Hawk Information Security Policy

Version	3.4
Status	APPROVED
Expires	Jul-30-2026
Owner	@Benjamin Pannier
Classification	RESTRICTED
Effective Date	Thu, 31 Jul 2025 09:47:44 GMT

Mission statement and introduction

At Hawk, safeguarding our clients' data and ensuring the reliable operation of our services is not just a responsibility — it is a matter of **trust**.

Today more than ever, information security is essential to organizations of all sizes. Not one day passes without a large- or small organization disclosing a data breach, being a victim of a ransomware attack, or similar catastrophic information security incidents. Our customers entrust Hawk with the financial- and personal information of millions of people, businesses, and organizations, for which a breach would mean a significant loss of privacy, financial resources, reputation and people's careers. Over the years since we started in 2018, we have invested a significant amount of our focus, energy, and resources in ensuring that information stays private,

protected, and in compliance with the laws and regulations. Introducing an information security management system is now the logical next step to further commit us toward that goal.

A structured approach is essential for the effective and, above all, sustainable implementation of information security. This is why we have implemented an information security management system (ISMS) at Hawk, which has the task of creating, maintaining, and improving information security in a continuous process. This structured, mature, and streamlined approach is essential to show and prove our commitment to information security to our existing and future clients.

The Information Security Policy is central to the entire information security process. In addition to the obligation of the management for information security, it defines goals and the importance of information security with the respective responsibilities. Supporting policies are used, drawn up together with the teams, and rolled out in the company. The cooperation between the Management, the teams, and the Information Security Officer enables practical and effective information security.

Information security is an essential part of safeguarding the continued existence of our company and, accordingly, has a high priority at Hawk and our client's TRUST. Hence everyone needs to play their part and must observe and adhere to the specifications and policies on information security.

Purpose, scope, and Users

This top-level policy aims to define the purpose, direction, and basic rules for managing information security within Hawk. It serves to:

- Protect Hawk's assets and information
- Comply with legal and contractual obligations
- Support continuous improvement
- Promote awareness and accountability among all users
- Address internal and external issues relevant to information security and satisfy the needs of interested parties.

These rules are in place to protect customers, employees, and Hawk. Inappropriate use exposes Hawk to risks, including virus attacks, compromise of network systems and services, and legal and compliance issues.

The Hawk "Information Security Policy" comprises this policy and all Hawk policies referenced or linked within this document.

This policy applies to:

- All aspects of the ISMS as defined in the ISMS Scope Document
- All employees, contractors, and relevant external parties

Terminology

Information security principles - Confidentiality, Integrity, Availability (CIA)

The CIA Triad is an information security model. It guides an organization's efforts toward ensuring information security. The three principles - confidentiality, integrity, and availability, which stands for CIA in cyber security, form the cornerstone of a security infrastructure. It is ideal for applying these principles to any security program.

Confidentiality

Ensuring information is accessible only to authorized parties, persons, systems, or processes.

Protecting the confidentiality of information includes:

- Controlling access to information
- Preventing network sniffing (e.g., man-in-the-middle)
- Prevent a data breach- or leakage

Integrity

Ensuring information is changed only by authorized parties or systems in an allowed way.

Protecting the integrity of information includes:

- Mitigating human error risk
- Preventing malicious actors from gaining access and changing information
- Establishing change control processes
- Preventing unintended transfer errors
- Ensuring no misconfigurations or security errors impact information
- Hardening hard- and software systems to prevent a compromise
- Auditing processes and procedures to ensure traceability

Availability

Ensuring information can be accessed by authorized persons when it is needed

Protecting the availability of information includes:

- Preventing natural disasters, human error, or storage failures from impacting physical integrity
- Protecting against system overload
- Protecting against physical theft of storage devices

Information security – preservation of confidentiality, integrity, and availability of information

Information Security Management System – part of overall management processes that take care of planning, implementing, maintaining, reviewing, and improving the information security

Business Terminology

C-Level Management Team - Chief Executive Officer, Chief Technology Officer, Chief Product Officer

ISMS Team - CISO, ISO, IT Security Engineers, technical team leads

Managing the information security

Objectives and measurement

The general objectives for the information security management system are the following:

