Title:	Information Security Policy
Code:	GF_PYCS002
Review No.:	***1***
Applicable to:	Protection and Cybersecurity
Persons responsible for issuing this document:	General Protection and Cybersecurity Coordinator Data Protection Officer
Reviewed by:	Industrial Director - Fertiberia Group
Date:	18 June 2021
Signed:	
Approved by:	CEO - Fertiberia Group
Date:	18 June 2021
Signed:	

Summary of amendments:	Rev.1: Initial document
Initial distribution list:	Management Committee - Fertiberia Group ADP Steering Committee General Departments of Fertiberia Group Companies Fertiberia Group Corporate Departments Fertiberia Group Factory and Workplace Departments General Protection and Cybersecurity Coordinator Fertiberia Group General QHSE Coordinators Fertiberia Group Factory and Workplace Safety Coordinators

Contents

1. Introduction

Information is one of the most important assets for any organisation, and it must therefore be properly protected, regardless of the form that it takes or the ways in which it is forwarded, stored or processed.

Aware of the importance and value of its information, Fertiberia Group has created a regulatory framework for its information security, supported by a continuous improvement process. Its aim is to manage security and ensure the integrity and availability of any information stored, forwarded or processed using its Information Systems, along with the communications for which it is responsible.

The Security Policy that relates to its Information Systems establishes a series of objectives aimed at protecting its information and the systems that guard against potential threats, reducing the damage caused by incidents and ensuring the continuity of its services while maintaining the following basic security criteria:

- Confidentiality: Guaranteeing that only duly authorised people have access to information and systems.
- Integrity: Guaranteeing the accuracy of information and protecting systems against alteration, loss and destruction, whether this occurs accidentally or with wilful intent.
- Availability: Guaranteeing that information and systems can be used within the time and in the manner required.

The parameters described above are essential in order to comply with current legislation in matters of information security and to provide a quality service.

2. Application

This Security Policy affects the Information Systems, and it applies mandatorily to all Fertiberia Group personnel, on the understanding that this includes both Fertiberia and all the organisations in its corporate group. It also applies to any collaborative organisations that make use of the information and the systems that they own and on which it is held.

Fertiberia's Security Policy takes the criteria set out in international standards UNE ISO/IEC 27001:2017, UNE ISO/IEC 27002:2017, ISO/IEC 27017:2015, ISO/IEC 27018:2019 and UNE ISO/IEC 22301:2015 as a reference, to the extent that it adopts the precautions necessary to ensure the level of security required under the terms of the legal framework relating to information security, particularly Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of

network and information systems across the Union, the regulations by which it is transposed and enacted in Spanish, French and Portuguese law, and Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, the General Data Protection Regulation or GDPR), and the regulations by which it is supplemented in Spanish, French and Portuguese Law.

3. Scope

The scope of the Security Policy extends to all Fertiberia Group's Information Systems and to all the personnel who are involved with or make use of them.

4. Undertaking with Management

The Security Committee is aware of the importance that Fertiberia Group places in information security. For this reason, it has drawn up this present Security Policy, and it wishes to express its support and approval for the Policy and to assign the resources necessary for its execution. The Policy is distributed to all personnel so that they may be aware of and comply with it.

5. Information Security Policy

5.1. Risk management and assessment

Fertiberia Group regularly carries out a risk analysis and management process, which serves as a cornerstone for all its security-related actions. This process allows it to ascertain the security situation and assess any risk to which its information assets may be subject.

In order to carry out its risk analysis, Fertiberia Group identifies the threats to which assets are subject and determines the degree to which such threats may arise. On the basis of this risk and the value of the asset in question, it determines the impact or harm that a particular situation may cause in the event that a threat materialises.

Together with this risk analysis, an impact analysis is also carried out, and with the results of both analyses Fertiberia Group plans its management and treatment of the risks identified, selecting the safeguards that are necessary in order to reduce risk to acceptable levels and thus reduce its impact.

5.2. Policies and Requirements for Compliance with Security

5.2.1. Organisational aspects of information security

Fertiberia Group has created an organisational security structure for the purposes of coordinating and approving all aspects relating to Information Security.

This organisational structure comprises the following:

Information Security Committee: The Information Security Committee coordinates and centralises all efforts concerning decisions about security, policy, regulations, risk analysis, continuity of service plans, disaster recovery, etc. Among other duties, it is responsible for approving policy, security objectives, regulations, risk analyses, plans for the continuity of services, etc., all the time ensuring alignment with defined security strategy. At its ordinary meetings, it makes an assessment and review of the situation at Fertiberia Group with regard to information security, and it studies any security proposals that need to be dealt with.

