

Global Email and Messaging Policy (DC-DG-10)

Section 1: Policy Overview

1.1 Purpose

Walmart is committed to creating and managing accurate and complete business Records and Information. This Email and Messaging Policy (“Policy”):

- 1) Defines the approved use of Email and Messaging tools;
- 2) Outlines the requirements for retaining and managing Records and Information within Email and Messaging tools.

This Policy is a part of Walmart’s Records and Information Management program, which includes standards, procedures, and the Global Records and Information Retention Schedule.

1.2 Target Audience

Walmart Inc., its subsidiaries, and any operating units in which Walmart Inc. has a majority or controlling interest (“Walmart”) is required to manage Records and Information from creation through disposal in a manner which complies with the laws and regulations that govern its activities.

All Walmart employees (whether full-time, part-time, or temporary) and business units (hereinafter collectively “Associates”) must comply with all aspects of this Policy and are responsible for the safekeeping of Walmart’s Records and Information under their custody. Walmart also expects suppliers, vendors, service providers, and other third parties who are granted use of Walmart Email or Messaging tools to comply with this Policy when using Walmart Email or Messaging tools in the creation of Walmart Records and Information. Specific requirements may be addressed within applicable contracts and agreements.

Walmart Associates are required to comply with Policy requirements in accordance with an implementation plan established by Records and Information Management Department and the market designee. The implementation plan will be revised and updated as needed as additional systems, tools and processes become available.

Any Associate who violates this policy may be subject to discipline, up to and including termination, in accordance with applicable market Human Resources policies.

Section 2: Detailed Requirements

2.1 What to Know

- 1) This Policy applies to all Walmart Records and Information, regardless of media or format, used in either Email or Messaging tools. “Records and Information” does not include day-to-day communications among associates, or communications relating to informal, ordinary course operations that have no value to Walmart and that would not otherwise require retention in accordance with Walmart policy.
- 2) Use of unapproved Email and Messaging tools to create or transmit Walmart Records and Information, including highly sensitive or sensitive information is prohibited. Definitions for sensitive and highly sensitive information are found in the [Global Data Classification Policy](#).
- 3) Subject to applicable law or legal process, and in accord with Walmart Policy, Walmart may:
 - a) Monitor, retrieve, access, view, analyze, copy, transfer, record, decrypt, disclose, delete, or otherwise process the contents of Email and Messaging communications transmitted or stored on Walmart-controlled systems;
 - b) In connection with an investigation or litigation, and as allowed by local law and Walmart policy, request permission of the Associate to collect and review personal devices to identify and retrieve Records and Information.
- 4) For Associates leaving/exiting Walmart, Email and Messaging accounts will be deleted subject to company policy, Legal Hold, or company investigation;
- 5) All communication tools must complete a Solution Security Plan (SSP) and an Enterprise Privacy Risk Assessment (EPRA) prior to connection to or use with Walmart data.

2.2 What To Do

- 1) Use only approved Email and Messaging tools to communicate Walmart Records and Information, except:
 - a) To report ethics (including the Code of Conduct), compliance, legal, or safety concerns, in which case Associates may use any channel, Walmart-approved or otherwise;
 - b) If there is a cyber-attack or attempted attack, in which case alternative messaging applications may be used to determine whether approved messaging applications have been compromised and how to communicate in the interim;
- 2) Associates who receive Records and Information or communications through non-approved tools must copy the record into a Walmart-approved tool and retain it in accordance with Walmart policy;
- 3) Highly sensitive Records and Information must be communicated only through secure email methods;
- 4) The [Records and Information Management Policy](#) outlines the retention requirements for all Walmart Records and Information, including those in Email and Messaging tools. Associates must

store Records and Information contained in Email or a Messaging tool in the appropriate market-approved digital record repository;

- 5) Emails and Messages subject to a Legal Hold must be retained in accordance with any directions provided by the Legal Department in its Legal Hold instructions;

2.3 Definitions

- 1) **“Email”** is a computer-based application for the exchange of messages between users. Examples include Outlook and Gmail.
- 2) **“Legal Hold”** refers to a directive or notification placed on a Record by the Legal Department based on a determination that it could contain information responsive to current or anticipated litigation, an audit, or an investigation. A Legal Hold can be placed on any type of Records and Information. If placed under Legal Hold, the Record or Information must be retained and cannot be destroyed even if it has met the stated retention period. All Associates are obligated to comply with all instructions within the Legal Hold.
- 3) **“Messaging”** A type of service available on the internet that allows the exchange of written messages with someone else using the service. Examples include Teams, Zoom, and Slack.
- 4) **“Records and Information”** refers to any recorded information created, received, processed, managed, or maintained by associates that provides evidence of decisions, operations, and compliance, and has value requiring its retention for a specific period of time. Records and Information may be in any form or medium such as paper, electronic documents, emails, faxes, voicemails, drawings, graphs, charts, photographs, audio or video recordings, or other form of recorded data, wherever they may exist.

Section 3: Contact Information

For questions about this Policy, please contact Records and Information@walmart.com. For questions about what is appropriate under local law, please contact your local Privacy Compliance or Legal Department.

For further guidance, contact:

- Records and Information Management (Records and Information@walmart.com)
- Global Security (gsatinfo@wal-mart.com)
- Global Compliance Hotline (800) 530-9923

Section 4: Resources

Reference Documents

- [Global Anti-Corruption Policy GEC-02](#)
- [Global Data Classification Policy DC-DG-03](#)
- [Walmart Global Records and Information Management Policy DC-DG-09](#)
- [Security Risk and Compliance Reviews, Solutions Security Plans, Exceptions, and Waivers \[GTPG-17-S-01\]](#)

Walmart Digital Citizenship

- [Walmart Code of Conduct](#)

U.S. Specific Documents

- [Workplace Standards Policy \(US\)](#)
- [Bring Your Own Device Policy \(US\)](#)
- [Walmart Privacy Notice](#)