1. Install a continuously improving state-of-the-art information security system to reduce the likelihood and impact of potential incidents significantly
2. Make transparent and prove our commitment to information security to existing and prospective clients
3. Guide our decisions as we build out our platform globally, addressing the local needs of customers and regulations
4. Provide a framework for employees

Objectives for individual security controls or groups of controls are proposed by:

- The technical teams, e.g., Non-functional requirements (NFR), Fraud & AML (FRAML), Direct customer (Dc), Transaction monitoring (TM), Screening, Banking, Platform Engineering (Pe)
- the C-Level Management Team
- the Chief Information Security Officer

and approved by the C-Level Management Team in the Statement of Applicability.

The C-Level Management Team must review all the objectives at least once a year.

The **Chief Information Security Officer (CISO)**:

- Defines the information security strategy
- Defines the measurement methods and frequencies
- Coordinates evaluations with responsible owners
- Analyzes results and prepares inputs for the annual Management Review

Hawk will measure the fulfillment of all objectives. The Chief Information Security Officer is responsible for setting the methods for measuring the achievement of the objectives. Their respective owners will perform the measurements at least once a year.

Information security requirements

This Policy and the entire ISMS must comply with legal and regulatory requirements relevant to Hawk in information security and personal data protection, such as EU GDPR and contractual obligations.

Hawk's internal Legal Registry provides a detailed list of all contractual and legal requirements.

Information security controls

The Risk Assessment and Risk Treatment Methodology documents define the controls and safeguards. Hawk's risk tolerance and criteria for accepting information security risks are defined in the Risk Management Policy.

The Statement of Applicability lists the selected controls and their implementation status.

Responsibilities

Responsibilities for the ISMS are the following:

- C-Level Management
  - Ensures the ISMS is implemented and maintained in accordance with this Policy
  - Allocates sufficient resources for ISMS effectiveness
  - Reviews the ISMS at least annually or upon significant change
  - Defines which information related to information security is communicated to which interested party (internal and external), by whom, and when
  - Approves ISMS objectives in the Statement of Applicability
  - Commits to the continual improvement of the suitability, adequacy, and effectiveness of the ISMS itself
- Chief Information Security Officer (CISO)
  - Responsible for the operational coordination of the ISMS
  - Coordinates compliance with information security policies
  - Leads employee awareness and training programs
  - Defines methods for measuring objective fulfillment
  - Analyzes and reports performance data during the Management Review
  - Maintains documentation such as the Measurement Report and Risk Treatment Plan

- Data Protection Officer (DPO)
  - Ensures compliance with applicable data protection laws, including GDPR
  - Oversees processing of personal data across the organization
- Asset Owners
  - Responsible for ensuring confidentiality, integrity, and availability of assigned information assets
  - Participate in the risk assessment and control implementation relevant to their assets
- Employees and Contractors
  - Must report data breaches, policy violations, or security incidents to the CISO
  - Must adhere to all information security policies and procedures
  - Are expected to complete regular awareness training

Policy communication

The CISO is responsible for ensuring that this policy is communicated and understood by:

- All employees and contractors
- Relevant third parties

Awareness training is conducted at on-boarding and refreshed annually. Please see Information Security Awareness Schedule for more details.

Support for ISMS implementation

The C-Level Management Team will support the ISMS implementation and continual improvement with adequate resources to achieve all objectives set in this Policy and satisfy all identified requirements.

Security Incident Reporting

All personnel must report known or suspected security incidents or policy violations promptly via:

- Slack: `#security` channel
- Email: `security@hawk.ai`
- Direct reporting to their manager or team lead

Reports should include a clear description and relevant context/details.

Additional Policies and Procedures

Policy	Purpose
Acceptable Use Policy	To share what is acceptable use and unacceptable use
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Business Continuity Policy	To prepare Hawk in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Clear Desk and Clear Screen Policy	To minimize the risk of unauthorized access to, or theft of, sensitive and confidential information by ensuring that desks are clear of such material and screens are locked when unattended.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Information Classification and Handling Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Physical Security Policy	To prevent unauthorized physical access or damage to the Hawk's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Hawk's information security risks in order to achieve the company's business and information security objectives.

Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
Third-Party Management Policy	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Policy Violation and Enforcement

All Hawk personnel must report violations of **any** policy to the CISO, the CTO or their team leads/managers.

All Hawk personnel (including employees, contractors, and relevant third parties) must maintain the security, confidentiality, availability, integrity, and privacy of Hawk assets. Violations of ISMS policies and procedures may be considered severe breaches of trust, resulting in disciplinary action up to and including termination of employment or contract and prosecution following applicable federal, state, and local laws.

Policy Exemptions and Exceptions

Hawk personnel must request an exception to **any** policy to the CISO for approval, as described in the related policy on exceptions.

Validity and document management

The owner of this document is the C-Level Management, who must review and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the Management Team needs to consider the following criteria:

- the number of employees and external parties who have a role in the ISMS but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization

- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

Changelog

Version	Date	Author	Approver	Description
1.0	Dec 6, 2021	SL	WB	Initial
2.0	May 3, 2022	SL	WB	• add exception and violation rules here • incident responds • mobile device policy • Remote Access Policy • Acceptable Use Policy • all other policies linked
2.1	Jun 6, 2023	WB	WB	Reviewed Policy and it's objectives, small updates on C-Level Team and Development Teams. Reviewed also with SL.
2.2	Jun 24, 2023	SL	(automatic)	Fixed links in the policy listing, edited minor grammar improvements, removed Jira links.
2.3	May 31, 2024	SIL	(automatic)	Reviewed for brevity and currency according to 2024 organizational objectives.
2.4	Sep 2, 2024	SL	WB	• Added Chief Risk Officer where applicable, retired CTO mentions • Changed ISMS responsibility to C-Level Management • Changed HAWK:AI to Hawk as branding changed

Page ID	Page Title	Version	Version Decription	Version Owner	Version Created	Version Approved	Approvals
3246260225	Hawk Information Security Policy	3.4 (66)	Correction of department names	ester.widera_ext	Wed, 30 Jul 2025 16:47:51 GMT	Wed, 30 Jul 2025 16:47:53 GMT	
3246260225	Hawk Information	3.3 (64)	Updates on CISO	Jovica Ilic	Tue, 29 Jul 2025	Tue, 29 Jul 2025	

Page ID	Page Title	Version	Version Decription	Version Owner	Version Created	Version Approved	Approvals
	Security Policy		responsibilities and exception management		18:04:44 GMT	18:04:45 GMT	
3246260225	Hawk Information Security Policy	3.2 (63)	Minor updates	ester.widera_ext	Tue, 29 Jul 2025 17:35:22 GMT	Tue, 29 Jul 2025 17:35:23 GMT	
3246260225	Hawk Information Security Policy	3.1 (61)	Added Additional links to other policies, clarified statements	Stefan Langwald (ext.)	Tue, 10 Jun 2025 15:14:16 GMT	Tue, 10 Jun 2025 15:14:18 GMT	
3246260225	Hawk Information Security Policy	3.0 (59)	Finally boost this document to V3 without any additional changes	Benjamin Pannier	Thu, 05 Jun 2025 07:33:37 GMT	Thu, 05 Jun 2025 07:33:39 GMT	
3246260225	Hawk Information Security Policy	2.0 (58)	boost the version without changes	Benjamin Pannier	Thu, 05 Jun 2025 07:32:33 GMT	Thu, 05 Jun 2025 07:32:35 GMT	
3246260225	Hawk Information Security Policy	1.0 (57)	boost the version without changes	Benjamin Pannier	Thu, 05 Jun 2025 07:31:23 GMT	Thu, 05 Jun 2025 07:31:24 GMT	
3246260225	Hawk Information Security Policy	0.1 (56)	Version 2.5 Syntax updated to align with organizational and compliance objectives Cleanup for clarity, grammatical corrections Improved definition of Purpose, Scope and Users Added ISO and Role definition Infosec Controls section overhauled	ian.looney	Tue, 03 Jun 2025 18:46:07 GMT	Tue, 03 Jun 2025 18:46:09 GMT	

Page ID	Page Title	Version	Version Decription	Version Owner	Version Created	Version Approved	Approvals
			to be more comprehensive Responsibilities updated Policy Communication section overhauled				