

# FPS Information Security Policy

FINAL, V20230707

Date: 07-07-2023

Status: APPROVED v0.2

## Document contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
1.1	PURPOSE OF INFORMATION PROTECTION AND CYBER SECURITY .....	3
1.2	SCOPE .....	3
1.3	STAKEHOLDERS.....	4
1.4	PRINCIPLES.....	5
<b>2</b>	<b>INFORMATION SECURITY STRATEGY .....</b>	<b>7</b>
2.1	GOALS.....	7
2.2	SECURITY STRATEGY .....	7
<b>3</b>	<b>INFORMATION SECURITY ROLES AND RESPONSIBILITIES .....</b>	<b>10</b>
3.1	OVERALL RESPONSIBILITY FOR INFORMATION SECURITY .....	10
3.2	FIRST LINE OF DEFENSE INFORMATION SECURITY .....	10
3.3	SECOND LINE OF DEFENSE INFORMATION SECURITY.....	11
3.4	THIRD LINE OF DEFENSE INFORMATION SECURITY .....	11
<b>4</b>	<b>INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS).....</b>	<b>12</b>
	<b>APPENDIX A – DEFINITIONS INFORMATION SECURITY.....</b>	<b>13</b>

## 1 Introduction

### 1.1 Purpose of information protection and cyber security

It is a priority for FPS to conduct its business in an ethical and legally compliant way. Information Protection and Cyber Security (hereafter: Information Security), including but not limited to Personal Data, is an integrated part of FPS's ethical business conduct.

The use of computer systems and the storage and exchange of personal (health) information have increased rapidly. This growing dependence comes at a time when the number of threats and actual attacks on these computer systems is constantly increasing. FPS's ambition is to be best in class in online and offline environments. In order to achieve this goal FPS needs a resilient organization, with the confidence to take risks, identify and embrace new technologies and realize new opportunities. Information Security is a significant driver of the success of digital products, services, and business models. Information Security goes beyond the boundaries of the IT department.

*We define Information Security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.*

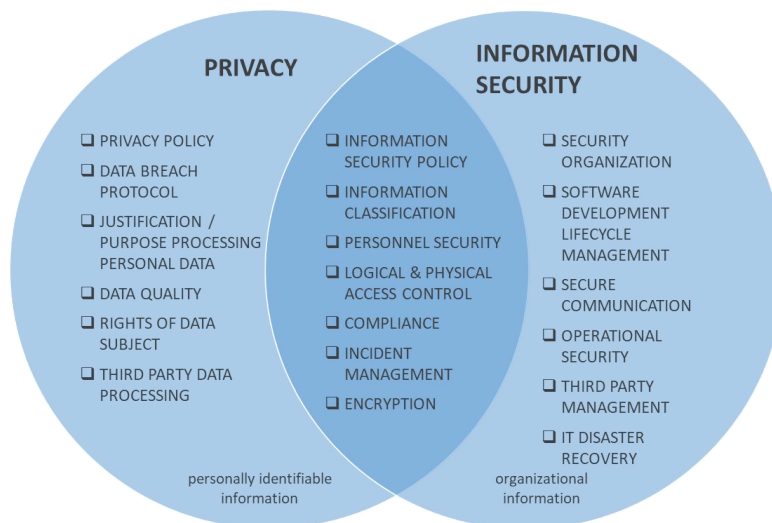
Information is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected information is essential to the successful operation of FPS and its Operating Companies (hereafter: OpCos) in the provision of services to our customers.

*Our protection philosophy is comprised of three tenets:*

- 1. Security and data protection is everyone's responsibility. Maintaining an effective and efficient security posture for FPS require a proactive stance on security risks from everyone. Security is not "somebody else's problem";*
- 2. Security and data protection is part of the whole organization. Security is not just focused on physical security or IT. Rather, FPS seeks to ensure reasonable and appropriate levels of security awareness and protection throughout our organization and infrastructure. There is no place in our business where security is not a consideration.*
- 3. Security and data protection is a business enabler. A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace and must be treated as a valued commodity.*

### 1.2 Scope

The purpose of this Information Security Policy (hereafter: ISP) and its supporting policies is to protect the continuity and value of the organization. The ISP applies to FPS, all dependent and associated OpCos, their employees, franchisees or a Third Party that works with or on behalf of FPS. This ISP applies to both the processing of Information by electronic means and in systematically accessible paper- based filing systems. The policy statements and requirements in this ISP and related policies are aligned with the FPS Minimum Control Standards (MCS).



