**Global Data Classification Policy**

**DC-DG-03**

**Purpose**

The Global Data Classification Policy enables Walmart associates to protect Walmart Data. Specifically, it establishes classification requirements, and the resulting controls associates must implement for Walmart Data comprising Business Information and Personal Information.

Walmart does not discourage or prohibit associates from speaking with or sharing information with others about the terms and conditions of their own employment. Nothing in this policy should be construed as prohibiting such information sharing.

**Target Audience**

This policy applies to all Walmart associates who define, create, receive, transfer or store Walmart Data, regardless of form or format (e.g., electronic, paper). “Walmart” means Walmart Inc., its subsidiaries, and any operating units in which Walmart Inc. has a majority or controlling interest.

Walmart expects its suppliers, vendors, service providers, and other third parties to uphold our digital trust commitments. Specific requirements for third parties are included in the Walmart Standards for Suppliers and in our legal agreements.

**Definitions**

**Business Data Owner** is defined in the Global Data Governance Policy (DC-DG-01).

**Business Data Steward** is defined in the Global Data Governance Policy (DC-DG-01).

**Business Information** is any information that is not Personal Information.

**Personal Information** is any information that identifies or relates to an identified or identifiable person or personal device, or is linked to or can reasonably be linked to a person or personal device. (A personal device is a device such as a laptop, tablet, or smartphone, which is used primarily by an individual to transmit and receive electronic information.)

**Walmart Data** includes all types of data, in any format, owned, controlled, gathered, or processed by or on behalf of Walmart, such data stored or processed in infrastructure environments and all datasets, new and existing.

**Detailed Requirements**

* 1. **Roles and Responsibilities**

1. Personal Information
   1. Digital Citizenship
      * 1. Digital Citizenship is responsible for the classification of Personal Information according to its sensitivity and in compliance with privacy laws, certification requirements, industry standards and guidance, codes of conduct, and Walmart policies.
   2. Business Data Stewards
      * 1. Either through an approved system or business process, Business Data Stewards are responsible for providing accurate and complete information to Digital Citizenship about the intended purpose of use of all Personal Information, and for providing a complete list of data elements involved in processing to enable Digital Citizenship to determine the classification of Personal Information.
   3. Business Data Owners
      * 1. Business Data Owners are responsible for being aware of the classification Digital Citizenship establishes for Personal Information.
2. Business Information
   1. Digital Citizenship
      * 1. Digital Citizenship is consulted for guidance on the classification for Walmart Data comprising Business Information.
   2. Business Data Stewards
      * 1. Business Data Stewards are responsible for determining data classification and for protecting business data resources in accordance with the Business Data Owners’ classification of the data.
   3. Business Data Owners
      1. Business Data Owners are accountable for determining the classification of data comprising Business Information in accordance with its sensitivity and value to Walmart.
3. Associates:
4. All associates must apply the appropriate controls based on the data classification to manage Walmart Data in accordance with Walmart policies.
5. Associates who manage service providers must ensure those service providers:
   1. Are aware of Walmart’s data classification requirements.
   2. Sign the Walmart Information Security Addendum (ISA) before receiving or handling Walmart Data comprising Personal Information (e.g., Sensitive and/or Highly Sensitive).
   3. **Classifying Walmart Data**
6. Requirements
7. All Walmart Data, whether comprising Personal Information or Business Information, must be classified as Highly Sensitive, Sensitive, or Non-Sensitive.
8. When information includes Walmart Data that could be classified into more than one category, associates must classify the information in accordance with the most sensitive data involved.
9. Non-Sensitive Data
10. Non-Sensitive Data comprises Business Information that would not result in harm to Walmart or individuals were it to be disclosed to an unauthorized party.
11. Non-Sensitive Data only requires a minimum baseline level of security.
12. Personal Information, even if publicly available, is always considered Sensitive or Highly Sensitive, and never Non-Sensitive.

|  |  |
| --- | --- |
| **Examples of Non-Sensitive Data** | |
| Business Information | Publicly available materials, such as published annual reports, news releases, marketing materials, and customer-facing websites |
| Personal Information | N/A |

1. Sensitive Data
2. Sensitive Data may comprise Business Information or Personal Information.
   1. Personal Information is Sensitive if an individual could suffer a low level of harm due to the information being disclosed to an unauthorized party.
   2. Business Information is Sensitive if low or moderate harm to Walmart could occur due to the information being disclosed to an unauthorized party.
   3. Sensitive Data requires a reasonable level of security and confidentiality.

|  |  |
| --- | --- |
| **Examples of Sensitive Data** | |
| Business Information | Internal policies, procedures, and communications (except for corporate policies that are distributed to all associates); routine business plans; organization charts; training materials; and non-highly sensitive Walmart financial data, audit reports or supplier information. This may also include some organizational charts. |
| Personal Information | Individual’s contact information or truncated government issued identifier |

1. Highly Sensitive Data
2. Highly Sensitive Data may comprise Business Information or Personal Information.
   1. Personal Information is Highly Sensitive if an individual could suffer moderate to substantial harm due to the information being disclosed to an unauthorized party.
   2. Business Information is Highly Sensitive if substantial harm to Walmart could occur due to the information being disclosed to an unauthorized party.
   3. Highly Sensitive Data requires the most stringent level of security and confidentiality.

|  |  |
| --- | --- |
| **Examples of Highly Sensitive Data** | |
| Business Information | Strategic corporate or financial plans; proprietary information; audit reports and internal investigations |
| Personal Information | Full government-issued identifiers, full credit or debit card numbers, health and medical information, information related to an individual’s ethnicity or sexual orientation, or biometric information |

**Compliance**

1. Any violation of this Policy may result in disciplinary action up to and including termination and may be referred to the appropriate law enforcement authorities when applicable.

**Contact Information**

For assistance, contact Data Governance at [globaldataGovernance@email.wal-mart.com](mailto:GlobalDataGovernance@email.wal-mart.com)

**Resources**

Supporting references, policies, standards, and processes:

Global Data Governance Policy (DC-DG-01)

[Data Classification Procedure (DC-DG-03-00-01)](https://one.walmart.com/content/uswire/en_us/work1/global-governance/digital-citizenship/access-privacy-risks/data-classification-procedure.html)