FCC Group Standard for Compliance with the Requirements of the General Data Protection Regulation

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	February 2018	IS	Document creation	Executive Security Committee
	October 2019	IS	General Review	Executive Security Committee
2.0	January 2026	IS	Document Review ISO/IEC 27001:2022 ENS	Chief Information Security Officer (CISO)

INDEX

1. Introduction

The present document is part of the Information Security Regulatory Framework of the FCC Group, which develops the mandatory principles applicable within the Group regarding Information Security.

The Information Security Regulatory Framework is periodically reviewed and updated by the Information Security department (hereinafter the IS department), in accordance with the provisions established in the Regulatory Framework Management and Maintenance Document. This document contains information on the version history, reviews, and approvals of this Standard, as well as its relationship with and dependence on the rest of the regulatory documents. This Standard will be reviewed at least annually, unless circumstances arise that recommend or require a review before that date.

On 25 May 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 entered into force, concerning 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, the Regulation or GDPR).

From the FCC Information Security Department — IS department (the department responsible for establishing the minimum guidelines on Privacy), and in order to comply with the European data protection regulations derived from the GDPR, this "**Standard**" has been developed. It must be applied in each of the FCC Group's Entities to adapt them to said regulation, with the collaboration of FCC as the parent company, the Data Protection Coordinators, and the entire structure created for this purpose.

1.1 Purpose

The objective of this Standard is to convey to the FCC Entities (that fall within the scope of application of the Regulation) the main new features introduced by the Regulation, as well as the actions and minimum requirements that must be fulfilled by each FCC Entity.

Nevertheless, the FCC Group may develop procedures that expand upon and detail certain points of this Standard.

1.2 Scope of Application

1.2.1 Geographic Scope

This Standard applies to, and is mandatory for, the Entities that belong to the FCC Group and are located in any State/Country/Region of the European Union, specifically:

- Those Entities in which FCC holds the majority shareholding (more than 50%).
- Those Entities in which, although FCC does not hold the majority shareholding, it nonetheless exercises the management or administration of the Entity.

1.2.2 Material Scope

This Standard shall apply to all information containing Personal Data (in paper and/or electronic format) under the responsibility of each of the FCC Entities, which is collected, accessed, managed, transferred, or otherwise processed by the personnel of the FCC Entities or by their Partners and/or Providers.

2. Development

2.1 Definitions

- **«Personal data»**: any information relating to an identified or identifiable natural person ("the data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity.
- **«Processing»**: any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **«Pseudonymisation»**: the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **«Filing system»**: any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.
- **«Controller»** or **«Data Controller»**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing; where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. In this respect, each FCC Entity shall act as Controller regarding the personal data it manages (e.g., data of Employees, Customers and Suppliers).
- **«Processor»**: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **«Data subject's consent»**: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **«Personal data breach»**: any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **«Data concerning health»**: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
- **«Data Protection Coordinator»**: the person belonging to an Entity of the FCC Group appointed to coordinate data protection actions within an area of the FCC Group.
- **«Data Protection Security Officer of the Entity or Entities»**: the person belonging to an Entity of the FCC Group appointed to manage data protection–related actions for one or several Entities of the FCC Group.

2.2 Relevant Developments Introduced by the Regulation

The Regulation establishes a series of new requirements that must be implemented in the FCC Entities that fall within the scope of application of the GDPR.

