Global Data Governance Data Access Standard
DC-DG-01-05

Last Updated: January 11, 2024

Purpose/Overview

The Global Data Access Standard defines checks and balances for data access, ensuring protection and security based on the principles of least privilege and 'need to know'.

Target audience

The Global Data Access Standard applies to all 'Structured Walmart Data' and ensures security, accuracy, and local compliance. It allows for market-specific rules within this framework and applies to all associates of Walmart Inc., its subsidiaries, and any operating units in which Walmart Inc. has a majority or controlling interest ("Walmart"). Walmart 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

A. **Production data** refers to the actual data generated, utilized, or stored within the production or live environment of a solution or a system during daily business operations. It encompasses various forms of data collected, processed, and stored as part of operational activities, such as customer or product information, transaction records, logs, sales data, etc. This data drives business decision-making, operational optimization, and trend identification. Given its sensitive and operational nature, production data is subject to stringent InfoSec, Privacy, and Data Governance Compliance controls

B. **Non-production data** refers to data generated, utilized, or stored outside of the production or live environment, typically within the development, testing, staging, and backup environments. Non-production data might be derived from production data; however, it must undergo processes like anonymization or de-identification when it contains Sensitive information. Alternatively, it could be synthetic data generated specifically for non-production purposes. Data in a non-production environment must be treated as production data if it contains Highly Sensitive information and has not been anonymized, de-identified, or replaced with synthetic data. Relevant controls must be applied despite the non-production environment

C. **Highly sensitive** data is defined in the Global Data Classification Policy (DC-DG-03)
D. **Sensitive** data is defined in the Global Data Classification Policy (DC-DG-03)
E. **Non-sensitive** data is defined in the Global Data Classification Policy (DC-DG-03)
F. **Business data owner** is defined in the Global Data Governance Policy (DC-DG-01)
G. **Business data steward** is defined in the Global Data Governance Policy (DC-DG-01)
H. **Technical data steward** is defined in the Global Data Governance Policy (DC-DG-01)
I. **Business unit** is defined in the Global Data Governance Policy (DC-DG-01)
J. **Personal information** is defined in the Global Data Classification Policy (DC-DG-03)
K. **Business information** is any information that is not Personal Information
L. **Structured Walmart data** is defined in the Global Data Governance Policy (DC-DG-01)
M. **Data product** is defined in the Global Data Product Policy (DC-DG-05)

Detailed requirements

General data access requirements

A. Customer and associate data must be managed and protected in accordance with Walmart's core value of respect for the individual
B. All information, whether contained in hard-copy or electronic formats, must be protected appropriately based on data classification
C. Access to data may only be given to associates to accomplish job responsibilities
D. Access to data by vendors and third parties should be limited to the purposes for which they are contracted
E. To avoid conflicts of interest, the requester and approver must always be different associates
F. Business information and personal information, especially sensitive PI, collection, and retention must be based on proper consent and tied to a particular purpose for which it was collected
G. Associates must have a clearly defined business case for collecting and/or maintaining datasets
H. Requests for data access originating from a Walmart legal entity different from the requesting Walmart legal entity must comply with the Global Data Sharing Policy (DC-DG-04)
I. Requests for data access by a third party must comply with the Global Data Sharing Policy (DC-DG-04)

J. Requests for data access for use in a data product must comply with the Global Data Product Policy (DC-DG-05)

K. Data access requests must comply with Market-specific data subject request management protocols and be executed within the permitted SLA

Business data owner (or approved designees) responsibilities

A. The business data owner is responsible for the effective management of data across their business unit, including how data is collected, managed, used, transferred, secured, and accessed. See Global Data Governance Roles and Responsibilities Standard (DC-DG-01-01) for additional information.

   1. The business data owner may delegate the day-to-day responsibility to the Data Steward or other domain stakeholders for managing data access

   2. The business data owner is responsible for approving data access management plan for their business unit

Business data steward (or approved designees) responsibilities

A. The Business Data Steward must classify data as per the Global Data Classification Policy (DC-DG-03)

B. The Business Data Steward is responsible for creating a detailed plan for managing data access that is specific to their business unit. They must seek input and alignment from the relevant Market Privacy SME, Legal, and Data Office (if set up) to ensure that the plan is comprehensive and effective

C. The Business Data Steward must manage access to Sensitive or Highly Sensitive data sets based on the approved data access management plan

D. The Business Data Steward is responsible for updating and maintaining evidence of the list of users who can access their data
    1. For Sensitive data, reviews should occur periodically at the joint discretion of InfoSec and the Global Data Governance team unless regulatory and contractual requirements dictate otherwise
    2. For Highly Sensitive data, reviews should occur every 180 days unless regulatory and contractual requirements dictate otherwise
    3. For Non-Sensitive data, reviews should occur on an as needed basis unless regulatory and contractual requirements dictate otherwise
    4. Data access must be promptly revoked when associates, vendors or contractors exit the organization
    5. Data access for associates or contractors should be re-evaluated and adjusted as necessary when their roles within Walmart change, affecting their data access needs

E. The Business Data Steward may collaborate with technology partners to provision data access after the data access request is granted

Data access request process

The following represents the required process components of data access requests. Each business unit is required to formally process data access requests to ensure accountability and security of the data that is governed in our ecosystem.

A. Data Access requests must provide the following information:
    1. User identity
    2. Manager identity
    3. Purpose/Justification

B. The Business Data Steward must receive all data access requests for data specific to their business unit

C. The Business Data Steward must review the request to ensure “fit for purpose” and that it complies with Global Data Governance, Legal and Privacy policies, including applicable market specific policies

D. The Business Data Steward must have authority (delegated by the Business Data Owner) to approve access to data within their business unit

E. Data access is provisioned if the request is approved by the Business Data Steward

    1. The Technical Data Steward, in collaboration with the Business Data Steward, creates and/or assigns AD Groups accordingly

F. The Business Data Owner has accountability for access to Highly Sensitive data specific to their business unit.

Compliance

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

Resources

Supporting references, policies, standards, and processes:

- **Global Data Governance Policies**
- Global Data Classification Policy (DC-DG-03)
- Global Data Sharing Policy (DC-DG-04)
- Global Data Product Policy (DC-DG-05)
- Global Data Governance Roles and Responsibilities Standard (DC-DG-01-01)

Contact information

If further assistance is needed, contact Data Governance at GlobalDataGovernance@walmart.com.