Data Classification Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

The Data Classification Policy provides a way to categorize any data processed by the Superhawk AI staff, software, and systems. The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value, and criticality to the organization. By understanding the types of available data, their classification, and access level, one shall be able to map the appropriate access or level of protection needed. This clarity ensures that critical company data can be secured.

2. Scope

The Superhawk AI Data Classification Policy applies to all data handled, managed, stored, or transmitted by Superhawk AI, its employees, contractors, and systems. This includes data stored in cloud platforms (for example AWS and GCP), data in code repositories (GitHub), and data in employee devices such as company-managed laptops and workstations. Managers and information owners shall assign the appropriate classification when data is created, modified, or ingested into company systems.

3. Policy Statement

Each individual at Superhawk AI shall be responsible for reviewing, adhering to, and handling data according to the classification levels defined below. The Data Classification definitions below provide a list of various types of data and their classification levels. In case of difficulty in identifying a specific data element or uncertainty regarding the associated risk and appropriate classification and handling, individuals are encouraged to contact Superhawk AI's Information Security Officer for guidance and assistance.

4. Data Classification Definitions

Superhawk AI’s data is classified as follows:

4.1 Public Data

This data or information may be shared with any person, organization, or system regardless of their relationship with Superhawk AI. This classification is not limited to data or information meant for public consumption but also includes any data or information that requires no special handling or any kind of safeguarding from disclosure. The distribution of such data does not expose Superhawk AI, its customers, or its partners to any harm.

Examples of Public Data include product blogs, company websites, press releases, marketing collaterals, career pages, etc.

4.2 Company Internal Data

This data shall be accessible by all staff within Superhawk AI and may be required for the smooth operational functioning of the organization. Such information shall not be made available to parties

outside Superhawk AI but may be shared if requested.

Examples of Company Internal Data include Information Security Policies & Procedures, HR Policies, Leave Policies & Holiday Lists, Operational Procedures, etc.

4.3 Company Confidential Data

This data & information shall be accessible by pre-authorized staff members and shall not be made generally available within Superhawk AI. Unauthorized access or disclosure could cause significant financial or material loss and poses a risk to Superhawk AI if exposed. Such exposure can lead to breaking contractual obligations and may adversely impact Superhawk AI, its partners, employees, and eventually its customers. Such information needs to be protected from unauthorized access and changes. Note that access to such data may also be limited to specific staff members or groups of staff members like executives, HR, legal teams, etc.

Examples of Company Confidential Data include employee salaries, legal documents, internal product specifications, customer lists, strategy documents, internal roadmaps, design documents, internal memos, emails, etc.

4.4 Customer Confidential Data

This data, if accessed by unauthorized parties, may adversely affect Superhawk AI's customers. This includes data that Superhawk AI is required to keep confidential, either by law or under a customer agreement. The company needs to protect such information from unauthorized access and unauthorized modification. Customer Confidential Data needs to be safeguarded when it is stored, processed, used, and transmitted.

Unauthorized access to such data can violate contractual confidentiality agreements with customers, cause a security incident, or affect Superhawk AI's customer and industry confidence.

Examples of Customer Confidential Data include data provided by customers by using our system, information on customer accounts, personally identifiable information of customers (or customers' customers), etc.

4.5 Personal Data

This data, if accessed by unauthorized parties, may adversely affect the privacy of individuals. Personal Data refers to any data relating to an identifiable individual or person. This includes data Superhawk AI is required to safeguard, either by law (GDPR for EU citizens' data) or under a customer agreement. The company needs to protect such information from unauthorized access and unauthorized modification. Personal Data needs to be safeguarded when it is stored, processed, used, and transmitted.

Unauthorized access to such data may potentially violate the law, break contractual data protection agreements with customers, cause a security incident, or affect Superhawk AI's customer and industry confidence.

Examples of Personal Data include name, email, phone number, IP Address, political views of individuals, cookies, Personal Health Records, Credit Card information, etc.

Note that personal health records, credit card information, and other sensitive personal data may be subject to additional laws based on the location of the owner of such data. For example, HIPAA regulations shall apply to US citizens' personal health information.

5. Labeling of Information

Asset owners should apply labels or tags to electronic information stored in cloud platforms (AWS, GCP), GitHub repositories, and company-managed devices to indicate classification level. Acceptable technical labeling methods include metadata tags in cloud storage objects, repository access controls and directory structure in GitHub, and classification labels applied to documents in Google Workspace. For physical media, apply a visible classification label where applicable. Where labeling is not technically feasible, owners must document the classification in the asset inventory and communicate handling requirements to relevant staff.

In general, most of the critical information managed by the company is in an electronic format.

6. Document Security Classification

Company Internal (as described in section 4.2 of this document).

7. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

8. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

The Information Security Officer shall coordinate with IT/Infrastructure (managing AWS and GCP), Engineering (managing GitHub repositories and deployment practices), and Operations (managing Google Workspace) to ensure classification labels are applied and enforced. Managers and data owners are responsible for assigning and documenting classifications for assets under their control. All employees and contractors must follow handling and labeling requirements and report classification uncertainties to the Information Security Officer.

9. Schedule

This document shall be reviewed at least annually and additionally when there are significant changes to systems, third-party providers (e.g., adding or removing AWS, GCP, GitHub, or Google Workspace integrations), applicable laws (such as GDPR), or organizational structure.

End of Data Classification Policy. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026