For informational purposes, and without prejudice to the effective measures to be implemented as set out in section 6 of this Standard ("Minimum Privacy Guidelines"), some of the GDPR's new features are outlined below:

- **The principle of "Accountability" («Responsabilidad Proactiva»)** is established, under which each FCC Entity is responsible for the correct and timely compliance with the Regulation and must be able to demonstrate such compliance at any moment through the implementation of a solid system of evidence.
- **The principles applicable to the processing of personal data are strengthened**: lawfulness, fairness and transparency; collected for specified, explicit and legitimate purposes («purpose limitation»); adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed («data minimisation»); accurate and kept up to date («accuracy»); kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed («storage limitation»); processed in a manner that ensures appropriate security of the personal data («integrity and confidentiality»).
- **The requirement for consent is reinforced**. One of the fundamental bases for processing personal data is consent. The Regulation requires that consent, in general, be free, informed, specific and unambiguous. To consider consent "unambiguous", the Regulation requires a statement by the data subjects or a clear affirmative action indicating their agreement. Consent cannot be inferred from silence or inactivity, and there must be evidentiary proof of such consent.
- **The right to information is strengthened**, obliging the Entity to provide more extensive information prior to the collection or recording of personal data of employees, customers and suppliers by any means.
- **New rights are introduced in favour of the data subject**, including notably the right to data portability, which allows data subjects to request from the Entity the delivery or recovery of their data in a format that allows their transfer to another controller.
- **The need to comply with data protection by design is established**, requiring data protection compliance from the beginning of the service or since the acquisition of the system. Techniques such as pseudonymisation («seudonimización») will be promoted (understood as the processing of personal data in such a way that they can no longer be attributed to the data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person).
- **The obligation to notify the Data Protection Authority within a minimum timeframe**, and to notify the data subject in certain cases, is introduced for those security breaches affecting data that may involve risks of harm to natural persons. All security breaches must be documented.
- **The need to establish technical security measures based on risk is imposed**, allowing the guarantee of an adequate level of security, as well as the obligation to carry out data protection impact assessments (hereinafter, PIAs), whenever processing operations—particularly when new technologies are used—are likely to result in a high risk to the rights and freedoms of natural persons, or in the processing types indicated by the Supervisory Authority.

- **The concept of the "right to be forgotten"** is introduced, allowing individuals to request that their personal data be erased under certain circumstances.

2.3 Data Protection Guidelines

Below are the minimum guidelines that must be observed and complied with by each FCC Entity, without prejudice to the fulfilment of the requirements demanded by any other applicable Data Protection regulations (as required by the mandatory law of the country in which the FCC Entity is domiciled or located).

