**Global Data Classification Procedure**

**Purpose/Overview**

This procedure, in conjunction with the Global Data Classification Policy (DC-DG-03), establishes the processes for classifying and handling Walmart Data that comprise Business Information and Personal Information, and for implementing controls based on the level of data classification.

**Target Audience**

This procedure applies to all Walmart associates who define, create, receive, transfer, or store Walmart Data. “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**

See the Global Data Classification Policy (DC-DG-03) for all defined terms.

**Detailed Requirements**

* 1. **Associate Responsibilities**

1. For a data processing activity that involves a business application or Technical Service Offering (TSO), an associate must initiate a data classification assessment (see the “DCA Process Flow” section at the bottom of this procedure for additional detail):
2. Register the business application or TSO in the Enterprise Application Portfolio Management (APM) portal.
3. Create a record and classify the data in APM by accessing Walmart Service Portal.
4. Complete the data classification assessment within the APM portal.
   1. This process will determine the data classification for data comprising Business Information and Personal Information.
5. If Personal Information is processed:
   1. The data classification assessment automatically triggers an Enterprise Privacy Risk Assessment (EPRA).
   2. The Walmart Information Security Addendum (ISA) is required if a Service Provider will receive or handle the information.
6. Where appropriate, Digital Citizenship may classify data comprising Personal Information differently from the data classification assessment based on considerations other than data sensitivity, such as the volume of data involved.
7. For a data-processing activity that does *not* involve applications or technology, submit a [Know Your Data](https://walmartglobal.service-now.com/wm_sp?id=sc_cat_item&sys_id=8667c542db9af3089b0a9609db961925) request to obtain the data classification from Digital Citizenship.
8. To understand the rationale underlying data classification, review *Data Classification Assessment Guidance* and *Data Classification Examples* below.
9. Use the *Data Classification Controls Matrix* below to apply the controls needed to meet the baseline requirements for handling Walmart Data based on its data classification.
   1. **Business Data Steward Responsibilities**
10. Walmart Data that comprises Business Information and exists outside of a technology application must be classified by the Business Data Steward in accordance with the Global Data Classification Policy (DC-DG-03), this procedure, and the Data Governance Policy (DC-DG-01).
11. If support is needed to determine the data classification for data comprising Business Information, email Digital Citizenship at globaldatagovernance@walmart.com.
    1. **Business Data Owner Responsibilities**
12. The Business Data Owner(s) for each business domain is responsible for updating the Highly Sensitive, Sensitive, and Non-Sensitive data sets listed in the *Data Classification Examples* section below, by contacting the Digital Citizenship team at globaldatagovernance@walmart.com
    1. **Data Classification Assessment Guidance**

|  |  |  |
| --- | --- | --- |
| **Non-Sensitive**  Business information Only | | |
| **Harm Potential** | **Access Restrictions** | **Protection** |
| No harm to **Walmart** if improperly disclosed | No restrictions (available to the public) | No security protection is needed. |
| **Sensitive**  Business Information or Personal Information | | |
| **Harm Potential** | **Access Restrictions** | **Protection** |
| Low to moderate harm to **Walmart** if improperly disclosed  No harm or very low harm to **individuals** if improperly disclosed | Limit access to those who need to know the information to accomplish the responsibilities of their job (i.e., Walmart associates or authorized third parties) | A reasonable level of security is required. This means if information is transmitted outside of the Walmart network, a secure transmission mechanism such as SecureMail or SFTP must be used and the recipient must have signed the Walmart Information Security Addendum (ISA) or have been otherwise approved by Legal to receive the information |
|  |  |  |
| **Highly Sensitive**  Business Information or Personal Information | | |
|  | | |
| **Harm Potential** | **Access Restrictions** | **Protection** |
| Substantial harm to **Walmart** if improperly disclosed   * substantial harm to company reputation or loss of customer trust * loss of proprietary information impacting company competitiveness * regulatory penalties * significant financial loss * substantial operational risk   Moderate to substantial harm to **individuals** if improperly disclosed   * financial harm * Harm to personal reputation, substantial embarrassment, or loss of privacy | Limit access to those who need to know the information to accomplish the responsibilities of their job (i.e., Walmart associates or authorized third parties) | The most stringent level of security is required. This means:   * If information is transmitted outside of the Walmart network, a secure transmission mechanism such as SecureMail or SFTP and the recipient must have signed the Walmart Information Security Addendum (ISA) or have been otherwise approved by Information Security to receive the information * Any information stored or otherwise processed outside of the Walmart network, must be managed by a third party that has signed the Walmart Information Security Addendum (ISA) or has been otherwise approved by Information Security |

