



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



070.207 E-mail Distribution Lists Policy



**Version 2.9
September 9, 2024**

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

Revision History

Date	Version	Description	Author
09/01/2002	1.0	Effective Date	CHFS IT Policies Team Charter
09/09/2024	2.9	Review Date	CHFS Policy Charter Team
09/09/2024	2.9	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	9/9/2024	Jeremy Rogers	DocuSigned by:  FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or designee)	9/9/2024	Kelvin Brooks	Signed by:  A0F3F24DC182406...

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE	6
3	ROLES AND RESPONSIBILITIES	7
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	7
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD	7
3.4	CHIEF/ DEPUTY CHIEF TECHNOLOGY OFFICER (CTO).....	7
3.5	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.6	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
4	POLICY REQUIREMENTS	8
4.1	GENERAL	8
4.2	REQUESTING A NEW DISTRIBUTION LIST	8
5	POLICY MAINTENANCE RESPONSIBILITY	8
6	POLICY EXCEPTIONS	9
7	POLICY REVIEW CYCLE.....	9
8	POLICY REFERENCES	9

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

1 Policy Definitions

- **Cabinet Level:** Defined by CHFS as the lists sent out with information or alerts pertinent to staff from all organizations within the Cabinet. Use of these lists is restricted to the Office of the Secretary, and the Office Human Resources Management (OHRM).
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law (Kentucky Revised Statute 61.878); Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e., System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Departmental Level:** Defined by CHFS as the distribution lists that are used for communications directed at a single department or office within the Cabinet. A primary and alternate designated owner will be appointed by each Commissioner or Executive Director. This appointee will be responsible for ensuring the proper usage of the list and will periodically review the list for correctness.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Identifiable protected health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Enterprise Identity Management (EIM):** Defined by the Enterprise Identity Management User Guide as the Commonwealth Office of Technology's (COT) solution for identity management for employees and other users in the Commonwealth. EIM is a centralized system designed to standardize account creation, modification, and removal for users in the Commonwealth. EIM manages Active Directory, Email, and Home Folder(s).
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61.931-934 and in accordance with National Institute of Standards and Technology (NIST) 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA). In addition, HIPAA identifies an individual's full name, date of birth, street or email address, biometric data, and other common identifiers as direct PII, not requiring a combined additional field of information.
- **Sensitive Data:** Defined by COT standards as data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: all information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth's proprietary information including but not limited to intellectual property, financial data and more.
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS with final approval and appointment by the Kentucky Personnel Cabinet.
- **User Defined:** Defined by CHFS as the lists may be used to correspond with a group of email users who may or may not be within a single Cabinet organizational unit. These groups are designed around a "business purpose" or "area of interest." Examples include groups such as timekeepers, wireless coordinators, personnel liaisons, EEO Coordinators, etc. These lists must be owned by a Cabinet employee who is a member of the list. The owner will be responsible to oversee the appropriate use of the list and to periodically review the list for accuracy.

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through formal contract such as the System Design/Development Services (SDS) contract or other approved agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of security controls through an e-mail distribution policy. This document establishes the agency's E-mail Distribution Lists Policy to manage risks and provide guidelines for security best practices regarding lists created for information distribution through e-mail.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

Coordination within CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within the CMS, the IRS, and the SSA.

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

3 Roles and Responsibilities

3.1 *Chief Information Security Officer (CISO)*

An individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 *Chief Privacy Officer (CPO)*

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) self-assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach. This position is responsible for adherence to this policy.

3.3 *Security/Privacy Lead*

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for the protection of the Payment Card Industry (PCI), PII, ePHI, FTI and other financially sensitive information to all CHFS staff/personnel. This role, along with the CHFS IS Team, is responsible for adherence to this policy.

3.4 *Chief/ Deputy Chief Technology Officer (CTO)*

This individual makes decisions related to a company's technology. This includes the integration and deployment of new technology, systems management and the overseeing of technical operations personnel. The CTO also works with outside vendors to ensure they meet customer service expectations. This individual is responsible for adherence to this document.

3.5 *CHFS Contract, State, and Vendor Staff/Personnel*

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS information system(s).

3.6 *System Data Owner and System Data Administrators*

Management/lead who works with the application's development team, to document components that are not included in the base server build and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality,

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 General

The process for distribution lists is established and owned by COT. Requests for distribution lists should be submitted to CHFSServiceRequests@ky.gov or via [ServiceNow](#). Once the distribution lists are created, regardless of category, they must have designated owners (i.e., CHFS Employees or contractors) who are responsible for overseeing the appropriate use of the list and periodically reviewing the list for accuracy.

CHFS IS Team recommends that a confidentiality statement be included below the user's signature line on the cabinet, departmental, and user-defined distribution lists as well as individual Email communications. An example of a confidentiality statement would include, but is not limited to:

- This message (including any attachments) contains confidential information intended for a specific individual and purpose and is protected by law. If you are not the intended recipient, you should delete this message, and any disclosure, copying, or distribution of this message, or the taking of any action based on it, by you is strictly prohibited.

4.2 Requesting a New Distribution List

Requests for distribution lists should be submitted to CHFSServiceRequests@ky.gov or via [ServiceNow](#). The following information needs to be included in the request:

1. The name for the distribution list. The name needs to include the Cabinet & Agency name. Example: "**CHFS DCBS DSR Central Intake**"
2. The owners of the distribution list. List a minimum two owners who can request modification to the distribution list.
3. The names of everyone who needs to be members of this distribution list.
4. If the distribution list needs to be restricted, then the names of the users that can send to the distribution list. This is to prevent members from sending/replying to large distribution lists.
5. Whether the distribution list is going to accept emails from external (non ky.gov) users, to allow Gmail/Hotmail/Yahoo and users to be able to reply to this distribution list when sent an email.

5 Policy Maintenance Responsibility

The IS Team is responsible for the maintenance of this policy.

070.207 E-mail Distribution Lists Policy	Current Version: 2.9
070.000 Administrative	Review Date: 09/09/2024

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.2
- CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy
- Enterprise IT Policy: CIO-084- E-mail Review Request Policy
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Service Now
- Social Security Administration (SSA) Security Information