| | | | |
|---|---|---|---|
| **TITLE**<br>Information Security | | | **IDENTIFICATION NUMBER**<br>A13-070 |
| **ORGANIZATION(S)**<br>University of Kentucky / UK HealthCare | **SITES AFFECTED**<br>X Enterprise<br>☐ Chandler<br>☐ Good Samaritan<br>☐ KCH<br>☐ Ambulatory | **CATEGORY**<br>X Enterprise<br>☐ Nursing<br>☐ Department<br>☐ Guideline<br>☐ Protocol | **REPLACES:**<br>CHANDLER HP01-15 |
| **REVIEW CYCLE** ☐ 1 year X 3 years<br>**REVIEW DATES:** 12/18/2012; 6/1/2015; 12/9/2019; 12/5/2022 | | **EFFECTIVE DATE:** 1/15/2023 | |

## POLICY STATEMENT

The success of UK HealthCare's mission depends in part on the security of its information assets. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by electronic means, shown on film or video, or spoken in conversation. Regardless of form or the means by which it is shared or stored, information has to be appropriately protected. UK HealthCare is committed to protecting the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to it. The objective of UK HealthCare's Information Security Program is to provide a plan of action for securing information, preserving business continuity, minimizing business risks, and maximizing return on investments and business opportunities.

## PURPOSE

The purpose of this policy is to provide managerial direction and support for information security in accordance with business requirements and relevant laws and regulations.

## SCOPE

This policy applies to all individuals who access, use, or control UK HealthCare's information assets. Those individuals covered include, but are not limited to, staff, faculty, students, those working on behalf of UK HealthCare, guests, tenants, visitors, and individuals authorized by affiliated institutions and organizations. Anyone who deliberately violates this policy and other information security policy statements shall be subject to disciplinary action up to and including termination and prosecution under applicable statutes.

## DEFINITIONS

1. Confidentiality – "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

   A loss of confidentiality is the unauthorized disclosure of information.

2. Integrity – "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

   A loss of integrity is the unauthorized modification or destruction of information.

3. Availability – "Ensuring timely and reliable access to and use of information…" [44 U.S.C., Sec. 3542]

A loss of availability is the disruption of access to or use of information or an information system.

## PROCEDURES

*Program Areas*

It is the policy of UK HealthCare to secure its information using methods based on the sensitivity of the information, and the risks to which the information are subject, including the dependence of critical business processes on information and related systems.

The Information Security Program framework, including appropriate policies, standards, guidelines, procedures, templates, and other tools is based on best practices and comprised of the following ten areas. These areas provide the basis for designing UK HealthCare's Information Security Program and safeguards:

1. **Information Risk Management**: Addresses protecting UK HealthCare information and information systems commensurate with sensitivity and risk, including system availability needs. Risk is the net negative impact of the exploitation of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Accordingly, information risk management is a central component of an information security program.
2. **Systems Security:** Defines the steps necessary to provide adequate and effective protection for information systems and information in the areas of systems life cycle security, information systems security plans, threat modeling, information systems hardening, and information systems interoperability security.
3. **Personnel Security Controls:** Reduce risk to information by specifying access determination and control requirements that restrict the access of information to only those individuals who require such access as part of their job. Personnel security also includes security awareness and training requirements to provide all information systems users with appropriate understanding regarding UK HealthCare information security policies and acceptable use requirements for information systems.
4. **Contingency Planning**: Directly supports an organization's goal of continued operations. Contingency planning defines processes and procedures that plan for and execute recovery and restoration of information systems and information that support essential business functions if an event occurs that renders information systems and information unavailable. Contingency planning includes continuity of operations planning, emergency response, crisis management, disaster recovery planning, and information systems backup and restoration.
5. **Threat Management:** Addresses protection of information systems and information by preparing for and responding to information security incidents. This includes malicious code prevention, threat detection, incident handling, and security monitoring and logging.
6. **Physical and Environmental Security Controls:** Shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. This includes measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with the physical environment.
7. **Logical Access Control:** Defines the steps necessary to protect the confidentiality, integrity, and availability of information systems and information against compromise. Logical access control requirements identify the measures needed to verify that all system users are who they say they are and that they are permitted to use the systems and information they are attempting to access. Logical access includes identification, authentication, authorization, and accountability.

8. **Data Protection**: Provides security safeguards for the processing and storing of data. This component outlines the methods to safeguard information, irrespective of medium, in a manner commensurate with the sensitivity and risk of the information stored. Data protection includes requirements in the areas of media protection and encryption.
9. **Compliance:** Measures compliance with information security policies and standards through processes that include, but are not limited to, monitoring and audits. Monitoring is used to improve information security, to assess appropriate use of information technology resources, and to protect those resources from attack. Use of information technology resources constitutes permission to monitor that use. There shall be no expectation of privacy when utilizing information technology resources.
10. **Regulatory:** Addresses reporting security breaches and coordinating responses to government agencies such as the Office for Civil Rights with the Privacy Officer and the Office of Corporate Compliance.

*Roles and Responsibilities*

The IT Governance Committee is responsible for promoting and providing business support for information security initiatives throughout UK HealthCare. This includes:

1. Verifying that information security processes are integrated with strategic and operational planning processes to secure the organization's mission;
2. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of UK HealthCare, and on information systems used or operated by UK HealthCare or by a contractor of UK HealthCare or other organization on behalf of UK HealthCare;
3. Verifying that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of UK HealthCare;
4. Providing senior officials within the organization with the necessary authority to secure operations and assets under their control;
5. Verifying that UK HealthCare has trained personnel to support compliance with information security policies, processes, standards, and guidelines; and
6. Verifying that the Chief Information Officer (CIO), in coordination with the Director of Information Security, reports to IT Governance on the effectiveness of the UK HealthCare Information Security Program, including the progress of remedial actions.

The CIO is responsible for providing oversight of the security strategy and plans for integration of security with business objectives. This includes:

1. Designating a Director of Information Security;
2. Integrating risk management in all activities;
3. Developing and maintaining an information security program;
4. Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;
5. Verifying compliance with applicable information security requirements; and
6. Reporting to IT Governance on the effectiveness of the information security program, including progress of remedial actions.

The Chief Information Security Officer is responsible for developing a security strategy and overseeing the security program and its initiatives. This includes:

1. Heading an office with the mission and resources to ensure compliance with information security requirements;
2. Assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of UK HealthCare;
3. Developing and maintaining risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each information system to ensure compliance with applicable requirements;
4. Facilitating development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
5. Verifying that UK HealthCare personnel, including contractors, receive appropriate information security awareness training;
6. Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
7. Testing and evaluating the effectiveness of information security policies, procedures, and practices;
8. Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices;
9. Developing and implementing procedures for detecting, reporting, and responding to security incidents;
10. Verifying preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of UK HealthCare; and
11. Supporting the CIO in reporting to IT Governance on the effectiveness of the information security program, including progress of remedial actions.

### Approval

| | |
|---|---|
| **Name and Credentials:**<br>Douglas Fee<br>**Title:**<br>Chief Information Security Officer | **Name and Credentials:**<br>Cecilia Page<br>**Title:**<br>Chief Information Officer |
| **Signature** | **Date** |
| **Signature** | **Date** |