Head of Information Security: Among other duties, this person is responsible for overseeing implementation of the security policy, regulations, guidelines and procedures in place at Fertiberia Group. He/she provides support in security-related matters for all areas of Fertiberia Group, following up the status of security incidents, ensuring compliance with policy, guidelines and security procedures, etc. He/she is responsible for maintaining and ensuring compliance with Regulations governing Duties and Obligations in matters of Information Security and Data Protection, working together with the Data Protection Officer when necessary; in addition, where applicable, he/she is also responsible for ensuring compliance with the Duties and Obligations resulting from the regulations governing the Protection of Critical Infrastructure and the Security of Networks and Information Systems (the PIC and NIS regulations), and more specifically, the duty to represent Fertiberia Group before the INCIBE-CSIRT and CNPIC, bodies that report to the Secretary of State for Security, in coordination with the Head of Security and Liaison appointed by Fertiberia Group for Spain and, whenever required, for the equivalent Administrative Bodies in France and Portugal.

Information Owners These are the people who are responsible for the security of certain information and those who are responsible for classifying information according to its confidentiality, integrity and availability, allocating the relevant security measures and naming the users who are to be allowed access to the information, along with the way it is to be used.

Custodians: These people are responsible for safeguarding the information entrusted to them by the owners and for implementing security measures to protect this information. They must make security copies and implement, operate and maintain the security measures that have been established.

Users who perform duties for Fertiberia (suppliers, subcontractors, work experience personnel, etc.): These people are responsible for complying with the rules set out in the Fertiberia Group Security Policy, and in particular for:

• Being aware of and applying the current guidelines and regulations relating to information security at the Digital Services Supplier, making proper use of the information and the systems in which it is held.
• Not disclosing Fertiberia Group information to unauthorised persons.
• Using the Information Systems owned by Fertiberia Group for the purposes for which they are intended, and not allowing unauthorised persons to use these systems.
• Using passwords and codes that are difficult to guess, keeping them secret and avoiding sharing them or passing them on to other people.
• Immediately reporting any event that might compromise the security of Fertiberia Group's information or the Information Systems in which it is held, and following the procedures put in place by Fertiberia Group.
• Participating in the training activities and plans organised by Fertiberia Group in relation to information security and the protection of personal data.

5.2.2. Security relating to HR

Fertiberia Group has established the technical and organisational measures required to prevent risk resulting from human activity, such as fraud, sabotage, theft, mistakes, etc.

All users, both from outside and inside the Company, are aware of and must comply with the security guidelines established by Fertiberia in order to prevent situations that may cause harm, such as the loss or improper use of information, the deterioration or unavailability of systems, the interruption of the supply of services, etc.

5.2.2.1 Segregation of Duties

Fertiberia Group is aware of the importance of the segregation of duties in activities regarded as critical, and it takes the measures it believes to be advisable in order to prevent a single person from being able to take on all the duties involved in these types of activities.

5.2.2.2 Training and Awareness

Depending on the needs identified, Fertiberia Group organises its training and awareness activities by target area, group or individual.

Personnel who make use of the services provided by Fertiberia Group are responsible for participating in training and awareness activities in relation to both information security and personal

data protection. These activities are provided by the organisations appointed to this end by the people with responsibility in this regard.

5.2.2.3. Acceptable use of Information Systems

Using the means that it deems appropriate, Fertiberia Group provides all of its personnel who use the information systems with the appropriate guidelines for making proper use of both the information and the systems on which it is held, with a view to preventing any risk arising from their improper or inappropriate use.

5.2.3. Asset management

The purpose of the inventory of assets relating to Information Security and the appointment of the persons responsible for each asset is to ensure that these assets are properly managed.

In order to ensure that the information that it owns is properly protected, Fertiberia Group has classified it and arranged for its protection using the security measures established in accordance with its confidentiality, as set out in the Procedure for the Protection and Management of Sensitive Information.

All Fertiberia Group personnel have been familiarised with the classification allocated and the associated security procedures.

If Fertiberia Group assets are held at other premises by a trusted third party, they must be processed using the same security measures as those established at the premises of Fertiberia Group.

