Data Classification Policy

Purpose

The purpose of this policy is to define a data classification framework that can be used to determine the sensitivity of <Company Name>'s data and systems, and to provide guidance surrounding the processes of assigning controls to protect the data's security, confidentiality and integrity.

Scope

The policy applies to all data and systems owned or operated by <Company Name>.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

All <Company Name> data is valuable to the organization. However, not all information has an equal value, or requires the same level of protection. Identifying the value of information assets is key to understanding the level of security that is required to protect them. Once the appropriate level of security is identified, relevant controls can be implemented to maintain the security, confidentiality and integrity of the asset. Incorrect classification of assets may result in inadequate or incorrect controls, and inadvertent disclosure or compromise.

Data classification

All company and customer data is classified as per the data classification policy.

<Company Name> classifies its data in four different categories: Customer Confidential, <Company Name> Restricted, <Company Name> Confidential, and Public.<Company Name>'s systems are then classified based on the classification of the data stored within them. If more than one class of data is stored on a system, the highest class determines the system's classification. The system classification is used to assign controls to each system.

Customer Confidential

Customer Confidential is the highest level of data classification, and information classified as such is protected with the strictest safeguards against unauthorized disclosure or modification. The confidentiality of this data is typically required by law or customer/partner agreements, and access to it must be severely limited and based only on a clear business need.

By default, customer data belongs in this classification. Customer data is defined as data that <Company Name>'s customers would consider themselves owners of, and would regard as their own confidential data. Typically, this data has either been sent to <Company Name> for storing or processing, or has been created as a result of using <Company Name>'s products.

Examples include:

- Operational customer data
- Personally Identifiable Information (PII) belonging to <Company Name>'s customers
- Data subject to a confidentiality agreement with a customer, such as intellectual property or confidential communication
- Regulated data, such as electronic personal health information (ePHI)
- Credentials that can be used to access Customer Confidential data

Compromising data that falls within this classification could expose the company to legal action. In addition, any exposure of such data could adversely affect <Company Name> customers and partners, and as a result severely damage the company's reputation, competitive advantage, and industry confidence.

Control applicability varies by the specific type of the system, but Customer Confidential systems (sometimes referred to as "sensitive systems" in control language) require all available data protection controls.

<Company Name> Restricted

<Company Name> Restricted data is internal to the company, and it is used to operate its business. Very few people in <Company Name> have access to <Company Name> Restricted data.

Examples include:

- Sensitive internal communication not intended for all employees, such as emails and confidential documents
- Legal documents and contractual agreements
- Employee PII
- Customer PII, further detailed below
- Private employee records, such as compensation details and performance reviews
- Customer support cases, as long as they don't contain Customer Confidential data, whether directly embedded or as attachments
- Sensitive company intellectual property (IP)
- Credentials that can be used to access Customer Confidential data

As mentioned above, some limited customer PII can be classified as <Company Name> Restricted. Examples includes:

- Business contact information
- Sales leads and opportunities
- Confidential communication around establishing and maintaining the relationship between <Company Name> and its customers

Exposure of <Company Name> Restricted data can adversely affect <Company Name> and can result in adverse effects such as erosion of employee trust and ceding critical information beneficial to competitors. Significant exposure of employee PII could pose a legal risk.

Access to <Company Name>Restricted data should be restricted to a limited set of employees based on their role (such as Human Resources or Legal), seniority (executives), or other similar business need.

<Company Name> **Confidential**

<Company Name> Confidential data is data internal to the company that is used to operate the business. Many people in the company have access to this data.

Examples include:

- Data in common messaging channels
- All-hands quarterly presentations
- Company policies
- Documents shared with everyone on the company's domain
- Intellectual Property, such as source code, which is not of significant competitive advantage

Access to some <Company Name> data and documents may be restricted, but its internal disclosure will not have any adverse impact. Examples in this category are product and engineering design documents, and product analytics data.

<Company Name> Confidential data is intended to stay private and confidential to<Company Name>, and should not be made public. Exposure of information within this classification could result in ceding critical information beneficial to competitors, as well as erosion of employee trust.

Public

Public information may be disclosed to any entity or person within or outside of the company. The data may be available through a public website, and does not have confidentiality requirements.

Data owned by <Company Name> is private by default, as are the information systems storing that data. As such, most company data and systems are not classified as Public. Making data public requires an explicit authorization and publishing step by the owner of the data or the system storing it.

As is true for any data associated with or produced by <Company Name>, the integrity of public data is an important factor that can affect the company's reputation and brand. For example, a press release must be thoroughly vetted by <Company Name> leadership, and open source software must be properly licensed and vetted by qualified engineers to be of sufficient quality.

Examples of public data include:

- Press releases
- Sales messaging and advertising
- Reports and ebooks intended for public distribution
- Software released under an open source license

Due to <Company Name>'s need to control and vet any publicly-available information in order to ensure its integrity, any systems hosting public data must themselves not be public. Such systems must be protected using adequate safeguards, such as strong authentication and limited access.

Data/System Ownership

All data and systems are required to have a designated owner. Owners are responsible for appropriately classifying their data and systems, as guided by this policy, and in coordination with the policy owner.

Owners are stewards of the data within their purview, and do not legally own it. They are responsible for understanding the nature of the data within their system as well as the security requirements and safeguards associated with it. Owners make decisions about who will have access to the data, including administrative access.