Draup

Information Security (IS) Policy

Information Security Policy

Draup is committed to safeguarding the data in its possession. Our customers and other stakeholders depend on us to protect their resources. Thus, it is crucial for all Draup staff to understand what information security is and the steps we can take to protect the security, availability, and confidentiality of the data we are committed to protecting.

Information Security Officer (ISO)

The Information Security Officer leads all the information-security efforts of the company. The Information Security Officer is responsible for identifying potential security threats and risks to the organization, formulating and implementing policies and procedures to combat such threats, and monitoring the efficacy of existing systems. Please refer to the company org chart (shared on the company intranet) to find out who the current Information Security Officer is.

The Information Security Officer has a direct line to the CEO and can communicate with the CEO whenever they need to.

Reporting service issues (failures, incidents, concerns, or other complaints related to the services or systems of Draup)

If any Draup staff believes they have discovered or noticed a service issue (as described above), please take the following first steps:

1. Please report the issue to your manager/supervisor as soon as possible.
2. If your manager/supervisor is not available, please approach the Information Security Officer (ISO) / CEO to report the issue.

Information Security Program

The company has crafted an Information Security Program based on the following pillars.

Information Security Training

All Draup staff are expected to complete information-security training within 30 days of joining Draup and annually thereafter. Further, all Draup staff are then required to acknowledge that they have attended information-security training and understand the information security policy. The training documents are also available on the company intranet for ready reference.

Incident Management

The company's Incident Management and Response Policy outlines guidelines for reporting and responding to security incidents in an efficient manner.

Vulnerability Management

The company's Vulnerability Management Policy describes our process of identifying, classifying, prioritizing, mitigating, and remediating security vulnerabilities.

Data Classification

The company's Data Classification Policy outlines a way to categorize data processed by Draup , its software, and systems, based on levels of sensitivity.

Data Backup

The company's Data Backup Policy describes how operational and other critical data is backed up to protect against loss or corruption.

Data Retention

The company's Data Retention Policy describes how we retain data, and the provisions we provide for customers and users to make data deletion requests.

Encryption

The company's Encryption Policy outlines how we can better protect private, proprietary, and sensitive data by encrypting the data we process at rest and in transit.

Endpoint Security

The company's Endpoint Security Policy describes how we protect unauthorized access to our production systems or critical data via endpoints like laptops that are used by staff members.

Physical Security

The company's Physical Security Policy describes how we protect the physical security of our office premises and other critical systems and devices that can affect the security of critical data.

Acceptable Usage Policy

All Draup staff must acknowledge that they've read and will conform with the organization's Acceptable Usage Policy. Our Acceptable Usage Policy covers staff duties and behavior for using Draup resources and assets, including but not limited to computers, devices, email, internal tools, and social media.

Employee Acknowledgement

All the above security policies, including the Acceptable Use Policy, are presented to new employees during onboarding, and all employees are required to read, review, and acknowledge them.

Non-Compliance

As stated earlier, our customers depend on us to protect their data. In order to uphold their trust in us, it is important to have appropriate penalties for any violations of our information security policy. Draup management will determine how serious an employee's offense is and decide the appropriate penalty. Penalties may include a warning (oral/written) or suspension or termination for more serious offenses.

Questions

If you have any questions regarding this policy, please reach out to the policy owner.

Information Security (IS) Policy

Version	v1
Created By	Scrut Team, Mar 17, 2025
Approved By	Kashish, Mar 26, 2025
Published By	Kashish, Mar 26, 2025