The figure above best illustrates the scope of this ISP and the relation with Privacy. The ISP and underlying policies cover all fields in the circle Information Security. An overlap exists between Information Security and Privacy which is also covered in the ISP. The remaining elements in the circle Privacy are covered in the FPS Personal Data Protection Policy. Periodic coordination between the data privacy officers and the information security officers is important to properly manage the cohesion between the two areas.

This ISP is based on (inter)national laws and/or standards on data protection and IT security:

- ISO/IEC 27001 – International standard for information security
- General Data Protection Regulation (e.g. GDPR/HIPAA/HDS)
- International IT Governance standards like COBIT/ITIL/NIST

Where applicable local law provides more protection than the rules stipulated in this ISP, local law shall apply. When the rules in this ISP provide more or additional protection than local applicable law, the rules in this ISP will apply.

*All FPS OpCos are required to implement this ISP and the underlying policies. The CFO of the OpCos (or the employee with that specific role) acts as the local Data Protection Officer for the purpose of implementing and enforcing the ISP. All OpCos must use a ‘comply or explain’ approach. OpCos are not entitled to deviate from this ISP without a documented explanation of the deviation.*

This policy (or an equivalent document e.g. a flyer) is made available to all employees, contractors and franchisers.

*This ISP is effective as per December 31, 2021.*

### 1.3 Stakeholders

FPS’s most relevant stakeholders are customers, employees, business partners, investors, and regulatory authorities. These stakeholders pose requirements on:

- Confidentiality: protecting the information from being exposed to an unauthorized party, individuals, systems or processes.
- Integrity (of information): ensuring the accuracy and completeness of information assets.
- Availability: making sure that information (and systems) is always available and usable to authorized users when required.

The requirements of these stakeholders on information security are relevant to the information security management system. We have documented their requirements towards information security.

Stakeholder	What they expect from us
<b>Customers</b>	Internal and external protection of personal (health) data. Timely response regarding requests by data holders to fulfil their rights regarding GDPR. Namely, the right to access, to be informed, to rectification, to erasure, to restrict processing, to data portability, the right to object and rights in relation to automated decision making and profiling.
<b>Employees</b>	Internal and external protection of personal data. FPS expects from employees knowledge and obedience of the ISP and other relevant policies to create and maintain a culture of responsible and safe handling of personal, customer, and employee data.
<b>Business partners</b>	Internal and external protection of information. FPS expects from business partners and franchisees knowledge and compliance to the ISP and other relevant policies.
<b>Investors</b>	To comply with global and local law and regulations. A strong security foundation, proactively enabled and maintained, is important for safeguarding the value of FPS.
<b>Regulatory Authorities</b>	To comply with global and local laws, as well global regulations (e.g. ISO27001 and GDPR) and to conduct ourselves in accordance with the spirit of the law. Timely reporting of 'data-breaches' to regulatory authorities. For the processing of health information OpCos also must comply with local health laws and regulations.

## 1.4 Principles

The following principles apply to this policy:

- This ISP is reviewed and approved by the Audit Committee of the Supervisory Board of FPS.
- Management of FPS HQ and management of each OpCos shall ensure that the ISP, as well as underlying policies are implemented and complied with ('comply or explain').
- The Management must ensure the availability of sufficient training and information material for all employees, in order to enable the users to protect FPS's data and information systems.
- This ISP shall be reviewed and updated annually or when necessary by IT System & Support Specialists (ITSSS), in accordance with principles described in relevant laws and regulations.
- All important changes to FPS's activities, and other relevant external changes which may increase risk, will result in a review and if necessary, a revision of this policy and communicated to the organization by the ITSSS.
- This policy is mandatory and by accessing or using any information or Information Technology (IT) resources which are owned or franchised by FPS or any OpCos, or by being on any of the

---

premises occupied by FPS or any OpCos, all parties which include employees, third parties, users and the likes are agreeing to abide by the terms of this policy.

## 2 Information Security Strategy

### 2.1 Goals

FPS is committed to safeguard the confidentiality, integrity and availability of all physical and electronic information assets of the company to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security at FPS are the following:

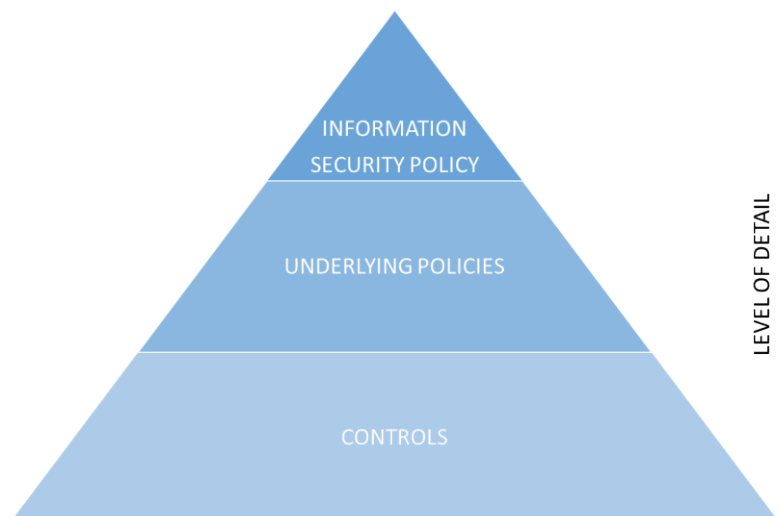
- Ensure that FPS can continue their services even if major security incidents occur.
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by FPS.
- Ensure the protection of personal data (privacy).
- Establish controls for protecting FPS's information and information systems against unauthorized access, theft, abuse and other forms of harm and loss.
- Comply with requirements for confidentiality, integrity and availability for FPS's employees and other users.
- Motivate administrators, employees and third parties to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure flexibility and an necessary level of security for accessing information systems from outside the company.
- Ensure compliance with current global and local laws, regulations and guidelines.
- Comply with methods from international standards for information security, e.g. ISO/IEC27001.
- Ensure that external service providers comply with FPS's information security requirements.

### 2.2 Security Strategy

FPS's business- and IT Strategies are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the ISP (this document).

Information security is ensured by the policy for information security and a set of underlying and supplemental policies.

#### FPS Information Security Framework



The structure of the policies is hierarchical, as shown in the figure above. The ISP (this document) is the top-level document, which is specified in underlying policies (Level 2) provided by FPS HQ. See table below for the set of underlying policies that are related to the ISP. On level 3 (Controls) FPS HQ provides minimum baselines. It is the responsibility of OpCos to implement these policies and baselines, as well as implement other OpCo specific controls (standards, procedures, measures etc.) for risks that are not covered by the central policies and baselines.

Title	Description	Owner
<b>Information Security Policy</b>	<b>This document</b>	<b>Global IT and Turkey Performance Director</b>
<b>ISMS Policy</b>	Provides guidelines for implementing and maintaining a local information security management system (ISMS) as required in this information security policy.	Global IT and Turkey Performance Director
<b>Information Classification Policy</b>	Provides guidelines for classification of information within FPS. Contains also guidelines for encryption and the secure exchange of data.	Global IT and Turkey Performance Director
<b>Cloud Policy (including 3<sup>rd</sup> party suppliers)</b>	Describes rules and principles on how we manage cloud services including 3 <sup>rd</sup> party supplier relationships.	Global IT and Turkey Performance Director
<b>IT End-User Policy (incl Social Media and Mobile Device policy)</b>	Describes a set of information security principles for all employees, franchisees and 3 <sup>rd</sup> parties and the secure usage of mobile devices / laptops and teleworking.	Global IT and Turkey Performance Director
<b>Access Control Policy</b>	Defines rules and principles upon which access rights and restrictions are configured both logical and physical. Contains also password requirements	Global IT and Turkey Performance Director
<b>Secure Development Policy</b>	Defines rules and principles applied in development and engineering of all applications.	Global IT and Turkey Performance Director
<b>Change Management Policy</b>	Defines guidelines in which changes to IT systems should be managed prior to be put in production.	Global IT and Turkey Performance Director
<b>Back-up and Disaster Recovery Policy</b>	Defines rules and principles on how backups should be configured and can be restored in case of an incident / disaster.	Global IT and Turkey Performance Director
<b>Business Resilience Policy</b>	Business resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack.	Global IT and Turkey Performance Director

Next, the following table contains existing FPS policies related to this ISP.

Title	Description	Owner
<b>Related FPS Policies</b>	<b>Existing policies related to the Information Security Policy</b>	





<b>FPS Personal Data Protection Policy</b>	The FPS Personal Data Protection Policy (PDPP) describes why data protection is needed, what the protection and processing of Personal Data entails and under what conditions Personal Data may be processed.	DPO
<b>FPS Data Breach Protocol</b>	Protocol handling every security incident in which the security of Personal Data has been breached and through which the Personal Data has been lost or exposed to unlawful processing by an outside and unauthorized party.	DPO

Title	Description	Owner
<b>FPS Data Retention Policy</b>	The policy of FPS with respect to the retention and destruction of its corporate records and data.	DPO
<b>Risk management Process</b>	The FPS approach on identification and adequate management of strategic, market, IT and business risks.	Internal Audit
<b>Minimum Control Standards</b>	A set of minimum internal control standards that all business units must comply with.	Internal Audit

### 3 Information Security Roles and Responsibilities

#### 3.1 Overall responsibility for Information Security

The Management Board has the overall responsibility for managing FPS's values in an effective and satisfactory manner according to current laws, requirements and contracts. All policy changes must be approved and signed by the Audit committee of the Supervisory Board.