5.2.4. Access control

Access to Fertiberia Group's information and systems is granted on a need-to-know basis, and access is only permitted when there is a legitimate need to gain access to the information in question in order for each user to perform his or her duties.

No other kind of access will be permitted, unless explicitly approved by the Fertiberia Group Head of Information Security.

- **Identification**

Fertiberia Group assigns identifiers that allow users to be identified and registered in an unmistakeable and personalised way.

Where possible, all Information Systems are fitted with logical access control mechanisms that confirm the identity of users and guarantee access solely and exclusively to personnel who have the necessary authorisation to access information.

- **Authentication**

Users of the services provided by Fertiberia are under an obligation to choose strong passwords that are difficult to guess, and these passwords must not be saved or kept on media that are legible or easily accessible, nor may they be shared with other users.

The Head of Information Security requests and carries out regular reviews of access to information and the permissions granted to users, in order to check that only authorised personnel are gaining access to information and that the established security guidelines are being observed.

5.2.5. Physical security and security of the environment

5.2.5.1. Secure Areas (Data Centres)

Fertiberia Group has established minimum security specifications for areas classified as critical, including:

- Physical security mechanisms
- Access and exit controls
- Measures to counter external threats
- Isolation of sensitive systems, etc.

In this way, risk resulting from unauthorised access and damage to information resources is reduced.

In order to ensure the continuity and effectiveness of its services, Fertiberia Group has identified the need to carry out corrective and preventive maintenance on its systems and supplies, in a way that ensures their correct configuration and operation, and it has developed the necessary security measures to allow it to continue providing its services in the event of a fault.

Fertiberia Group has prepared a series of security guidelines to be followed by personnel working at its facilities, with a view to preventing various risk situations. Procedures have been put in place for the notification of events that may compromise the security of the Information Systems.

5.2.5.2. Offices

Fertiberia Group analyses the minimum security measures required (guards, locks on doors, cupboards and filing cabinets with keys, etc.) in order to prevent unauthorised access to the information kept at Fertiberia Group offices and other premises.

Fertiberia Group personnel check that all devices are blocked or switched off and that information is stored or properly protected from unauthorised access when these offices and other premises are empty.

5.2.6. Security of operations

5.2.6.1. Management of changes and adjustments

Fertiberia Group has established the procedures and measures necessary to manage any changes or adjustments that may arise, ensuring that such changes and adjustments are approved by the people responsible and implemented in a correct and efficient manner.

The use of new systems or applications is approved by the Fertiberia Group Information Security Committee.

The monitoring process carried out by the Security Committee includes identifying the need for resources and the prioritisation of the various areas for planning purposes.

5.2.6.2. Malicious Code

Malicious code, such as viruses worms, trojans, spyware, etc. are programmes that may be created for purposes such as: compiling sensitive information on users, controlling devices, damaging devices or rendering them unusable, modifying or deleting data, etc.

As a means of protection, all of Fertiberia Group's systems are fitted with updated antivirus software.

To prevent malicious software, users assume responsibility for taking the necessary precautions, such as not downloading, running or opening files that originate from unknown sources, not installing unauthorised software, transferring the antivirus programme to the media that they are going to use, etc. They are also made aware that the antivirus programme does not on its own guarantee security.

If a user suspects infection by a virus, he/she must report this using the procedures established by Fertiberia Group so that the relevant measures can be taken.

5.2.6.3. Management of Media and Security Copies

Fertiberia Group has established a register to record the entry and exit of media, depending on its classification, in a way that ensures that this occurs in an authorised and controlled manner.

It has specific spaces (shared units, network files, etc.) for the storage of information on personnel and users, of which copies are made and on which regular checks are carried out. Any security copies that are made will be stored in external locations as a security measure.

Fertiberia Group has procedures for carrying out checks and recovering data, and the Head of Information Security is charged with overseeing that these are complied with and carried out in accordance with the established rules.

Users are responsible for requesting security copies from the relevant support personnel, bearing in mind that, as a general rule, sensitive information must not be stored on equipment locally.

In order to guarantee the required confidentiality of the information, Fertiberia Group applies encryption mechanisms to its security copies, protecting them using mechanisms that ensure that the information cannot be accessed by unauthorised persons.

5.2.7. Security of communications

Fertiberia Group takes the necessary measures to protect and strengthen its networks and its communications, implementing procedures and security controls on the basis of the critical nature of the information or systems to be protected.

