SPOTDRAFT

Data Classification Policy

Version 2 - Approved by Madhav Bhagat

Contents

1. Objective

The Data Classification Policy provides a way to categorize any data processed by the SpotDraft 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 SpotDraft Data Classification Policy applies to all the data handled, managed, stored, or transmitted by SpotDraft and the SpotDraft staff. Managers and information owners shall assign the appropriate classification as and when required.

3. Policy Statement

Each individual at SpotDraft 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 SpotDraft's Information Security Officer for guidance and assistance.

4. Data Classification Definitions

SpotDraft’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 SpotDraft. 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 SpotDraft, 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 SpotDraft and may be required for the smooth operational functioning of the organization. Such information shall not be made available to parties outside SpotDraft 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 SpotDraft. Unauthorized access or disclosure could cause significant financial or material loss and poses a risk to SpotDraft if exposed. Such exposure can lead to breaking contractual obligations and may adversely impact SpotDraft, 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 SpotDraft's customers. This includes data that SpotDraft 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 SpotDraft'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 SpotDraft 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 SpotDraft'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. Document Security Classification

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

6. 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, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. 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.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

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

Version history

Version	Log	Date
2 Current	Policy version approved by Madhav Bhagat	29 Jul, 2024
2	New Policy version Created	29 Jul, 2024
1	Policy version approved by Madhav Bhagat	02 Aug, 2022
1	New Policy version Created	02 Aug, 2022