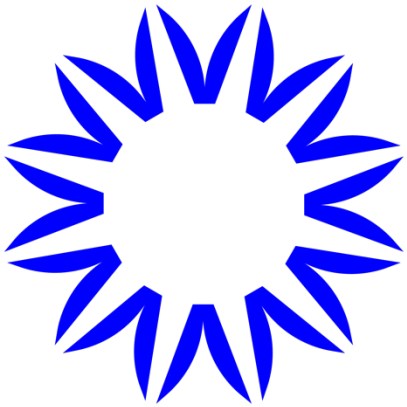


HAWK INFORMATION SECURITY PRIVACY POLICY

Data Classification	**Public**
Author	Ira Goel
Approver	Management
Approved Date	Dec 09, 2024
Effective From	Dec 10, 2025
Current Version	1.0

1.0 Introduction

Information Security and Privacy Policy is central to the entire information security and privacy processes of Hawk. It reflects to the obligation of the management for information security, defines goals and the respective responsibilities.

2.0 Purpose

Information Security and Privacy Policy is the top-level Policy and aims to define the purpose, direction, principles, and basic rules for information security and privacy management at Hawk. These rules allow Hawk to protect its customers, its employees, and its business.

3.0 Scope

The policy applies to:

1. All Hawk-managed offices, facilities,
2. Cloud production environments, particularly the AML services Hawk provides to its clients, and
3. All employees and involved people-resources.

4.0 Mission

Hawk has extraordinary responsibilities for our client's data and the flawless, reliable operation of the critical service we provide to them on that data. It's a matter of TRUST, our client's TRUST.

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.

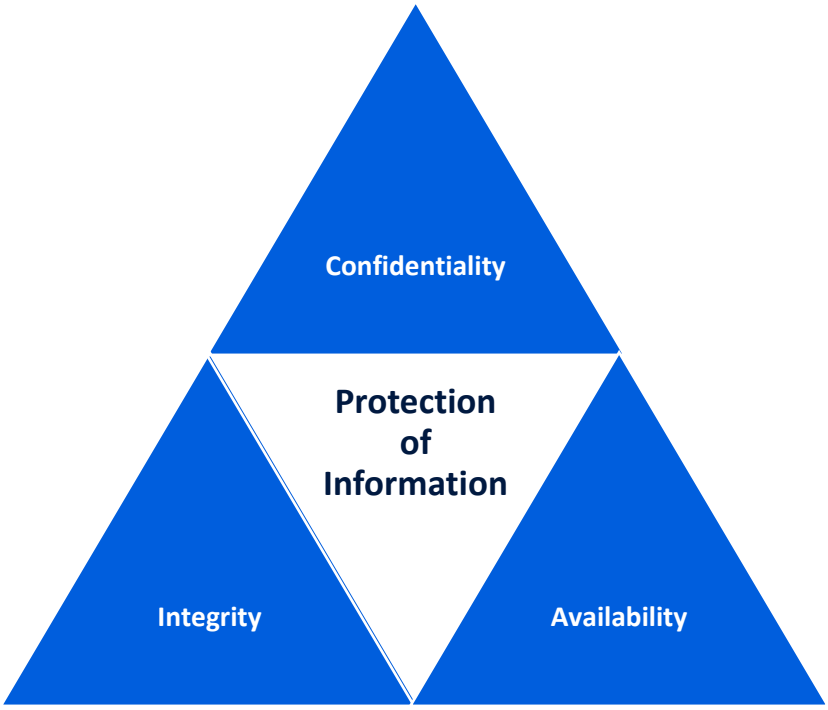
Over the years since we started in 2018, we have invested a significant amount of our focus, energy, and resources in ensuring that those information stays private, secure, protected, and in compliance with the laws and regulations.

Information security and privacy are 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.

5.0 Information Security and Privacy

5.1 Information Security Principles

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program at Hawk is designed to implement one or more of these principles.



- **Confidentiality**: To ensure that only authorized users have access to information assets
- **Integrity**: To ensure the accuracy and completeness of information assets
- **Authenticity**: To ensure the person's identity is maintained; that they are who they say they are
- **Availability**: To ensure that authorized users have access to information assets when required

Information security is achieved by implementing a suitable set of controls, including organizational structures, policies and procedures, processes and technical IT controls. These controls need to be designed, implemented, monitored, reviewed and improved.

5.2 Privacy and Data Protection

The protection of personal data is generally referred to as the protection of individuals' privacy. This document establishes applicable guidelines with regards to handling of private information, generally referred to as Personal Data Protection.

Personal data means any information relating to an identified or identifiable natural person ('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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Hawk adheres to the definitions of personal data defined in the regulations of the jurisdictions it operates in.

5.3 Information Security and Privacy Domains

5.3.1 Information Security and Privacy Governance

Information security and privacy governance is the combination of information security and privacy processes and structures implemented by the management of Hawk to inform, direct, manage and monitor the information security and privacy activities of the company towards the achievement of its information security and privacy objectives.

5.3.2 Information and Privacy Risk Management

Information and Privacy risk management encompasses the establishment of information security and privacy controls for the protection of Hawk's information regardless of the form or source of that information.

- Hawk has established information security and privacy controls on a risk-based approach that uses the criticality of information with regards to the previously defined information security and privacy dimensions to select the required controls. This process is known as information classification.
- Information and privacy risk management also encompasses the implementation of a number of secondary security control domains such as human resources security, information security, data protection, incident management, business continuity management and compliance.

5.3.3 Physical Security

Physical security encompasses the establishment and implementation of physical security controls for all physical premises of Hawk such as office spaces, archives, and technical rooms. The objective of physical security is to ensure the protection of information assets contained in the physical premises against unauthorized access, modification or destruction.

5.3.4 IT Security and Privacy

IT Security encompasses the establishment and implementation of IT security and privacy controls for information in electronic form that is processed, stored or transmitted on IT infrastructure created or managed by Hawk. The IT security and privacy controls can be technical IT controls, organizational IT controls as well as IT control processes. Their purpose is to avoid unauthorized access, modification or destruction of information situated on IT systems.

6.0 Hawk's Practices and Team

Hawk's information security and privacy practices are combination of industry standards and best practices. To this effect, HAWK is ISO 27001 and SOC 2 Type certified.

Hawk has a small but effective information security and privacy team, comprising of Information Security Officer, Data Protection Manager, and team members.

7.0 Policy Governance

Any violations to **any** Hawk Policy must be reported to the Information Security Officer at security@hawk.ai.

All Hawk personnel (including employees, contractors, and relevant third parties) must maintain the security, confidentiality, availability, integrity, and privacy of Hawk assets. Violations of Hawk 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.