* 1. **Data Classification Examples**

1. **Non-Sensitive Data**
   1. **Business Information Examples**

|  |  |  |  |
| --- | --- | --- | --- |
| News releases | Phone Number\* | Business address\* | Walmart brands or entities\* |
| Marketing materials | Job code | IP address\* | Number of employees\* |
| Website postings\* | Company name | Total revenues\* | Facility locations\* |
| Occupation and title | Annual reports\* | Corporate contact information\* | Number of stores and retail square feet\* |

\*Published/publicly available material only

* 1. **Personal Information Examples**

None. All Personal Information, even if publicly available, should not be classified as Non-Sensitive (Sensitive or Highly Sensitive only).

1. **Sensitive Data**
   1. **Business Information Examples**

|  |  |  |  |
| --- | --- | --- | --- |
| Facility maps, plans, or assets | Legal Agreements (e.g., Service Agreements, Statements of Work, NDAs) | Store sales data | Organization charts |
| Internal policies, procedures, or processes (except for corporate policies that are distributed to all associates) | Training materials or internal technical documents | Company sales volume or data by channel or market | Identification of buyers or suppliers |
| Presentations on company department strategy | Operations or business plans | Information about business partners that is not public information | Product sales information by channel or market |
| Presentations containing company or department metrics | Information used to prepare Annual Reports or Financial Reports |  |  |

* 1. **Personal Information Examples**

|  |  |  |  |
| --- | --- | --- | --- |
| Age | Gender | Call logs | Language skills |
| Academic record | Department | Marital status | Number of children |
| Date of Birth | Walmart assigned user ID | Password (hashed/encrypted) | Employee ID Number (e.g., WIN) |
| Individual’s contact information | Truncated government issued identifier | Family member and relative information | Licenses or professional memberships |
| Place of work, title, role, grade, responsibilities, and reporting line | Letters, email, calls, SMS, MMS, Instant Messaging |  |  |

1. **Highly Sensitive Data**
   1. **Business Information Examples**

|  |  |  |  |
| --- | --- | --- | --- |
| Patented or proprietary technology or data | Accounting details or data | Board meeting information | Internal Audit Reports |
| Commercial or real estate valuation data | Information held for enforcement purposes | IT Security information or security data | HIPAA- protected data |
| PCI DSS-protected data | Attorney-client communications | Full or partial track data (e.g., CVV, PIN/PIN Block, or Service Code) |  |
| More than 10 digits of credit or debit card number | Planned or considered M&As, purchases, acquisitions, divestures, sales, or closures | Trade Secrets, financial data, confidential information |  |

* 1. **Personal Information Examples**

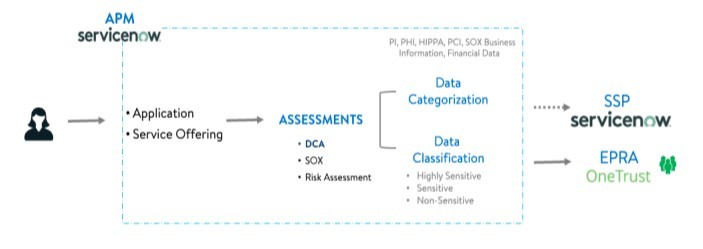
|  |  |  |  |
| --- | --- | --- | --- |
| National ID | Sexual orientation | Racial or ethnic origin | Background checks |
| Full credit or debit card numbers | Criminal convictions and offences | Religious or other beliefs | Health and medical information |
| Full government-issued identifiers | Biometric data (e.g., Imagery of face or fingerprints) | Information related to an individual’s sexual orientation. |  |

