Spotler Group BV
Henri Faasdreef 312,
2492 JP Den Haag
Telephone (088) 103 0999
Email: contact@spotlergroup.com
www.spotlergroup.com

Information Security Policy

How we secure our company

Version	1.0
Status	Approved
Date	28 Juni 2024
Authors	M. Spee
Reference	P002
Classification	Public

Documentmanagement

Document history:

Version	Date	Author	Change
0.1	06-05-2024	M. Spee	Initial Concept
1.0	28-06-2024	K. Cooper	Approved
1.0	24-09-2024	L. Chadwick	Approved

Distribution:

Name	Function	Date	Version
K. Cooper	Tech Ops Director	22-05-2024	0.1
L. Chadwick	CEO Spotler Group	24-09-2024	1.0

1. Purpose

The purpose of the Information Security Policy is to describe the information security objectives of Spotler Group for protecting our information assets. This is the primary policy under which all other information security related polices reside. A minimum standard is achieved by following this policy.

Spotler Group has established an Information Security Management System (ISMS) framework to support this policy. The framework consists of policies, processes and procedures supported by both management and technical controls appropriate to the risk profile of Spotler Group.

2. Definitions

An '*information asset*' is information held by Spotler Group that is private, confidential or has value to Spotler Group. It includes third party information (such as Client or Supplier data) and Spotler's IT systems.

Information, and related processes, systems, networks, and people are also important assets in achieving information security objectives. Spotler Group information assets are grouped into the following categories:

- Information - such as data, customer data, intellectual property, knowledge, application, and system software documentation, not only in electronic media (databases, files in PDF, Word, Excel, and other formats), but also in paper and other forms.
- System and Software – our products, applications, software, and source code.
- Infrastructure – our IT infrastructure, servers, routers, switches, firewalls, etc.
- People - often a single point of contact and have information in their head which is not available in other forms.
- Facilities – our offices, buildings, and data processing facilities.
- Outsourced services, like legal services or cleaning services, and online services like Windows 365 or Exact. Whilst these may not be considered assets as per the definition, such services need to be similarly controlled.

3. Scope

This policy, together with all supporting controls, processes, and procedures, applies to:

- All Spotler personnel, regardless of location. This includes any personnel under the supervision, guidance, or management of Spotler staff and external parties that provide information processing services to Spotler.
- All Information Assets for which Spotler has ownership and/or a legal, regulatory, or contractual responsibility.

This policy extends to information assets held by Spotler Group on behalf of third parties and partners, and by third parties and partners on behalf of Spotler Group.

4. Responsibilities

All personnel are responsible for compliance with this policy and the framework that underpins it. Managers are responsible for implementing this policy and ensuring compliance within their teams.

The Head of Information Security is responsible for:

- the implementation and deployment of the ISMS across Spotler Group
- defining, managing, and ensuring compliance with the ISMS.

5. Information Security Objectives

The following objectives apply across Spotler Group:

a) Protect the confidentiality, integrity, and availability of Spotler's information assets.
b) Provide information with minimal disruption to personnel, suppliers, clients and interested parties, as required by Spotler Group and the appropriate compliance and regulatory framework.
c) Increase client confidence in Spotler's ability to protect client information entrusted to it.
d) Protect the reputation of Spotler Group and enhance Spotler's brand value.
e) Reduce the risk of information security breaches, incidents and loss of data and information assets.
f) Comply with data protection laws on the protection of personal data, both as a data controller and as a data processor (See Privacy Policy for further information).
g) Reduce the risk of personal data breaches and protect the rights of data subjects (See Privacy Policy for further information).
h) Increase personnel and supplier awareness to information security threats.
i) Recognize Spotler expertise in applying management systems by gaining third party recognition of the ISMS.
j) Provide a structured approach to securing information, led by senior management who are committed to continual improvement of the ISMS.

6. Intent of the ISMS

The Spotler Group Board and the Spotler Management Team's support the information security objectives and the Tech Ops Director is responsible for Information Security within the Spotler Board.

Spotler Group commits that it will:

a) Take a risk-based approach to managing information assets to minimize the risk of information security breaches.
b) Allocate resources, responsibility and authority which will be regularly reviewed by Executive Management to ensure the ongoing protection of Spotler Group's information assets including client data.
c) Monitor and review the ISMS by regularly assessing the effectiveness of the ISMS, against the Information Security Policy, objectives and plans.
d) Report findings related to the performance of the ISMS to the Spotler Group board for review.
e) Maintain and improve the ISMS, based on the results of the internal ISMS audit and the management review process, both of which will identify corrective actions, as well as issues, risks, and opportunities.
f) Consider legal and regulatory requirements, specifically when monitoring and reviewing the ISMS and running the internal compliance program.
g) Adopt business continuity management practices, to protect critical business processes from unplanned disruptions.
h) Report any actual or suspected breaches of information security to line managers. These will be recorded and investigated by those with responsibility for information security, led by the Head of Information Security.
i) Ensure all personnel, suppliers, clients and interested parties (including visitors) are made aware of their information security obligations through communications, contracts, training, and policies.

7. Compliance

Policy compliance will be monitored by the Head of Information Security and in accordance with the information security procedures. Activities related to the policy may be logged and audits of control effectiveness will be undertaken by the Information Security Officer (ISO), as part of the Information Security Management System (ISMS), and by the Internal Auditor. External audits will be carried out as part of our ISO 27001 certification.

Failure to comply may be treated as a disciplinary matter and addressed in accordance with contracts of employment and HR (Human Resource) disciplinary policies. Appropriate action will be taken in all cases of suspected criminal activity and offences may be reported to the local law enforcement agency or other proper authority and could lead to civil or criminal proceedings.

If personnel are in any doubt that an action is not compliant with policies, or need assistance with interpreting or applying these policies, they should seek advice from their line manager or the Information Security Officer.

All security incidents and data breaches must be reported immediately to the Head of Information Security via the following link: securityofficer@spotler.nl

8. Improvement

Spotler Group strives to continuously improve its information security and adopt its information security management system to significant changes in the organization, technology or in the external environment. Spotler Group will keep its information security current and in line with the expectations of its customers and the applicable legal requirements.

9. Signature

Lee Chadwick, CEO Spotler Group