The Global IT and Turkey Performance Director has the overall executive responsibility for information security at FPS. The Global IT and Turkey Performance Director is the owner of the ISP (this document). The Global IT and Turkey Performance Director delegates the responsibility for security-related documentation to the FPS Group IT System & Support Specialists (Group ITSSS).

The Global IT and Turkey Performance Director of the OpCos has the overall executive responsibility for information security at the OpCos. The Global IT and Turkey Performance Director may delegate this responsibility to an Information Security officer and/or Security Manager within the OpCos.

FPS has implemented a 3 lines of defense approach to risk management. The implementation of information security will be part of this existing framework. The information security roles and responsibilities are defined on different layers in this model (see figure below) and explained in the remaining of this chapter.



#### 3.2 Managing Information Security

Management teams in the OpCos, both business and IT are responsible for implementing the ISP, identifying underlying risks, and ensuring effective controls by using the 'comply or explain' approach. They form the first line of defense as the risk owners.

The Information Security Officer is responsible for ensuring that the security processes at the OpCos are coordinated in accordance with this ISP. The ITSSS is the linking pin between both business and IT and the Group ITSSS.

The Security Manager is responsible for the operational aspects of protecting OpCos assets against threats, such as security breaches, computer viruses or attacks by cyber-criminals (preventive) and the operational handling of security incidents (resilience).

The Data Protection Officer (here after: DPO) supervises the application of the Data Protection Policy within an OpCos.

All applications and all types of information must have a defined application owner from the Business. The application owner is responsible for setting functional requirements and maintenance of the application. The application owner is responsible for data classification and must define which users or user groups are allowed access to the information in the application. The application owner must ensure that all 3<sup>rd</sup> parties interacting with the application know and abide by the current ISP. The application owner also oversees that contractual partners and contracted consultants have signed a confidentiality agreement prior to accessing sensitive information. See Information Classification and Access Control policies for further details.

All systems have a system administrator (IT). The system administrator is responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is not lost. They will further implement, run and maintain the security systems in accordance with the information security policy.

The abovementioned regarding the first line of defense applies to FPS as well. The Global IT and Turkey Performance Director has the overall executive responsibility for information security at the FPS.

### 3.3 Controlling Information Security

The Group ITSSS is responsible for ensuring that information security processes at FPS and OpCos are coordinated in accordance with this ISP.

For that purpose, FPS has established a forum for information security coordinated by the Group ITSSS and consisting of OpCos ITSSS'. The security forum will advise the Global IT and Turkey Performance Director about measures increasing the security level of the organization. The security forum has the following responsibilities, among others:

- Review and recommend on information security policy and accompanying documentation and general distribution of responsibility.
- Monitor substantial changes of threats against the information assets of the organization.
- In conjunction with compliance, assess the impact of regulatory change (e.g. regarding GDPR, employment or Health) insofar as any change has an effect on information security and any provision of this policy.
- Review and monitor reported security incidents.
- Identify remediation for known or suspected infringements of this Policy, including security incidents and oversee the implementation of actions required to mitigate further risk.
- Authorize initiatives to strengthen information security.
- Follow up implementation and monitor effective operation of the ISP.

The Data Protection Officer supervises the application of the Personal Data Protection Policy within FPS. Periodic coordination between the DPO and the ITSSS, both on Group and OpCos level, is important to properly manage the cohesion between privacy and information security.

### 3.4 Auditing of Information Security

The Internal Audit function of FPS provides independent assurance regarding Information Security.

## 4 Information Security Management System (ISMS)

The FPS Information Security Management System (hereafter: ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by the organization, in the pursuit of protecting its information assets. The FPS ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization's information security posture to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analyzing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of the ISMS.

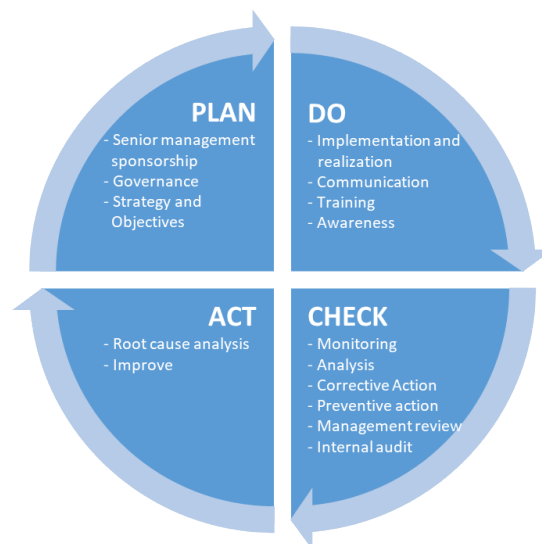
Our ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and is integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls.