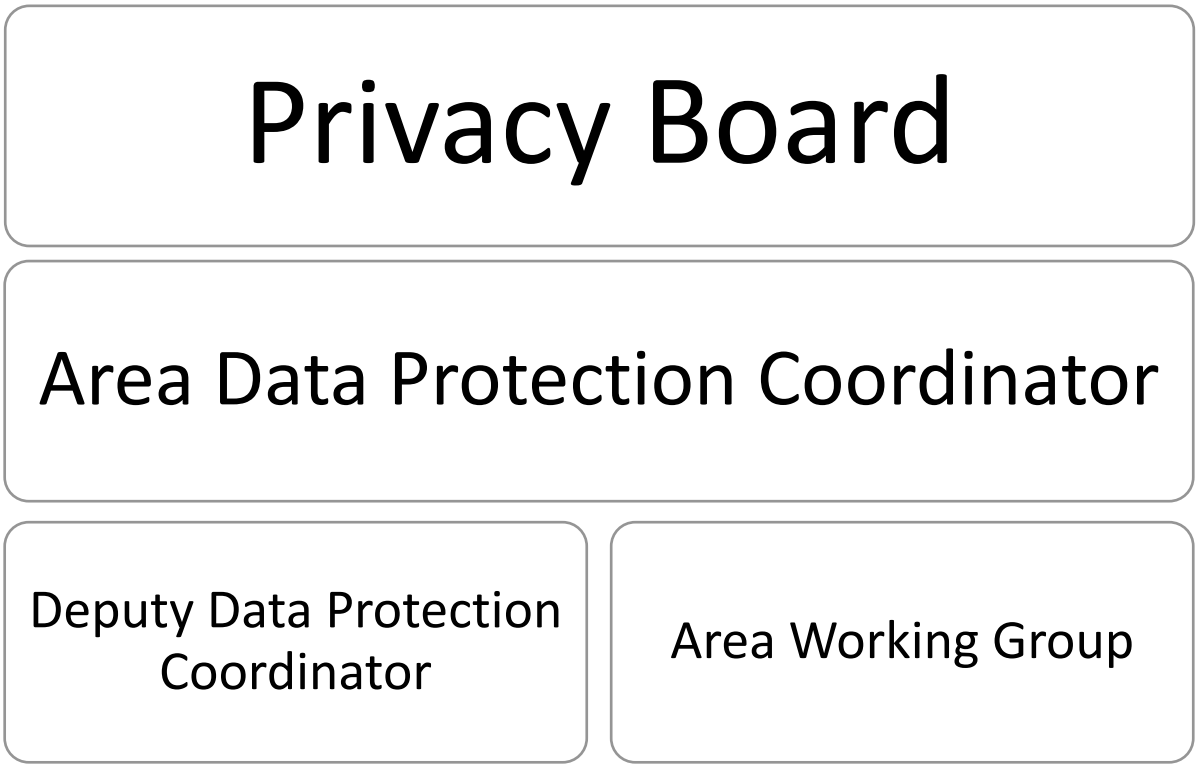
2.3.1 Privacy Structure within FCC

To ensure compliance with all regulations derived from the Regulation, the FCC Group has created an organisational structure that decides, coordinates, implements and supervises data protection matters throughout the Group.

This structure must be composed, at a minimum, of the following:

- **Privacy Board:** A multidisciplinary, top-level body within the FCC Group in the field of Privacy. It is composed of: the Director of the Legal Advisory Department, the Director of Human Resources, the Director of the Internal Audit, Risk Management and Compliance Department of FCC, the Director of the Information Systems and Technology Division, and the FCC Group Data Protection Coordinator.
- **Area Data Protection Coordinator:** A person belonging to an area of the FCC Group and appointed by such area to promote, implement, coordinate and manage, within the FCC Entities belonging to it, the actions required to comply with Privacy obligations. This role may operate at national and/or international level. Likewise, an Area Data Protection Coordinator may be appointed for a specific country or countries, reporting in all cases to the Area Data Protection Coordinator. For the purposes of this document, the following are considered Areas: FCC Corporación, FCC Construcción, FCC Servicios Medioambientales, FCC Servicios Aguas, and Grupo Cementos Portland Valderrivas.
- **Deputy Data Protection Coordinator:** To support the Area Data Protection Coordinator, Deputy Coordinators may be formally appointed as deemed necessary within each area of activity.
- **Working Group**: Unless an exception is duly justified to the Privacy Board, each area must also establish a Working Group composed of the heads of the Group's Departments (local managers of each Entity, Delegation or region) with the greatest impact on Privacy matters, together with the Area Data Protection Coordinator (and any appointed Deputies and/or Country Coordinators). This Working Group is established for the purpose of promoting, coordinating, implementing, managing and discussing issues relating to data protection that arise within the area of activity, and verifying correct compliance with the Regulation and with any applicable local Data Protection regulations in the FCC Entities that fall within its scope of action.

The organisational Privacy structure for each of the areas shall be, where applicable, as follows:



To understand the functions and responsibilities of each role, refer to the document “Privacy Governance Model”.

2.3.2 General Principles of Action

Below are the general Privacy principles that must be observed and complied with for the processing of personal data:

- Processed lawfully, fairly and transparently in relation to the data subject (**«lawfulness, fairness and transparency»**).
- Collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes; further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered incompatible with the initial purposes (**«purpose limitation»**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**«data minimisation»**).
- Accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**«accuracy»**).
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as they are processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, without prejudice to the implementation of the appropriate technical and organisational measures required by the Regulation to safeguard the rights and freedoms of the data subject (**«storage limitation»**).
- Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures (**«integrity and confidentiality»**).
- Where processing is based on the data subject's consent, the FCC Entity must be able to demonstrate that the data subject has consented to the processing of his or her personal data. If the data subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent shall be presented in a manner clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

2.3.3 Organisational Aspects

At an organisational level, at a minimum, the following actions must be carried out:

2.3.3.1 Establishment and Appointment of the Privacy Governance Model in each area

Within each area of activity, a Privacy Governance Model must be designed and formally appointed, which must include at least one Data Protection Coordinator for the area of activity (national and/or international). Additionally, within each area, any Deputy and/or Country Coordinators deemed necessary may also be appointed.

