrid managers, so that it can be coordinated and integrated with the rest of the strategic initiatives to form a fully coherent and effective framework.
- Comprehensive security: Information security will be understood as a process system made up of technical, human, material, and organizational elements, avoiding, except in cases of urgency or necessity, any specific action or conjunctural treatment. Information security must be considered as part of normal operations, being present and applied throughout the process of design, development, and maintenance of information systems.
- Risk management: Risk analysis and management will be an essential part of the information security process. Risk management will allow the maintenance of a controlled environment, minimizing risks to acceptable levels. The reduction of these levels will be carried out through the deployment of security measures, which establish a balance between the nature of the data and the treatment, the impact, and the probability of the risks to which they are exposed and the effectiveness and cost of security measures.
- Proportionality: The establishment of protection, detection and recovery measures must be proportional to the potential risks and the criticality and value of the information and services affected.
- Continuous improvement: Security measures will be periodically reassessed and updated to adapt their effectiveness to the constant evolution of risks and protection systems. Information security will be addressed, reviewed, and audited by qualified personnel.
- Security by default: Systems must be designed and configured in such a way that they guarantee a sufficient degree of security by default.
- Documentation: To assure the security, robustness, and reliability of the system, is mandatory to create the relevant documentation prior and post execution.
- Code management: Code management is an essential praxis to maintain the intellectual property of the company under control.

Plexigrid considers that Information Security functions should be integrated into all hierarchical levels of third-party personnel. Since Information Security is the responsibility of all Plexigrid and third party or externals included. This Policy must be known, understood, and assumed by all.

To achieve the objectives of this Policy, all externals and third parties must establish a preventive analysis strategy on the risks that could affect it, identifying them, implementing controls for their mitigation, and establishing periodic procedures for their reassessment. Throughout this cycle of continuous improvement, the definition of both the level of residual risk accepted (risk appetite) and its tolerance thresholds is important to be tracked.

1.6 MANAGEMENT COMMITMENT

Externals and third parties should be committed to:

- Promote in the organization the functions and responsibilities around information security.
- Provide adequate resources to achieve information security objectives.
- Provide interactive learning and masterclasses about security.
- Promote the dissemination and awareness of the Information Security Policy among employees.
- Demand compliance with the Policy, current legislation, and the requirements of regulators regarding information security.
- Consider information security risks in decision making.

1.7 TRAINING AND AWARENESS

Ensure that all staff receive an adequate level of training and awareness in Information Security, especially in terms of confidentiality and prevention of information leaks.

Likewise, externals and third parties must inform their employees of updates to the security policies and procedures in which they are affected and of existing threats, so that compliance with this Policy can be ensured.

On the other hand, externals and third parties have an obligation to exercise diligence with respect to information, ensuring that such information does not fall into the possession of non-unauthorized entities.

1.8 RESPONSIBILITIES

The whole responsibility model can be found in the Plexigrid ISMS policy:
Information Security Management System Policy.docx

1.9 GENERAL

- Externals and third parties are responsible for immediately reporting abnormalities and security incidents that they observe in the systems.
- Modifications to data and information in production systems must be strictly restricted to transactions and processes expressly designed for this purpose.
- All IT equipment (computers, workstations, graphics stations, servers and accessory equipment, mobile devices, tablets, Smartphones), that are connected to the Network must abide by the rules and installation and configuration parameters following best security practices issued by Plexigrid as a minimum.
- Systems will be managed by suitably trained and qualified personnel to oversee their day-to-day operation and to preserve security and integrity in collaboration with the individual system owners, as a minimum:
    - Encryption technologies
    - Cyber security
    - System and software vulnerabilities
    - Access and identity management
    - Cloud security technologies

2 INFORMATION SYSTEMS

- All Information Systems[1], data tools (programs, databases, information systems, interfaces, and others) developed with or through Plexigrid resources will remain the property of the Plexigrid, respecting its intellectual property, including its layouts, fonts, documentation, and other aspects of development.
- All Information Systems done for Plexigrid must be developed and documented in accordance with the standard methodology, based on the project area technical concept sheets.
- For all information systems, security must be considered mandatory from the principles of the life cycle. Likewise, the vulnerability and security tests that the area in charge deems pertinent must be carried out and they will not be put into production until the existing vulnerabilities have been corrected.
- During each phase of the system development, maintenance, and tuning process, security aspects must be explicitly defined, documented by the development team, and established as a specific security requirement.
- In the initial phase of project definition, of a new system, the "owner" of the system must be assigned, in compliance with the basic responsibilities in computer security, as well as stipulate the formats for monitoring and control of changes.
- Plexigrid could require perform a test of vulnerabilities or Ethical Hacking carried out by whoever they consider to third parties, that guarantees system is optimal and secure.
- When tests are carried out, they must be carried out in a test environment before putting the application into production and the parallel use of the new system and the old system must be considered, to detect errors.
- The production process of the applications, systems or their updates must be carried out in such a way that it does not deteriorate the services to the users or the normal operation, therefore, it must be properly coordinated and carried out with pre-established schedules.
- Must ensure that every system has a contingency scheme which must consider aspects of software, hardware, and personnel necessary for the continuity of the service; This must be reviewed by the person responsible for each process in conjunction with Management.
- Every information system must be assigned a system administrator responsible for activities of operation, management, compliance with established security.
- By default, ftp and sftp are not standard ways to work in Plexigrid, avoid always that possible. However, in the case of need, at least a secured sftp will be the minimum-security approach.
- All changes must be documented. Such maintenance windows must be duly documented indicating the date, person in charge, server, and affected application, as well as the reason for the changes made. Following the “change management procedure process”.