* 1. **Data Classification Controls Matrix**

| **Data Handling** | **Non-Sensitive** | **Sensitive** | **Highly Sensitive** |
| --- | --- | --- | --- |
| **Collection** | No restrictions | Collect minimum information required for intended and disclosed business purposes in applicable privacy policies or notices. | Collect minimum information required for intended and disclosed business purposes in applicable privacy policies or notices. Follow Information Security, Data Governance, and Privacy Policies |
| **Use and Handling** | No restrictions | Collect, use, process, access, store only Personal Information or Business Data needed to perform your job. Follow the Information Security, Data Governance, and Privacy and Records Policies. | Collect, use, process, access, and store only the Walmart Data (Personal Information or Business Information) needed to perform your job. Follow the Information Security, Data Governance, and Privacy and Records Policies. |
| **Electronic Transmissions within the Walmart Family of Companies** | No restrictions | Apply appropriate access controls required by Information Security Policies (See Data and Communications Protection Policy (GTPG-15-P) and Identity, Authentication and Access Control Policy (GTPG-18-P) and corresponding standards. | Apply appropriate access controls required by Information Security Policies. Highly Sensitive electronic information must only be transmitted for intended and disclosed business purposes in applicable privacy policies or notices. See Data and Communications Protection Policy (GTPG-15-P) and Identity, Authentication and Access Control Policy (GTPG-18-P) and corresponding standards. |
| **Electronic Transmission outside of the Walmart Family of Companies** | No restrictions | Transmission allowed only under valid contract, which includes an Information Security Addendum or other Terms and Conditions approved by Digital Citizenship Legal. (See Global Data Sharing Policy (DC-DG- 04), Data and Communications Protection Policy (GTPG-15-P), Identity, Authentication and Access Control Policy (GTPG-18-P) and corresponding standards). | Highly Sensitive electronic information must only be transmitted under valid contract, which includes an Information Security Addendum or other Terms and Conditions approved by Digital Citizenship Legal. (See Global Data Sharing Policy (DC-DG- 04), Data and Communications Protection (GTPG-15-P), Identity, Authentication and Access Control Policy (GTPG-18-P) and corresponding standards). |
| **Physical Transmission and Mailing Paper-Based Information** | No restrictions | Transmission to external parties must only occur under a valid contract, which includes an Information Security Addendum or other Terms and Conditions approved by Digital Citizenship Legal. (See Apply controls detailed in Global Data Sharing Policy (DC-DG-04) and Media Protection and Handling Standard (GTPG-02-S-03)). Paper-based information must be in a sealed envelope and sent via Walmart’s mailing services with tracking and delivery confirmation where feasible. | Transmission of Highly Sensitive information to external parties must only occur under a valid contract. (See Global Data Sharing Policy (DC-DG-04) and Media Protection and Handling Standard (GTPG-02-S-03)). Paper-based information must be in a sealed envelope and sent via Walmart’s mailing services with tracking and delivery confirmation where feasible. |
| **Printing by Associates** | No restrictions | Do not leave material on printers. Copies must be destroyed after use or stored in accordance with Records Management Guidelines. | Copies must only be made using equipment provided on Walmart-controlled premises. Do not leave copies unattended on printers. Copies must be destroyed after use or stored in accordance with Records Management Guidelines. |
| **Access Restrictions** | No restrictions | Information must only be accessed by authorized individuals as part of their roles and responsibilities. (See Identity, Authentication and Access Control Policy (GTPG-18-P)). | Highly Sensitive information must only be accessed by authorized individuals as part of their roles and responsibilities. Business Data Owners are responsible for access approval. (See Identity, Authentication and Access Control Policy (GTPG-18-P)). For access control methods see Access Control Standard (GTPG-18-S-02). |
| **Access Control Methods** | Unprotected (access controls still apply) | Apply controls required in the Access Control Standard (GTPG-18-S-02). | Apply controls required in the Access Control Standard (GTPG-18-S-02). Multi-factor authentication is required. |
| **Access Non-Disclosure Agreements** | N/A | All suppliers or contractors accessing Walmart Data must complete a Non-Disclosure Agreement, Information Security Addendum, or other appropriate contract approved by Walmart Legal. | All suppliers or contractors who access Walmart Data must complete a Non-Disclosure Agreement, Information Security Addendum, Business Associate Agreement (when applicable,) or other appropriate contract approved by Walmart Legal. |
| **Subpoenas and Law Enforcement Requests** | Associates may release Walmart Data to law enforcement upon receipt of a subpoena or other appropriate legal document, or where the company is a victim of fraud, but only under the direction of Walmart Legal.  Follow the Information Security, Data Governance, and Privacy and Records Policies. | Associates may release Walmart Data to law enforcement upon receipt of a subpoena or other appropriate legal document, or where Walmart is a victim of fraud, but only under the direction of the Walmart Legal Department.  Follow the Information Security, Data Governance, and Privacy and Records Policies. | Associates may release Walmart Data to law enforcement upon receipt of a subpoena or other appropriate legal document, or where Walmart is a victim of fraud, but only under the direction of the Walmart Legal Department. Follow the Information Security, Data Governance, and Privacy and Records Policies. |
| **Marking and Labelling all Paper and Electronic Documents:** | Label “Non-Sensitive” | Label “Sensitive.” All unlabeled information is to be treated as Sensitive. Additional marking may be required at the direction of Legal counsel. | Label “Highly Sensitive.” Additional marking may be required at the direction of Walmart Legal. |
| **Electronic Storage** | No restrictions | Store in accordance with Media Protection and Handling Standard (GTPG-02-S-03) and Data and Communications Protection Policy (GTPG-15-P). Examples: Walmart managed and monitored servers or approved cloud providers. | Store in accordance with Media Protection and Handling Standard (GTPG-02-S-03) and Data and Communications Protection Policy (GTPG-15-P). Examples: Walmart managed and monitored servers, company devices, corporate file share or database, or approved cloud providers. |
| **Paper Storage** | No restrictions | Secure in a locked desk, cabinet, office, room, or other locked storage area when unattended. If the records retention period has expired, and the material is not subject to a legal hold or preservation directive, then the paper must be shredded.  Always shred the paper if the records contain any form of Personal Information or Sensitive Business Information | Work areas must be clear of Highly Sensitive information when left unattended. Highly Sensitive Information must be kept locked in a desk, cabinet, office, or room. If the retention period has expired and the information is not subject to a legal hold or preservation directive, the paper must no longer be stored. (See “Paper Disposal” below) |
| **Retention** | Follow Records Management policy and guidelines | Follow Records Management Policy and guidelines. | Follow Records Management Policy and guidelines. |
| **Paper Disposal** | Any | Shred or dispose of in a designated confidentiality bin. | Shred or dispose of in designated confidentiality bins. The paper must never be thrown in the trash. |
| **Electronic Disposal** | Any | *See* Global Data Classification Policy (DC-DG-03) & Media Protection and Handling Standard (GTPG-02-S-03). | *See* Global Data Classification Policy (DC-DG-03) & Media Protection and Handling Standard (GTPG-02-S-03). |
| **Data Incident Reporting** | If a data incident is suspected, reporting is required in accordance with the Global Policy for Reporting Data Incidents (DC-PR-03). | If a data incident is suspected, reporting is required in accordance with the Global Policy for Reporting Data Incidents (DC-PR-03). | If a data incident is suspected, reporting is required in accordance with the Global Policy for Reporting Data Incidents (DC-PR-03). |

