Information Security Policy and Standard Lifecycle

Current Version	Compliance Date	Approved Date
1.5	12/31/2018	11/13/2018

1. Purpose

The purpose of the *Information Security Policy and Standard Lifecycle* is to define the approach to the development, approval, and maintenance of Information Security policies, standards and procedures. The elements of University of Oklahoma Health Sciences Center (OUHSC) policies, standards and procedures are as follows:

- Policy Framework Structure
- Policy Directory
- Policy Development, Review, and Revision
- Roles and Responsibilities
- Assistance

2. Policy

OUHSC IT policies, and the principles and procedures within these policies, provide internal explanation of the University and regulatory requirements.

OUHSC IT *policy* consists of principles, procedures, or both, with the following characteristics:

- The policy is proposed for long-term application to OUHSC as a whole or to a broad cross-section of the OUHSC campuses.
- The Information Security policies reflect the intent of the University, but they are NOT configuration settings, detailed process definitions, or detailed operational guidelines.
- An Information Security policy is a concise statement agreed upon by the Information Security Review Board, of information values, protection responsibilities, and organizational commitment to Information Security.
- Policies uphold the mission of the University. They are designed to protect the rights of individuals and the University. At a minimum, they help influence use of technology in ways the University community expects and respects.
- Security policies help ensure that OUHSC complies with relevant legislation, national standards and best practices, and community expectations; assist the University to attain its strategic goals; promote operational efficiency; and mitigate risks to an acceptable level, as deemed by the Information Security Review Board and Dean's Council.

2.1 OUHSC Policy, Procedures and Standards

OUHSC Procedures

Procedures mandate the operational activities. Procedures step through the practical actions required to support the implementation of policy or to assist OUHSC's operations and compliance with external requirements. Procedures may apply to a specific activity or be of more general application.

2.2 OUHSC Standards

Standards provide detailed information and guidance regarding the associated policy. Standards may take the form of checklists and provide detail and context on aspects of an OUHSC policy. They may recommend particular practices or processes; provide illustrative examples of the exercise of judgement in accordance with an OUHSC policy, or list matters that might be taken into account in carrying out an OUHSC activity.

2.3 Policy Directory

The OUHSC Information Security policy directory, managed by OUHSC Information Security, is located at https://it.ouhsc.edu/policies.

2.4 IT Policy Life Cycle Process

The IT policy life cycle process applies to campus-level guidance including policies, standards, and procedures. Standards and procedures required fewer approvals than policies submitted to be added to the IT Policy Directory.

Identification, Planning and Initiation of a Policy, Procedure or Standard by Information Security

a. Identify compelling need for new or updated policy/guidance. Drivers may include new regulatory requirements, technology developments, operational needs, an Information Security event, and identification of current issues or gaps. Request may come from any unit, Department, or Internal Audit.
b. Determine whether the need should be satisfied by a policy, procedure, or standard (See 2.5 IT Policy Criteria Decision Tree)
c. Identify sponsorship, stakeholders, and working group members and their relevant roles
d. Develop high level implementation impact analysis
e. Obtain approval to proceed with draft policy (or procedure, standard)
f. Prioritize and schedule policy work

Development, Review, and Approval Process by Information Security

a. Draft initial policy (procedure, standard)
b. Distribute to a small group of stakeholders for initial review and input
c. Incorporate initial feedback
d. Distribute to a larger group of stakeholders for review and input
e. Post final draft on the IT policy SharePoint site for general feedback
f. Review and, where appropriate, incorporate feedback
g. Present to appropriate governance entity for approval
h. Obtain approval or direction for modification, if needed

Rollout by Information Security

a. Post and announce guidance (policy, standard, procedure)
b. Conduct educational activities
c. Initiate implementation activities (efforts to develop/update standards and procedures may be needed for some new policies)
d. Determine ongoing review cycle (default review cycle is every two years)

Compliance, Review and Maintenance by Information Security

a. Monitor compliance and effectiveness of implemented policy, procedures or standards

b. Review and implement modifications at least every two-year review cycle (last revision and review dates shall be posted on each policy), or sooner if circumstances warrant. The policy owner will generally be responsible for most policy reviews.

Policy Retirement by Information Security

a. As part of the maintenance and review process, policies, standards, and/or procedures may be identified as out-of-date or no longer needed. They will be retired via the applicable processes by which they were approved.

2.5 IT Policy Criteria Decision Tree

An IT Policy Decision Tree flow chart is available as a planning guide and process reminder for policy development working groups. It is based on the process flow described below.

