Commonwealth of Kentucky
Cabinet for Health and Family Services

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

070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls

Version 2.1
April 27, 2017

Revision History

Date	Version	Description	Author
3/1/2005	1.0	Effective Date	CHFS OATS Policy Charter Team
4/27/2017	2.1	Revision Date	CHFS OATS Policy Charter Team
4/27/2017	2.1	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	4/27/2017	ROBERT E PUTT	
CHFS Chief Security Officer (or designee)	4/27/2017	DENNIS E. LEBER	

Table of Contents

1 070.203 SECURITY EXCEPTIONS AND EXEMPTIONS TO CHFS OATS POLICIES AND SECURITY CONTROLS 4

1.1 PURPOSE 4
1.2 SCOPE 4
1.3 ROLES AND RESPONSIBILITIES 4
1.3.1 OATS Information Security Department 4
1.3.2 Privacy Lead 4
1.3.3 CHFS Staff & Contractor Employees 5
1.4 MANAGEMENT COMMITMENT 5
1.5 COORDINATION AMONG ORGANIZATIONAL ENTITIES 5
1.6 COMPLIANCE 5

2 POLICY REQUIREMENTS 5

2.1 GENERAL 5
2.2 DEFINITIONS 7

3 POLICY MAINTENANCE RESPONSIBILITY 7

4 EXCEPTIONS 8

5 POLICY REVIEW CYCLE 8

6 REFERENCES 8

1 070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls

Category: 070.000 Administration

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) as part of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes Risk Management process and procedures. This policy document establishes the agency's Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls. This policy provides the procedures, guidance, and documentation required to CHFS Branch Managers and Division Directors to submit requests for exceptions or exemptions to CHFS/OATS regulatory policies, procedure documents and security controls.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, 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, application, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) for exceptions to this policy.

1.3 Roles and Responsibilities

1.3.1 OATS Information Security Department

The individual(s) responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This role is responsible for the adherence of the Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls.

1.3.2 Privacy Lead

The individual(s) responsible for providing security and privacy guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of the Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls in concert with the OATS Information Security (IS) Department.

1.3.3 CHFS Staff & Contractor Employees

Individual(s) must adhere to the Security Exceptions and Exemptions to the CHFS OATS Policies and Security Controls Policy as well as referenced documents that pertain to the agency's applications, application servers, appliances, web servers, operating systems, networking components, and database (server or components) that reside on CHFS/OATS, COT, or third party information systems.

1.4 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and CHFS Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy.

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy.

1.6 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in though state laws and regulations as well as federal guidelines outline in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy framework outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Policy Requirements

2.1 General

The OATS IS Team must approve any deviations from CHFS OATS Policies and Security Controls.

Requests for exceptions to OATS Policies and Security Controls must be completed using the CHFS Security Exception and Exemption to CHFS OATS Policies and Security Controls Request Form. Once completed, this form is sent via email to the OATS Information Security Department at CHFSOATSSECURITY@ky.gov for review. Only forms that have been physically signed and scanned to PDF will be accepted. At a minimum, each request shall have the following information completed by the

requestor:

- Date Required by.
- Type of exception or exemption based on NIST Security Control Families/Other types as defined in the request form.
- Explanation of the Request.
- Business Justification/Reason.
- Explanation of the Mechanisms Used to Mitigate the Risks.
- Risk Mitigation Plan for Compliance (or Risk Analysis/Assessment), as needed/required.

The Security Exception and Exemption form must have each approver's printed name, branch, and division office. This form must then be signed by the applicable Branch Manager(s), the Division Manager(s), CHFS OATS Executive Director(s), CHFS Executive Manager, or equivalents, and the CHFS CIO or his/her designated representative- the Chief Information Security Officer (CISO).

It is recommended for all requests for exceptions or exemptions to CHFS/OATS Policies and Security Controls shall be submitted at least one business week to ensure adequate time is available to research and review the request and obtain the required signatures.

Important Note*: It is recommended exemption requests contain a formal Information Security Risk Assessment (IS RA) that is completed by the requestor. The IS RA would then be approved by the OATS IS Team as the exemption is being considered.*

The OATS IS Team reviews the exception or exemption request; the requester will be notified of the decision to either approve or deny the request. Exceptions or exemptions will be applicable for a maximum of one year. Any exception or exemption exceeding one year must be resubmitted and approved for acceptance. The OATS IS Team will maintain a log of all exceptions requested and granted.

NOTE: Any exception, addition, or modification related to Kentucky Information Technology Standards (KITS), require approval from the Information Technology Standards Committee (ITSC). The exception/exemption must go through the CHFS IT Technical Architecture Committee and approval from the CHFS Technical Officials and Technical Officer (CTO) just be obtained. Representatives from CHFS, COT CISO, and State CIO are on the committee. If such a request is required, the requestor will submit the approved COT ITSC Exception/Addition/Modification Request Form.

Requests that require ITSC approval shall be submitted with at least two (2) business weeks' notice to allow adequate time for consideration, and to obtain the required signatures.

2.2 Definitions

- Application – A software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- Application Server – A component-based product that resides in the middle-tier of a server centric architecture (e.g., IBM WebSphere).
- Appliances - An appliance server is one where all of the required functional components, plus the application software itself, are integrated and configured into a unit and purchased from a single vendor (e.g., IBM DataPower, QRadar).
- Database (server or components) – A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.
- Exception – A person or thing that is excluded (or omitted) from a general statement or does not follow a rule. A case to a rule which does not apply or excluded from (e.g., use of a non-KITS approved product).
    - Exceptions are approved on a case-by-case basis and have a limited duration not to exceed one (1) calendar year.
    - Renewal of exceptions requires a completion of new exception request.
- Exemption – The process of freeing or state of being free from an obligation or liability imposed on others. The act of exempting or state of being exempt. Completely excluded or immune from compliance on a permanent basis (e.g., non-expiring passwords).
    - Exemptions are approved on a case-by-case basis and have a limited duration not to exceed one (1) calendar year.
    - Renewal of exemptions requires a completion of new exception request.
- Network Components – Hardware or software (virtualized) components that perform networking or communication functions, control access, manage incoming or outgoing network traffic, monitor for spam or malicious content (e.g., routers, firewalls, switches, IDS/IPS, web or email gateways, or vendor appliances).
- Operating System – Software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
- Web Server - A computer that runs a Web site. Using the HTTP protocol, the Web server delivers Web pages to browsers as well as other data files to Web-based applications (e.g., Internet Information Server (IIS), or Apache).

3 Policy Maintenance Responsibility

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

4 Exceptions

There are no exceptions to this policy.

5 Policy Review Cycle

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

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0;
- CHFS OATS Policies List
- CHFS OATS Standards List
- CHFS Security Exception and Exemption to CHFS OATS Policies and Security Controls Request Form.
- Commonwealth of Technology (COT) Enterprise IT Policies;
- CMS Information Security Risk Assessment (IS RA) Template;
- COT Enterprise Architecture and Kentucky Information Technology Standards (KITS) Library;
- COT ITSC Exception/Addition/Modification Request Form;
- Enterprise Security Exemption Request, COT-F085
- Health Insurance Portability and Accountability Act of 1996 (HIPAA):
- HIPAA Security Rule § 164.308 (1)(ii)(A)(B);
- Internal Revenue Services (IRS) Publications 1075;
- National institute of Standards and Technology (NIST) Special Publication 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems;
- National institute of Standards and Technology (NIST) Special Publication 800-30, Rev. 1, Guide for Conducting Risk Assessments;
- National institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- National institute of Standards and Technology (NIST) Special Publication 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- Social Security Administration (SSA) Security Information