3 TRANSFER OF FILES / INFORMATION

1. All information must be labelled properly.

2. The software documentation, or any type of usage information property of Plexigrid, must not be transferred to third parties without prior authorization or a confidentiality agreement with Plexigrid.

[1] Information systems means everything that has to do with IT.

3. All information that is generated, processed, stored and/or transits through the Plexigrid network is considered property of Plexigrid.

4. Only Plexigrid company datastore platform is allowed to store files.

5. If sensitive information is required to be transferred to a third party, the owner of the information must request IT advice on information encryption and use of cryptographic keys; Efforts should be made to transfer information always encrypted.

4 BACKUPS

Externals are responsible of backup the essential data managed by them to support business continuity and to ensure data recovery within a reasonable time.

Backup requirements must be applied in accordance with the established risk assessment. That means properly defining acceptable backup media, methods, and frequency.

Plexigrid can require access to those external backups related to Plexigrid backups at any moment if needed. Or ask for recovery simulations.

5 SECURITY OF THE INFORMATION

5.1 INFORMATION LIFECYCLE MANAGEMENT

Third parties must adequately manage the information life cycle, so that incorrect use can be avoided during any of the phases. The life cycle of an information asset consists of the following phases:

1. **Create or collect:** This phase deals with records at their point of origin.

2. **Distribution:** It is the information management process once it is created or received.

3. **Use or access**: Occurs after information is distributed internally, and may drive business decisions, generate new information, or serve other purposes.

4. **Storage:** it is the process of organizing information in a default sequence and creating a management system to ensure its usefulness.

5. **Destruction**: Establishes practices for the disposal of information that has defined retention periods that have been met and information that is no longer.

Business needs should also be considered. If none of these requirements requires that the information be kept, it must be discarded through means that guarantee its confidentiality during the destruction process.

5.2 ACCESS MANAGEMENT AND RESPONSIBILITIES

- The classification of the data and sensitivity labelling will be done by the creator of the data. The data must be protected against undesired access being stored in the correct folder with the correct permissions and the correct sensitivity labelling.
- RBAC access must be defined to securely store the data and protect undesired access.

5.3 INCIDENT, SUPPORT AND DISASTER RECOVERY ACTIVATION

Third parties should act according to ISO27001 recommendations even if they don't have the ISO certification. This means that third parties must use best practices and have the respective processes to activate and solve a petition from a customer in case of an incident.

6 AUDITS AND COMPLIANCE

Compliance with legal, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software products must be ensured.

The security of personal data must be guaranteed. Computer systems must support the protection of personal data through the implementation of technical controls, this includes:

- Encryption technologies
- Access controls
- Availability mechanisms
- Backups

The handling of personal data must be aligned with the requirements of local regulation, as well as with the specific requirements that may be requested by clients, this may include:

- To delete personal data after a certain storage period
- To make data available for a specific period
- To allow customers to modify their personal data upon request
- To manage specific customer requests regarding their personal data

Compliance with local regulation regarding cryptographic mechanisms must also be ensured by Plexigrid teams, as some countries impose limitations or have specific requests as the CIS directive in Europe for example.

7 SOFTWARE AND LICENSING

Plexigrid will not be responsible of any use of unlicensed software.

8 MISCELLANEOUS

Responsibilities

Externals are responsible for complying with this Policy and any other relevant IT security policies and procedures.

In case of doubt Plexigrid will provide guidance and support to Externals on IT security best practices and procedures.

Data Handling

Externals must handle Plexigrid’s resources with the same level of care and confidentiality as Plexigrid’s employees. Externals must not share, copy, or distribute Plexigrid’s resources without prior written permission from our organization.

System Use

Externals must use Plexigrid’s resources only for authorized purposes.

Externals must not install or use unauthorized software or hardware on Plexigrid's systems.

Termination of Access

In the event of an External’s termination or departure from Plexigrid relationship, any access to Plexigrid's resources must be terminated immediately.

Monitoring and Enforcement

Externals are aware that Plexigrid's IT department will monitor their access and use of Plexigrid’s resources to ensure compliance with this policy.

Non-compliance with this Policy may result in disciplinary action, up to and including termination of the External's contract or agreement as well as a financial penalty to cover the damages caused to Plexigrid

by External non-compliance. The financial penalty amount shall be fixed by Plexigrid, External already accepts the amount to be fixed by Plexigrid of compensation as fair and balanced.

Amendments

This Policy may be amended or updated at any time without notice.

The Externals will be obliged to comply with any changes to this Policy.