ISO 27001 is the international standard that describes how to implement an Information Security Management System. All FPS OpCos are required to implement a local ISMS in line with ISO 27001.

To implement an ISMS the following steps are necessary:

- a) identify information assets and their associated information security requirements (Plan);
- b) assess and treat information security risks and select and implement relevant controls to manage unacceptable risks (Do);
- c) monitor, maintain and improve the effectiveness of controls associated with the organization's information assets (Check and Act).



To ensure the ISMS is effectively protecting the organization's information assets on an ongoing basis, it is necessary for steps (a) to (c) to be continually repeated to identify changes in risks or in the organization's strategies or business objectives. See ISMS policy for more details on how to implement an ISMS.

## Appendix A – Definitions Information Security


Below please find the definitions of several terms used in this Information Security Policy.

Term	Definition
Application owner	The person or persons who are responsible for setting functional requirements for development and maintenance of the information (system), data classification and must define which users or user groups are allowed access to the information (including contractual partners and contracted consultants).
Control	Appropriate technical and/or organisational measure (e.g. standard, procedure, baseline) to mitigate a risk.
Corporate Policies	A documented set of broad guidelines formulated or approved, directly or indirectly by FPS's Supervisory and Management Board. Corporate policies lay down FPS's response to known and knowable situations and circumstances. They also determine the formulation and implementation of strategy, and direct and restrict the plans, decisions, and actions of FPS's officers and employees in achievement of FPS's objectives.
Data Protection Officer or DPO	The Data Protection Officer supervises the application of the Data Protection Policy within a company. The Data Protection Officer for FPS is the FPS CFO. The Data Protection Officer for the Operating Company is the local CFO (or another "named" employee for that role).
FPS	FPS , a company existing under the law of The Netherlands, with its principal place of business at WTC Schiphol Airport, Tower G5, Schiphol Boulevard 11, 1118 BG Schiphol, The Netherlands, and all subsidiaries.
Information	Means confidential information belonging to or in the possession of FPS as well as personal data and special personal data relating to individuals.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.
Information Security Forum	Information Security Forum is a forum coordinated by the Group ISO and comprising of OpCo ITSSS'. Its purpose is to work on information security issues and best practices. The security forum will advise the VP IT about measures increasing the information security level of the organization.
Information Security Management System (ISMS)	The ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.
IT System & Support Specialists (ITSSS)	The Group ITSSS is the person appointed by FPS who is responsible for ensuring that information security processes at FPS HQ and OpCos are coordinated in accordance with this ISP. The OpCos ITSSS the person appointed by FPS who is responsible for ensuring that the information security processes at

	the OpCos are coordinated in accordance with this ISP. The ITSSS is the linking pin between both business and IT and the Group ITSSS.
Measure	See Control.
Operating Company or OpCos	A corporation or company owned or controlled by FPS. A corporation is controlled by FPS either when FPS has effective control and/ or majority ownership (e.g. subsidiaries, joint-ventures and franchisees).
Personal Data	All data relating to an identified or identifiable natural person or Data Subject. Personal Data that is encrypted or hashed is Personal Data. Personal Data that is anonymized to the extent that it cannot be re-identified, according to applicable IT security standards, no longer qualifies as Personal Data.
Security Manager	The person appointed by FPS who is responsible for the operational aspects of protecting IT assets (preventive) and the operational handling of security incidents (resilience) within FPS. Security Managers exist both within FPS HQ and the OpCos.
Special Personal Data	Personal Data as described in the applicable Data Protection Act (DPA) including, without limitation, medical data and biometric data for the purpose of uniquely identifying a nature person, personal data revealing race or ethnic origin, political opinions, religious or philosophical belief and trade union membership.
System Administrator	The person appointed by FPS who is responsible for implementing, running and maintaining the systems in accordance with the Information Security Policy.
Third Party	A person that, or a legal entity which, is not part of FPS or FPS group. A Third Party may however work with, or on behalf of, FPS or its Operating Companies. A Third Party can, in practice, be a Data Processor on behalf of FPS.

Global IT and Turkey Performance Director

Doğan Ali Yılmaz


  
07.07.2023