



Information Technology (IT) Policy



020.301 CHFS Network User Accounts

Version 2.1
April 29, 2016

020.301 CHFS Network User Accounts	Current Version: 2.1
020.300 Administrative Security	Effective Date: 9/2/2002

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS IT Policies Team Charter
4/29/2016	2.1	Revision Date	CHFS IT Policies Team Charter
4/29/2016	2.1	Review Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	4/29/2016	ROBERT PUTT CIO	



020.301 CHFS Network User Accounts	Current Version: 2.1
020.300 Administrative Security	Effective Date: 9/2/2002

Table of Contents

1	020.301 CHFS NETWORK USER ACCOUNTS.....	4
1.1	PURPOSE.....	4
1.2	SCOPE.....	4
1.3	ROLES AND RESPONSIBILITIES.....	4
1.3.1	<i>Security Lead</i>	4
1.3.2	<i>Privacy Lead</i>	4
1.3.3	<i>CHFS Staff</i>	4
1.4	MANAGEMENT COMMITMENT.....	4
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES.....	4
1.6	COMPLIANCE.....	5
2	POLICY REQUIREMENTS.....	5
2.1	GENERAL INFORMATION.....	5
2.2	SUPERVISOR/MANAGEMENT PROCEDURES.....	5
2.2.1	<i>Request and Approval</i>	5
2.2.2	<i>Deletion Request and Approval</i>	5
2.3	NETWORK ACCESS.....	5
2.3.1	<i>Off Shore Access</i>	6
3	POLICY MAINTENANCE RESPONSIBILITY.....	6
4	EXCEPTIONS.....	6
5	POLICY REVIEW CYCLE.....	6
6	REFERENCES.....	7

020.301 CHFS Network User Accounts	Current Version: 2.1
020.300 Administrative Security	Effective Date: 9/2/2002

1 020.301 CHFS Network User Accounts

Category: 020.300 Administrative Security

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Service (OATS) must establish an acceptable level of security controls to be implemented through an incident response and reporting policy. This document establishes the agency's Network User Accounts Policy which help manage risks and lays out guidelines for implementing security best practices in regards to network accounts and access.

1.2 Scope

The scope of this policy applies to all CHFS OATS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. This policy covers the applicable computer and data communication systems owned and administered by CHFS OATS or third party providers under contract with a CHFS agency.

1.3 Roles and Responsibilities

1.3.1 Security Lead

Responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This role is responsible for the adherence of the Network User Accounts Policy Reporting Policy.

1.3.2 Privacy Lead

Responsible to provide the security and privacy guidance of sensitive information to all CHFS information technology (IT) staff. This role is responsible for the adherence of the Network User Accounts Policy alongside the Security Lead.

1.3.3 CHFS Staff

Must adhere to the Information Network User Accounts Policy as well as referenced documents that pertain to user accounts and access.

1.4 Management Commitment

This policy has been approved by OATS Division Directors and the OATS 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 who access their applications or systems. All organizational entities that interact with OATS are subject to follow guidelines outlined within this policy.

020.301 CHFS Network User Accounts	Current Version: 2.1
020.300 Administrative Security	Effective Date: 9/2/2002

1.6 Compliance

CHFS has chosen to adopt the security awareness and principles established in the National Institute of Standards and Technology (NIST), the Internal Revenue Services (IRS), the Social Security Administration (SSA), the Centers for Medicare and Medicaid Services (CMS), as well as other federal and state organizations as the official guidance domain for this policy.

2 Policy Requirements

2.1 General Information

Cabinet for Health and Family Services (CHFS) adheres to Commonwealth Office of Technology (COT) Enterprise Policy: CIO-072 - Identity and Access Management Policy. Creation and maintenance of CHFS Domain accounts for CHFS staff is coordinated through COT.

The immediate supervisor of a new employee is responsible for ensuring that the employee reads all information associated with the Confidentiality Agreement and signs the CHFS-219 upon initial hire and annually thereafter. The immediate supervisor, or designee, is responsible for requesting that an employee's CHFS Domain account be created, modified, or deleted as needed through the Kentucky Online Gateway (KOG).

2.2 Supervisor/Management Procedures

2.2.1 Request and Approval

Supervisors or approved designee must submit a ticket through KOG to request any action (create, modify or delete) for a CHFS Domain account or email account. It is important that the KOG request has been properly approved and all relevant information is provided (office location, direct management, position/roles). Once approved, by management, for submission, the ticket will be input through KOG's Request Application Portal for completion.

2.2.2 Deletion Request and Approval

Supervisors or approved designee, upon an employee's departure from the agency, must immediately submit a deletion request through the KOG Request Application Portal. Any special requirements for access to employees' files should be addressed on the request

2.3 Network Access

Once the user's network account has been set up, as specified and approved by appropriate management, network access can then be requested, if deemed necessary

020.301 CHFS Network User Accounts	Current Version: 2.1
020.300 Administrative Security	Effective Date: 9/2/2002

(i.e. database access, server access, etc.). Users must fill out the appropriate COT forms (F181- Staff Service Request Form and F085- Security Exemption Form) and have it approved by management.

Once forms are completed and required management approval is received, the Agency's IT Services Contact can then submit the access request forms to the Commonwealth Service Desk for (CommonwealthServiceDesk@ky.gov) for completion. Please refer to the COT Forms Page (<http://technology.ky.gov/Pages/cotForms.aspx>) for instructions and more detailed information. For Agency approved contact listing please click here: <https://gotsource.ky.gov/docushare/dsweb/Get/Document-391539/>.

2.3.1 Off Shore Access

Production data is prohibited to be accessed off-shore. All users requesting production data must be located within the United States. This applies to all CHFS OATS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. Production data is still defined as "production data" when located in any environment, other than production, unless obfuscated then it is not considered live production data.

3 Policy Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) IT Security & Compliance Team is responsible for the maintenance of this policy.

4 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS IT Policy: 070.203. For any staff located in the CHFS Secretary's Office who have not yet been on boarded or utilized the KOG system, the COT F181EZ form must be used to request any action (create, modify, or delete) for a CHFS domain account or email account.

Once forms are completed and required management approval is received, the Agency's IT Services Contact can then submit the access request forms to the Commonwealth Service Desk for (CommonwealthServiceDesk@ky.gov) for completion. Please refer to the COT Forms Page (<http://technology.ky.gov/Pages/cotForms.aspx>) for instructions and more detailed information. For Agency approved contact listing please click here: <https://gotsource.ky.gov/docushare/dsweb/Get/Document-391539/>.

5 Policy Review Cycle

Annual

020.301 CHFS Network User Accounts	Current Version: 2.1
020.300 Administrative Security	Effective Date: 9/2/2002

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy:070.203- Exceptions to Standards and Policies Policy
- Commonwealth Office of Technology (COT): Contact Commonwealth Service Desk Webpage
- Enterprise IT Policy: CIO-072- Identity and Access Management Policy
- Enterprise IT Form: F181EZ Form
- Enterprise IT Form: F181EZ Form Instructions
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publications (SP) document 800-30- Risk Management Guide for Information Technology Systems
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Office of Administrative and Technology Service (OATS) Network Access Request Procedure Social Security Administration (SSA) Framework