**Cabinet for Health and Family Services (CHFS) Standards:**

**Category: 5000 Controls Domain**

[**5100**](#a010007) **- Cloud Security Standards**

**Definition:**

Cloud Security Standards consist of a collection of mandatory security measures designed to protect CHFS cloud-based infrastructure, applications, and data. These measures are designed to ensure the confidentiality, integrity, and availability of information and information being processed, stored, and transmitted within the context of cloud computing and deployment models.

**Security Controls Standards:**

All data must be stored and processed in either a FedRAMP moderate-certified government cloud environment or a FedRAMP moderate-certified commercial cloud environment unless the data owner receives a prior approved exception from CHFS Security.

For existing CSPs that preceded the FedRAMP requirement or new CSPs for which a security waiver has been granted, the CSP must implement trusted safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, data, applications, or other computer systems. Many of the security controls required for cloud environments will be the same as on-premise environments, but with emphasis on monitoring and management of the performance of the controls. The following standards may be used in meeting this objective:

* Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) V4
* NIST Special Publication 800-53 Rev. 4 Security and Privacy Controls for Information Systems and Organizations or higher
* SSAE-18 Statement on Standards for Attestation Engagements 18 – SOC 2 Type 1
* SSAE-18 Statement on Standards for Attestation Engagements 18 – SOC 2 Type 2

**Authentication and Authorization Standards:**

Authentication is the mechanism by which a user’s identity is verified. Authorization is the means by which a user is allowed to access and perform approved actions in a system (read, write, modify, delete, administer), and not allow access or functionality that is not approved or required for that user or administrator. The Commonwealth of Kentucky requires a role-based approach, using the principle of least-privilege, to granting user and administrator access. The following standards may be used to meet this objective:

* RFC 6749: The OAuth 2.0 Authorization Framework
* OpenID Connect (OIDC) 1.0
* Security Assertion Markup Language (SAML) 2.0

The Kentucky Online Gateway (KOG) is the Commonwealth of Kentucky’s enterprise identity and access management system and web Single Sign-On (SSO) platform that utilizes an Okta back-end solution. KOG must be leveraged for SSO for all new business applications, including both user authentication and authorization.

**Confidentiality Standards:**

Confidentiality is preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. All application data must be encrypted both in-transit and at rest using an approved method. The following standards may be used in meeting this objective:

* RFC 5246 Transport Layer Security (TLS) at version 1.2 or higher
* FIPS 140-3 Security Requirements for Cryptographic Modules at qualitative level 3 security or higher
* FIPS 197 Advanced Encryption Standard (AES) using 256-bit encryption key length

**Integrity Standards:**

Integrity controls must be implemented to guard against the improper information modification or destruction and include ensuring information non-repudiation and authenticity. The following standards may be used in meeting this objective:

* XML signature (XMLDSig) Version 2.0
* FIPS 180-4 Secure Hash Standard (SHS)
* FIPS 186-4 Digital Signature Standard (DSS)
* RFC 5246 Transport Layer Security (TLS) Version 1.2 or higher

**Identity Management Standards:**

Users must be properly identified before being permitted to access data and applications. A trusted organizational and technical identity management process must be used for registering and authorizing access during identity provisioning, and for managing the authorization and access of individuals or groups of people to applications, systems or networks based on previously authorized access rights throughout the identity lifecycle. Identity management must also provide for deprovisioning of access. The following standards may be used in meeting this objective:

* NIST SP 800-210- General Access Control Guidance for Cloud Systems
* FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors
* Web Services Federation Language (WS-Federation) Version 1.2
* Security Assertion Markup Language (SAML) V2.0
* WS-Trust 1.4
* eXtensible Access Control Markup Language (XACML) Version 3.0
* OpenID Connect 1.0

The Kentucky Online Gateway (KOG) is the Commonwealth of Kentucky’s enterprise identity and access management system and web Single Sign-On (SSO) platform that utilizes an Okta back-end solution. KOG must be leveraged for SSO for all new business applications, including both user authentication and authorization.