It takes account of segmentation of the network and the use of secure communications protocols, and it has prepared a set of guidelines for the use of email and the Internet, in such a way that its use is limited to matters relating directly to Fertiberia's business activities and the duties inherent in the job being performed by its personnel.

In this way, it guarantees the security of any information transferred both within the organisation and to any external organisation.

5.2.8. Acquisition, development and maintenance of Information Systems

5.2.8.1. Segmentation of environments

Fertiberia Group takes the measures necessary to ensure that its development, testing and production environments remain distinct, in such a way that testing and development is carried out in a secure and controlled way before moving on to the production phase.

In the event that services are subcontracted or outsourced, the developments and material generated while this service is being supplied is regarded as belonging to Fertiberia Group, which assumes all legal rights of ownership.

5.2.9. Relations with Suppliers

Fertiberia Group establishes the mechanisms required to ensure the protection of any of the organisation's assets that may be accessible to suppliers.

5.2.10. Management of security incidents

Fertiberia Group has the means necessary to ensure that all of its personnel are aware of their responsibilities and of the actions to be taken in the event that they identify a security incident.

Following the instructions given by Fertiberia Group, employees immediately report any event that may compromise Fertiberia Group's Information Systems to the person named to this end in the relevant procedure, or to their direct superior, or to the Head of Information Security. Such events may include fire or water damage, a breakdown in supply, theft, unauthorised access to systems or facilities, breakdowns or irregularities in operations, identity theft, attacks, viruses, etc.

Fertiberia Group manages security incidents in a way that, where possible, allows it to analyse and evaluate the causes and consequences of these incidents and take the necessary corrective or preventive action as quickly as possible, and it adheres to the protection plan in place at the building in which it is located.

5.2.10.1. Monitoring and Auditing

The auditing records contain the information necessary to guarantee the tracking of activities that are not permitted and that depart from established procedure.

Fertiberia Group monitors and manages events relating to all of its processes and systems, and this allows it to carry out audits and to review access and use. It is thus able to check compliance with the applicable policies, directives, laws and regulations and to confirm that the security controls and safeguards that it has implemented are operating correctly.

Fertiberia Group carries out reviews and audits both internally and externally in order to verify compliance with its security guidelines and identify any corrective or preventive action or improvements that may be necessary.

All contracts entered into with suppliers and outsourced workers establish the necessity of including *auditability* clauses that allow Fertiberia Group to verify compliance with the established security regulations.

5.2.11. Aspects of information security for the continuous management of the business

Fertiberia Group has a management process to ensure the continuity of its services, based on the results of its Risk Analysis. This means that any eventual breakdown or interruption of the affected services can be reduced to acceptable levels.

The management process for the continuity of its services includes controls designed to identify and reduce risk, limit the consequences of incidents and ensure the timely resumption of essential operations.

For services regarded as critical, Fertiberia Group regularly develops and tests contingency plans which take account of the back-up procedures and resources needed to ensure the effective and efficient recovery of the services affected.

5.2.12. Compliance

Fertiberia Group has drawn up a list of the legal requirements that apply to matters of information security, and it keeps this list updated.

In this way, all the contracts, licences and agreements entered into by Fertiberia Group include compliance with security regulations, clauses relating to intellectual property, exploitation rights, the protection of personal data, confidentiality and non-disclosure and the safety requirements that must be complied with as the result of the legislation and regulations in force.

In compliance with the legal and regulatory requirements in force, Fertiberia Group ensures the confidentiality, integrity and availability of any records that may be required for legal reasons, and it protects them against their potential loss, destruction or modification.

In order to comply with the rues governing personal data protection, pursuant to the European Union's regulatory provisions and their implementation in Spain, France and Portugal, Fertiberia Group has both a Personal Data Protection Policy and a Clear Desk Policy that have been approved

by the various administrative bodies at all the organisations belonging to the Fertiberia Group, as well as by the Data Protection Officer in Spain, France and Portugal. It also has a record of processing activities which is kept by each of these Data Protection Officers and which identifies the files that contain personal data, the person responsible for each file, its location and its allotted protection level. In addition, with regard to the protection of personal data, its Regulations governing Duties and Obligations apply in all matters relating to Information Security and Data Protection.

In order to ensure compliance with all security requirements, the Head of Information Security, working where necessary with the Data Protection Officer, carries out regular technical and compliance reviews, establishing the necessary security measures and issuing the reports required for review at meetings with the Information Security Committee.