HAWK ORGANIZATIONAL, INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) MEASURES

Data Classification	**Public**
Author	Ira Goel
Approver	Management
Approved Date	Dec 12, 2024
Effective From	Dec 12, 2024
Current Version	1.0

1.0 Introduction

Hawk's organizational, and information and communication technology (ICT) measures are core controls direct information security and data protection activities in alignment with Information Security and Privacy policy.

2.0 Purpose

Organizational and ICT controls document lists core control categories that drive the information security and data protection activities at Hawk.

3.0 Scope

The document applies to:

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

4.0 Organizational and ICT Controls

4.1 Organizational Controls

Hawk's Technical Organizational Measures ensure our services and offerings have an adequate level of protection in accordance with the GDPR, other global regulations and standards. The controls align with the principles of confidentiality, integrity and availability.

4.1.1 Confidentiality

- Measures for access control of data processing centers
  - Physical security controls for the data center of the Cloud Service Provider
  - Physical security controls for Hawk
- Measures for access control of data processing systems
  - Access controls

▪ Password policy and MFA controls

  - Authentication and Authorization Controls
- Measures for access control of personal data in data processing systems
  - Authentication and authorization controls
  - Least privilege access
  - Role-based access controls
- Measures of separation control
  - Segregation of duties
- Pseudonymization measures

4.1.2 Integrity

- Measures for transfer control
  - Encryption and cryptography

    - Tokenization
    - Secure data transfer controls
    - Access controls
- Input control measures

4.1.3 Availability and Resilience

- Availability control
    - Uninterrupted power supply controls
    - Backups
    - Redundant application architecture and availability zones
    - Endpoint protection controls
    - Incident management
    - BC/DR controls
    - Crisis management

4.1.4 Procedures for Regular Review, Assessment and Evaluation

- Data Protection Management
    - Data subject requests
    - Cookies management
- Incident Response Management
    - Crisis management
    - Incident response plan
    - BC/DR plan
- Order Control
    - Purpose limitation
    - Data processing agreement

4.2 ICT Controls

Hawk drives many of its ICT controls from its organizational capabilities. To achieve this objective, Hawk has mapped ICT activities to its organizational controls.

ICT and DORA Pillar	ICT and DORA Actions	Organization Capabilities
ICT Risk Management	▪ Inventory and Scope ICT assets (incl. supporting applications and tooling). ▪ Integrate ICT risks into existing risk management framework. • Integrate and review response and recovery processes. • Strengthen awareness and cyber risk hygiene plans.	• Cyber governance • Security risk management framework • Important business services • Network and Infrastructure security • Third party security • Information security policies and standards • User access management • Change management • Incident Response/SIEM • BCP/DR/Crisis Management

		• Security Awareness • Vulnerability Management • DevSecOps • Crisis Communications
ICT Incident Management	• Update incident classifications according to DORA requirements. • Update incident reporting processes for major incidents. • Review crisis communication strategies.	• Incident Management • Incident Response • Crisis management
Digital Operational Resilience Testing	• Perform 'Stress-Test'. • Perform the required level of threat-led penetration testing. • Align testing procedures with DORA testing requirements.	• Vulnerability management ▪ DevSecOps • Penetration Testing • Source code reviews • Network security • Secure configuration ▪ SAST/DAST • Cyber scenario testing
Third Party Risk Management	• Map third parties. • Evaluate vendor exit strategies. • Contract reviews. • Risk concentration including third party dependencies.	• Third party risk management • Critical ICT third party service providers • Multi-vendor strategy
Information Sharing	• Build a trusted community and ecosystem for Hawk's clients to share cyber threat information and intelligence.	• Incident Response • Threat Intelligence • Cyber Governance • Guaranteed data security

4.3 Other Information Security, Privacy and Data Protection Controls

In addition, to the above controls, Hawk is certified under ISO 27001 and SOC 2 Type 2 standards. Thus, also complies with:

- ISO 27001 Information Security Management System
  - Chapters 4-10
  - Annex A
- ISO 27002 Information Security Controls
- COSO controls for Security Operations Criteria (SOC) Type 2
- Information security and data protection controls imposed by the regulations in which Hawk operates.

5.0 Hawk's Practices and Team

Hawk's information security and privacy practices are a combination of industry standards and best practices.

Hawk has an information security and privacy team, comprising of Information Security Officer, Data Protection Manager, and team members.

6.0 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.