In all cases, there must be a formal appointment, and the functions and responsibilities assumed by each appointed role must be clearly defined.

Any appointments made, as well as any changes made to the Governance Model (whether changes in responsibilities, appointments, etc.), must be reported to the Area Data Protection Coordinator and to the IS department.

2.3.3.2 Control and updated inventory of FCC entities in each area

Each Area Data Protection Coordinator must keep control of the FCC Entities existing in their area at all times (and to which this Standard applies), so that the data protection guidelines are applied to them, and with a view to potential inspections or audits.

To this end, the data protection management tool of each area must be kept up to date, incorporating any new FCC Entities that are created or acquired, and removing those entities that have disappeared or are no longer under FCC control.

2.3.3.3 Obligation to evidence proper compliance with the regulation

Based on the principles of Accountability and with a view to possible inspections or audits, all aspects concerning the processing of personal data, compliance with the applicable regulations, as well as any corrective measures applied, must be evidenced.

That is, all actions, policies, measures and even the meetings held (through minutes) for the management and implementation of this Standard, as well as other actions related to data protection to which the FCC Group is obliged under the applicable regulations, must be evidenced and safeguarded by each of the FCC Entities.

2.3.4 Legal aspects

Regarding legal aspects, at a minimum, the following actions must be conducted:

2.3.4.1 Records of processing activities

In each FCC Entity, all points at which processing of personal data is carried out must be identified and inventoried in order to ensure their alignment with the GDPR.

This processing inventory shall also serve as the basis for creating the Record of Processing Activities required by the Regulation under Article 30.

This Record must contain, at a minimum, the information set out in Article 30 of the GDPR.

It shall be the responsibility of each Area Data Protection Coordinator to ensure the proper management and diligent, up-to-date maintenance of the Records of Processing Activities of personal data.

2.3.4.2 Contractual clauses

The clauses and/or contracts relating to Data Protection used in each FCC Entity (clauses/contracts for Employees, Customers and Suppliers) must be reviewed and updated in accordance with the requirements established by the GDPR.

To this end, the clause/contract templates provided by the IS department shall always be used as the basis. These templates must be reviewed in accordance with the requirements established by the applicable Data Protection regulations.

In particular:

EMPLOYEES

All FCC Entities must regularise, in accordance with the GDPR (and any requirements that may be established by the applicable Data Protection regulations), the information and consent clauses relating to Data Protection for all current employees.

Likewise, with respect to future employees, FCC Entities must have them sign an information and consent clause in accordance with the requirements of the GDPR (and any requirements that may be established by the applicable Data Protection regulations).

CUSTOMERS

All FCC Entities must regularise, in accordance with the GDPR (and any requirements that may be established by the applicable Data Protection regulations), the information and consent clauses relating to Data Protection for all current customers.

Likewise, with respect to future customers, FCC Entities must have them sign an information and consent clause in accordance with the requirements of the GDPR (and any requirements that may be established by the applicable Data Protection regulations).

SUPPLIERS

In the event that it is necessary to contract an application and/or Services from an external Entity or any other Entity of the FCC Group (hereinafter, “Supplier”), whereby the Supplier may/must access or process Personal Data, the FCC Entity must select a Supplier that offers sufficient guarantees to implement appropriate technical and organisational measures, so that the processing complies with the requirements of the Regulation. Before accessing/managing any data, a Service Provision Contract must be signed, expressly establishing the minimum content required under Article 28 of the GDPR (and any requirements that may be established by the applicable Data Protection regulations).