**Security Policy Management Standards:**

The cloud solution vendor’s Security Policy Management Standards must clearly define the organization's overall information security program's objectives, scope, and goals, with the objective of creating a solid foundation for implementing an information security program. The following standards may be used in meeting this objective:

* NIST SP 800-100 Information Security Handbook: A Guide for Managers
* NIST Cyber Security Framework (CSF) mapped to NIST 800-53 controls

**Cloud Application Development and Management Standards**

All CSP-developed applications intended for CHFS or KY State resident use (including operational applications, applications under new development, and applications undergoing a major change/modification or upgrade) must follow a trusted Software Development Life Cycle (SDLC) process, utilizing industry-standard methodologies. This process must begin in the initiation phase of the application life cycle, with CSPs for applications being assessed prior to the systems development phase of the SDLC process. Application security controls must be compliant with [CHFS Policies](https://www.chfs.ky.gov/agencies/os/oats/Pages/ITpolicies.aspx) and [CHFS Standards](https://www.chfs.ky.gov/agencies/os/oats/Pages/itstandards.aspx) and are a subset of the overall functional and nonfunctional requirements, which must be simultaneously incorporated into the SDLC process. In addition to the stated compliance requirements, applications must employ resource isolation. The following standards may be used to meet this objective:

* NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software
* NIST Special Publication 800-218 Secure Software Development Framework (SSDF) Version 1.1
* NIST Special Publication 800-190 Application Container Security Guide

**Risk Management Standards**

Risk management standards must be used by the cloud service provider to identify risks, assess risks, identify ways to manage risks, and implement risk control and mitigation efforts according to CHFS strategy. The following standards may be used in meeting this objective:

* NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM)
* NIST Special Publication 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
* FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
* FIPS 200 Minimum Security Requirements for Federal Information and Information Systems

**Regulatory Compliance:**

Regulatory requirements include additional requirements that must be met if the solution or platform will be used to process or store specific categories of information. For all categories of information, the Cloud-vendor’s data center must reside in the continental United States and all data and processing must remain in the continental United States, including for redundancy or disaster recovery purposes. Storage, processing, and access to data must remain restricted to US citizens. All Information as a Service (IaaS) and Platform as a Service (PaaS) application solutions must have both process and memory isolation controls. The categories of information are subject to the applicable regulatory requirements listed below:

* Health Insurance Exchange Information: Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2
* Protected Health Information (PHI):
  + HIPAA Security and Privacy Rule
  + HITRUST CSF v9.6.0
* Federal Tax Information (FTI):
  + IRS Publication 1075
  + This category of information requires the use of a government cloud environment. Commercial cloud environments do not yet meet FTI requirements.
* Social Security Administration Information (SSA):
  + Social Security Administration Technical System Security Requirements (TSSR)
* Personal Identifiable Information (PII):
  + NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  + NIST SP 800-53 Rev 4 Appendix J – Privacy Control Catalog
* Payment Card Information:
  + PCI Data Security Standard Version 4.0

**Commonwealth Office of Technology (COT) Compliance Standards:**

The software deployment and all vendor services shall abide by privacy and security standards as outlined in the Commonwealth’s Enterprise Information Technology Policies. These standards are as follows:

* [Enterprise Security Policies](https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx)
* [Enterprise IT Policies](https://technology.ky.gov/policies-and-procedures/Pages/policies.aspx)

**Security Monitoring Standards:**

The cloud service provider must utilize security monitoring to automatically process, collect, and analyze indicators of potential security threats and violations of policies, and triage these events with appropriate action. The following standards may be used in meeting this objective:

* FedRAMP Continuous Monitoring Strategy Guide Version 3.2
* NIST Special Publication 800-53 Rev. 4 or higher
* NIST 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
* NISTIR 7275 Rev. 4 Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2
* X.1500 Cybersecurity information exchange techniques Edition 1.12
* X.1520 Common vulnerabilities and exposures Edition 2
* X.1521 Common Vulnerability Scoring System Edition 3
* NIST Special Publication 800-126 Rev. 3 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3

**Incident Response Standards:**

Incident Response is the mitigation security incidents to protect data and effectively and quickly recover the operating environment to the pre-incident state of operation. The following standard may be used in meeting this objective:

* NIST Special Publication 800-61 Rev. 2 Computer Security Incident Handling Guide

**Approved Product(s) for New Applications:**

N/A

**Exceptions:**

Any exceptions to this standard must follow the procedures established in CHFS IT Policy #070.203.

**Review Cycle:**

Annually

**Timeline:**

Last reviewed: 02/29/2024

Next review: 02/01/2025

**Cross Reference:**

**Link to all COT Software Domain Standards:**

[KITS\_Report.pdf (ky.gov)](https://cgp.ky.gov/sites/COTPUBDOCS/Standards/KITS_Report.pdf)

**Link to all CHFS IT Standards:**

[CHFS IT Standards - Cabinet for Health and Family Services (ky.gov)](https://chfs.ky.gov/agencies/os/oats/Pages/itstandards.aspx)

**Link to all CHFS IT Policies:**

[CHFS IT Policies - Cabinet for Health and Family Services (ky.gov)](https://chfs.ky.gov/agencies/os/oats/Pages/ITpolicies.aspx)