### **DCA Process Flow**

1. All applications should be registered in APM. For details on how to register your application please visit [wmlink/apm](https://wmlink/apm).
2. As a part of the APM registration process, please complete a DCA.
3. The system will provide an auto population of data category and data classification which will be leveraged to initiate a [SSP reques](https://wmlink/hellossp)t.



**Contact Information**

If further assistance is needed, associates should contact Digital Governance at GlobalDataGovernance@walmart.com

**Resources**

* [Digital Citizenship Policies](https://one.walmart.com/content/uswire/en_us/work1/policies/non-people-policies/data-governance.html) *(Data Governance, Privacy, Incident Response)*
* [Global Tech Policies](https://one.walmart.com/content/uswire/en_us/work1/technology/global-tech/tech-policy-digital-library.html)
* [Enterprise Privacy Risk Assessment (EPRA)](https://one.walmart.com/content/uswire/en_us/work1/global-governance/digital-citizenship/protect-privacy/access-privacy-risks.html)
* [Solution Security Plan (SSP)](https://one.walmart.com/content/uswire/en_us/work1/home-office/information-security0/ssp.html)
* [Know Your Data (KYD) Process](https://one.walmart.com/content/uswire/en_us/work1/global-governance/digital-citizenship/data-policies/data_governance/dg-procedures/dg-pr-01.html)
* [Anything APM Service Request](https://walmartglobal.service-now.com/wm_sp?id=sc_cat_item_guide&sys_id=e5a706c887c3cd102d2433fc3fbb35c3)
* [APM Record Onboarding Process](https://teams.wal-mart.com/sites/GBSConnect/SitePages/APM-Onboarding.aspx)
* [Data Classification Assessment (DCA)](https://walmartglobal.service-now.com/wm_sp/?id=kb_article_view&sys_kb_id=edf1f37b47361dd802996433846d431b)