For the drafting of the Service Provision Contract, each FCC Entity must use as a basis the Service Provision Contract model provided by the Area Data Protection Coordinator to which the FCC Entity belongs.

Any Service Provision Contract signed with a Processor must be immediately communicated to the Area Data Protection Coordinator to which the FCC Entity belongs and correctly filed by the area.

Likewise, all “Request For Proposal” (RFP) documents and/or requests for quotation must include a Data Protection clause in accordance with the GDPR requirements. The template for this clause will be provided by the Area Data Protection Coordinator.

Regarding the existing contracts with Suppliers whose end date is before May 2018, the following applies: In principle, there is no obligation under the Regulation, as these contracts should already include a Data Protection clause that complies with the legislation in force at that time. Nevertheless, any such contracts for which an extension of their term is foreseen must be regularised in accordance with the Regulation.

Regarding contracts with Suppliers whose end date is after May 2018: The signing of the Data Protection clause must be managed, which shall at minimum comply with the requirements set out in Article 28 of the GDPR (and any requirements that may be established by the applicable Data Protection regulations). The Data Protection Clause model provided by the Area Data Protection Coordinator to which the FCC Entity belongs must be used as the basis.

2.3.4.3 Compliance with country-specific data protection laws

Each FCC Entity must also comply, in addition to the requirements established by the GDPR, with any other provisions of any Data Protection regulations that apply by mandatory law in the country in which that Entity is domiciled/located.

2.3.5 Technical aspects

2.3.5.1 Inventory of information systems

In each FCC Entity, all information systems (internal and external) through which personal data are processed/managed must be identified and inventoried, in order to ensure their alignment and their security measures with the requirements of the Regulation.

2.3.5.2 Risk analysis and privacy impact assessment

Taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the FCC Entity shall implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, which may include, among others:

- The pseudonymisation and encryption of personal data (in some cases).
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The information system must also ensure data portability, meaning that it must meet the technical requirements needed to respond to the exercise of the right to data portability, whereby the data subject shall have the right to receive the personal data concerning him or her, provided to FCC, in a structured, commonly used and machine-readable format, and to transmit them to another controller.
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

In this regard, all information systems used within the FCC Group must undergo a risk analysis that allows the identification of the security measures necessary in accordance with the above.

Likewise, as established in Article 35 of the Regulation, whenever an FCC Entity intends to carry out a processing of personal data that, by its nature, scope, context or purposes, is likely to result in a high risk to the rights and freedoms of natural persons, a Privacy Impact Assessment (PIA) must be carried out, prior to the processing, on the impact of such processing on the protection of personal data.

In any case, a PIA must always be carried out when the processing of personal data involves: a systematic and comprehensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling; large-scale processing of the special categories of data referred to in Article 9 of the GDPR; or large-scale systematic monitoring of a publicly accessible area.

Both the risk analyses and the Privacy Impact Assessments (PIAs) carried out within the FCC Group shall be conducted in accordance with the Risk Assessment Methodology that will be approved by the Privacy Board.

2.3.5.3 Audits to verify compliance

FCC Entities must carry out periodic audits (internal or external) in order to verify the proper compliance with this Standard, with the established guidelines and with the security measures implemented.

Prior to their execution, the IS department shall provide the corresponding instructions for their performance to the FCC Entity, and the FCC Entity must report the results to the IS department.

2.3.5.4 Notification of personal data security breaches

The FCC Entity shall immediately notify in writing —and without prejudice to any notifications that may be required to the corresponding Supervisory Authority— the FCC Information Security Director (sdseguridad@fcc.es) of the existence of any “Security Breach”, understood as any breach of security that results in the accidental or unlawful destruction, loss or alteration, the loss and alteration, the unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, including the information required by the GDPR and any other applicable regulations.

