**Global Policy for Reporting Data Incidents**

**DC-IR-01**

**Purpose**

Walmart is committed to complying with all applicable privacy laws and regulations in the locations where we operate. To support our mission of being the most trusted company and to maintain the trust of our associates and customers, we require reporting and addressing any actual or suspected data incidents in a timely manner.

**Target Audience**

This Policy applies to all Walmart associates who create, receive, transfer, or store Sensitive or Highly Sensitive Data. "Walmart” means Walmart Inc., its subsidiaries, and any operating units in which Walmart Inc. has a majority or controlling interest.

Walmart also expects its suppliers, vendors, service providers, and other third parties to uphold our digital trust commitments. The Walmart Standards for Suppliers as well as Walmart legal agreements include specific requirements for third parties.

**Definitions**

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

**Data Incident** is an actual or suspected unauthorized access, use, disclosure, compromise, or loss of Sensitive and Highly Sensitive Data.

**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 a device such as a laptop, tablet, or smartphone, which is used primarily by an individual to transmit and receive electronic information.

**Detailed Requirements**

**All Associates:**

1. Associates must manage Sensitive and Highly Sensitive Data securely.
2. Associates who become aware of a Data Incident must immediately notify the applicable market-specific reporting channel or the Emergency Operations Center. Associates for Walmart entities not listed in Appendix 1 must report Data Incidents to the Emergency Operations Center. Reporting contact information is listed in Appendix 1.
3. Associates must ensure that any third party that is provided access to Sensitive and Highly Sensitive Data or systems containing Sensitive and Highly Sensitive Data have signed an agreement requiring them to maintain the confidentiality of the information, protect the information, and promptly report any Data Incident to Walmart. These agreements must be approved by the Legal Department
4. Associates who provide government entities with access to Sensitive and Highly Sensitive Data must obtain prior approval from Information Security and the Legal Department.
5. Examples of Data Incidents to report include:
   1. Loss, inappropriate disclosure, or other compromise of Personal Information or Business Information classified as Sensitive or Highly Sensitive
   2. Lost or stolen laptops, computers, or portable devices containing Sensitive and Highly Sensitive Data (e.g., Bring Your Own Device (BYOD) or corporate-owned devices, jump or flash drive, CD, or other portable media device)
   3. Improper access to or use of computer or network resources that process or store Sensitive and Highly Sensitive Data, including access to login credentials
   4. Lost, stolen, misplaced, or improperly disposed (e.g., in a dumpster) paper records or files containing Sensitive and Highly Sensitive Data
6. Once a Data Incident is reported, the market incident response team must review the reported incident in accordance with the local country or market Data Incident Response Plan(s) and the Data Incident Escalation and Internal Communication Protocol. No additional escalation or communication about a Data Incident is required once it is reported through the local country or market data incident reporting channel.
7. Incidents involving bribery, officer misconduct, or falsifying financial records must be reported to both through the appropriate market reporting channel and to Global Ethics.

**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.

**Resources**

|  |  |
| --- | --- |
| Policies: | [Walmart Standards for Suppliers](https://corporate.walmart.com/suppliers/requirements)  [Global Data Classification Policy](https://one.walmart.com/content/uswire/en_us/work1/policies/non-people-policies/data-governance/data-classification-policy--dg-03.html) (DC-DG-03) |

**Appendix 1: Contact Information**

|  |  |
| --- | --- |
|  |  |
| **Global (U.S)** | Emergency Operations Center (EOC) – (479) 277-1001 – Available 24x7  Health & Wellness Field Operations report in the Safety Culture Reporting Tool (SCRT) available at <https://rl6appservers.wal-mart.com/SCRT> |
| **Global Ethics:** | 1-800-WM-ETHIC; [ethics@walmart.com](mailto:ethics@walmart.com); walmartethics.com |
| **Africa** | [databreach@massmart.co.za](mailto:databreach@massmart.co.za) |
| **Canada** | [caprivacy@walmart.com](mailto:caprivacy@walmart.com) |
| **China** | [cndatabreach@walmart.com](mailto:cndatabreach@walmart.com) or contact EOC  沃尔玛中国应急处理中心联络方式  电话： (86) 0755 – 2151 1668  危机事件支持请按“1”;  电邮：应急处理中心（EOC): cneoc@wal-mart.com  Walmart China EOC Contacts  Hotline: (86) 0755 - 2151 1668  For EOC support, please press “1”.  E-mail: EOC: cneoc@wal-mart.com |
| **Chile** | [privachile@walmart.com](mailto:privachile@walmart.com) |
| **CAM** | Email [CAMPRIVA6@email.wal-mart.com](mailto:CAMPRIVA6@email.wal-mart.com) or report it through SharePoint in ENLACE (Intranet): ENLACE/Privacidad de Datos/Denuncia de Fuga de Información. |
| **Flipkart** | [write2infosec@flipkart.com](mailto:write2infosec@flipkart.com) |
| **Global Sourcing** | [ethics.globalsourcing@wal-mart.com](mailto:ethics.globalsourcing@wal-mart.com) |
| **WMT Global Technology Services - India** | [ethicwmgts@wal-mart.com](mailto:ethicwmgts@wal-mart.com) |
| **India** | EOC email ID: indieoc@wal-mart.com or toll free number for India: 1800 103 9594  or InfoSec – India: [ISDSECIN@email.wal-mart.com](mailto:ISDSECIN@email.wal-mart.com) |
| **PhonePe** | [privacy@phonepe.com](mailto:privacy@phonepe.com) |
| **Mexico** | Email: [privacidad@wal-mart.com](mailto:privacidad@wal-mart.com) or Intranet: Pipeline/Es mi Walmart/Privacidad |

*Walmart entities that are not listed here must report Data Incidents to the Emergency Operations Center.*