SECURITY STATEMENT

www.fssc.com

Version 1.1 Maart 2025

CONTENTS

REVISION HISTORY TABLE

Rev.	Date	Nature of Changes	Approved By
0.1	May 2022	First draft	Matthijs
0.2	August 2022	Review IT Controls	Hent
1.0	07/09/2022	Original issue	Management board
1.1	26/03/2025	Textual Updates	Paula van Petersen & Melle Koedijk

1 SECURITY STATEMENT

The Foundation FSSC and its underlying wholly owned legal entities (hereinafter: 'FSSC'), are committed to protect its data and that of our clients from threats and/or threat actors like hackers, human errors, abuse, leakage, fire, theft and so forth. This is necessary to prevent damage to the interests of the parties involved – including FSSC itself – and to be able to (continue to) provide effective, efficient, competitive and reliable services. Protection of information is set out in terms of Confidentiality, Integrity and Availability.

This statement is aimed at providing you with more information about our security practices. For more information about how we handle personal data, we refer you to our Privacy Statement.

1.1 PRINCIPLES

The principles of information security within FSSC reflect the organization values and thus create the basis for executing the information security management process:

- Information security management at FSSC always follows a risk based approach;
- the Information Security Management System (based on ISO 27001) is subject to continuous improvement, ensuring its effectiveness and alignment with organizational strategies;
- the Management Board is accountable for information security related decisions and
- information security is a combined organizational effort, every FSSC team member is responsible for contributing towards information security objectives in their role and related daily activities.

1.2 OBJECTIVES

FSSC aims to provide trust and deliver impact to the consumer goods industry by, among others, adequate information security management. To support the achievement of these goals, FSSC has established the following information security objectives:

- establishment of a policy framework to support the organization in managing its information security risks;
- promote cybersafe behavior by continuously addressing information security awareness;
- composition of a governance structure by defining roles and responsibilities to create ownership and responsibility on information security across the organization and
- market trust by the establishment and continuous operation of an Information Security Management System to bring and keep its information security risks in control to protect its interests and assets.

1.3 HOW DO WE DO THIS?

The Management Board is accountable for information security and have set out a Security & Privacy Office to be responsible for security management. All managers within FSSC are directly responsible for implementing and maintaining security for their respective business areas. It is the responsibility of all FSSC Team Members to adhere to the security policies. The Security Officer is responsible for maintaining the Security Policy and provide guidance on its implementation.

Specifically, security at FSSC is ensured through the following:

- FSSC maintains a written Information Security Policy that defines the responsibilities of FSSC Team Members and acceptable use of information system resources.
- The Security & Privacy Office manages the Information Security Management System based on the ISO 27001-standard to ensure a risk-based approach and continuous improvement.
- The Security & Privacy Office and responsible managers set-up and maintain operational security policies and other controls.
- FSSC Team Members are periodically reminded of their role in information security in various ways such as newsletters, trainings or workshops.
- In corporation with our partners, security is always part of the discussion. We aim to use security-by-design and privacy-by-design principles as much as possible in developing new functions or systems.
- FSSC has an incident response plan for when the confidentiality, integrity or availability of information is breached. This plan includes the inclusion of an external Computer Emergency Response Team. The incident process and escalation to the external CERT is trained yearly.
- In case of a (cyber) crisis or discontinuity of our services FSSC has a Crisis Manual to mitigate the situation as fast as possible.

1.4 INTELLIGENT SECURITY OPERATIONS

In order to ensure an adequate level of information security at FSSC, we work together with Northwave. Northwave is a cyber security company which specializes in a 360 degree view on information security in business, bytes and behavior. The Security & Privacy Office of Northwave provides knowledge, skills and structure to continuously improve security at FSSC.

1.5 VULNERABILITIES

Although FSSC takes security of our systems very seriously, there could be vulnerabilities which we don’t know. If you have found a vulnerability, we kindly ask you to provide us with the information so we can mitigate the issue as quickly as possible. Please send us an e-mail at security@fssc.com.