2.3.5.5 Prior consultation with area data protection coordinators

Whenever any FCC Entity is to initiate a new project, contract a new application, or carry out any activity (whether commercial, marketing-related, advertising, or of any kind) that may involve the processing of personal data, the Data Protection Coordinators of the corresponding area must be consulted beforehand regarding the impact of such activity or project on data protection.

2.4 Implementation

This Standard must be fully complied with as of 25 May 2018, the date on which the content of the General Data Protection Regulation becomes applicable. However, the implementation of measures must begin sufficiently in advance to ensure compliance with all the provisions of the GDPR when it becomes applicable.

3. Responsibilities

As established in the FCC Code of Ethics, all employees are responsible for knowing and complying with laws and internal regulations. In any case, the FCC Group will provide them with the necessary means to ensure they are aware of and understand their obligations.

Likewise, each FCC Entity (regardless of its legal form) is responsible for complying with the obligations and requirements set forth by the European Data Protection Regulation, by the applicable local Data Protection regulations, and with the decisions and instructions issued by the IT department on this matter. This responsibility will extend beyond the effective date of the GDPR.

In general, each FCC Entity is responsible, at a minimum, for:

- The proper adaptation to and timely compliance with the obligations established by the Regulation and the applicable local Data Protection regulations, as well as those derived from these Rules.
- Establishing a solid system of evidence that allows it to subsequently demonstrate correct compliance.
- Communicating to the Data Protection Coordinator of the area any corporate change that may have an impact on Privacy management. This communication must be made prior to its actual execution.
- Bearing the financial penalties imposed by the Supervisory Authority in the event of non-compliance with the requirements of the Regulation and the applicable local Data Protection regulations.

The legislator has significantly increased the amount of financial penalties. In the event of non-compliance or defective compliance, the imposition of administrative fines is foreseen, which may reach up to €20,000,000 or 4% of the total global annual turnover of the previous financial year (whichever is higher), in the case of very serious infringements, in addition to the corresponding reputational damage.

4. Normative reference

This document has been reviewed by the IT department, and its wording takes the following regulations as a reference:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- Set of FCC Group Information Security guidelines, from a legal, technical, and organizational perspective.
- International standard ISO 27001:2022 and ENS.

4.1 Regulatory controls ISO27001:2022 and ENS

ID Control ISO	ISO/IEC 27001:2022 control	ENS Correspondence
5.1	Information security policies	[org.1] Security Policy; [org.2] Security Standard
5.2	Roles and responsibilities in information security	[org.4] Authorization Process
5.24	Planning and preparation for information security incident management	[op.exp.7] Incident Management
5.25	Assessment and decision-making regarding information security events	[op.exp.7] Incident Management
5.26	Response to information security incidents	[op.exp.9] Incident Management Log
5.28	Evidence collection	[op.exp.7] Incident Management; [op.exp.9] Incident Management Log
5.31	Identification of legal, regulatory and contractual requirements	[op.leg.1] Identification of legal requirements
5.34	Privacy and protection of personal data	[op.pdp.1] Personal data protection
5.36	Compliance with information security policies, rules and standards	[org.4] Authorization Process; [op.exp.3] Configuration Management; [op.exp.4] Security Maintenance and Updates
5.37	Documentation of operational procedures	[org.3] Security Procedures
6.3	Awareness, education and training	[mp.per.3] Awareness; [mp.per.4] Training

6.8	Reporting of information security events	[op.exp.7] Incident Management
8.10	Information disposal	[mp.si.5] Erasure and destruction
8.11	Data masking	[mp.info.1] Personal data
8.12	Data leakage prevention	[mp.com.1] Secure perimeter; [mp.com.2] Confidentiality protection; [mp.si.2] Cryptography; [mp.eq.3] Portable device protection
8.24	Use of cryptography	[op.exp.10] Cryptographic key protection; [mp.si.2] Cryptography; [mp.info.3] Electronic signature