During the **Planning and Initiation** step of the IT policy life cycle process, the need for new or updated guidance may be triggered by various issues such as:

- Laws, regulations, or best practices that require new or updated guidance
- Implementation of IT services or new technologies that require new or updated policies
- Risk assessment, audits, and/or reviews of existing policies/guidance that reveal inconsistencies or gaps
- Operational issues that require clarification of University's or campus's position

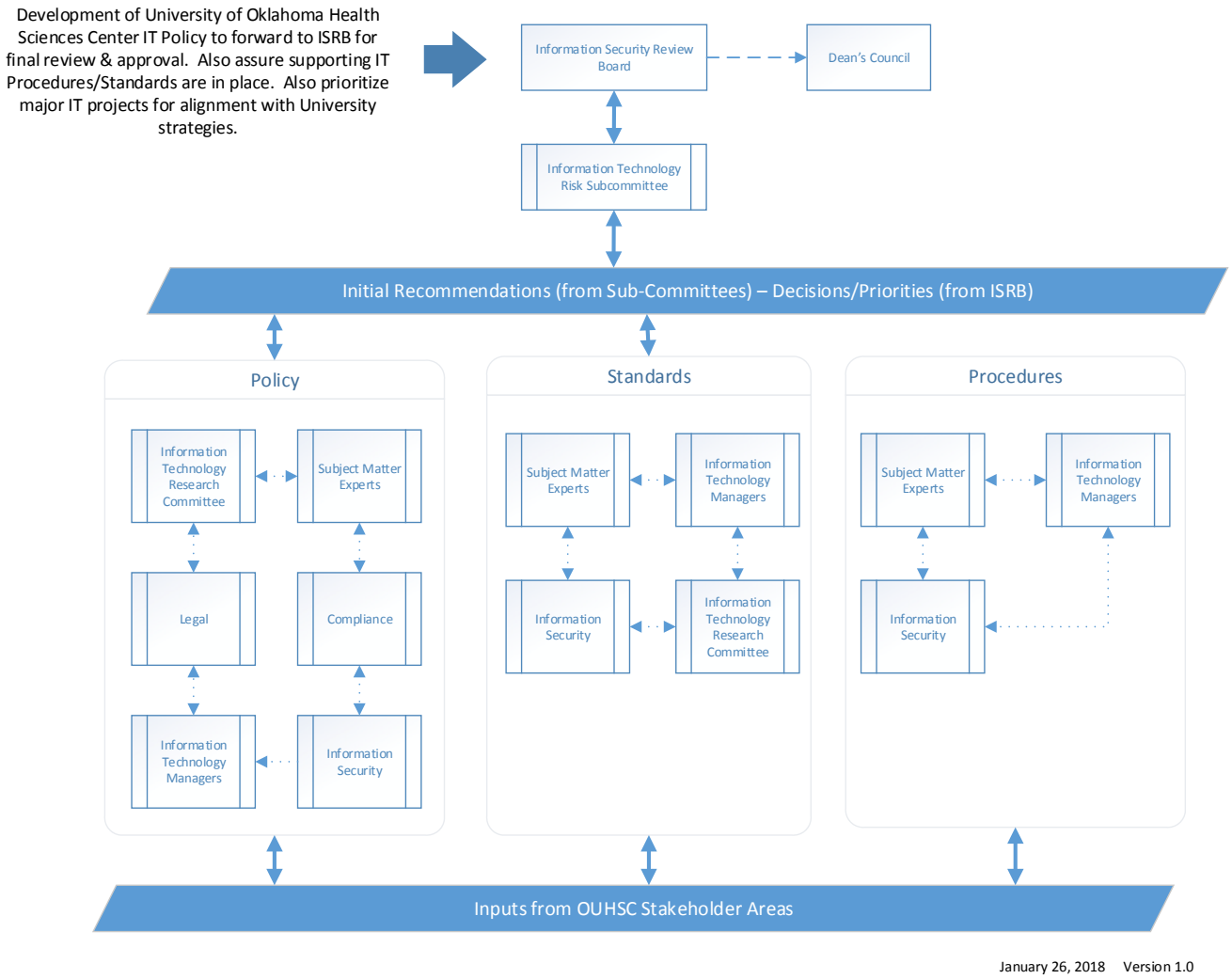
The planning process involves stepping through a list of questions to determine whether there is a compelling need for a guidance effort and, if so, what type of guidance (policy, standard, procedure) needs to be created. Questions and suggestions for relevant decisions are listed below.

1. **What are the consequences/risks of not having documented guidance covering this topic?** If the answer to any of the below is "yes," documented guidance may be necessary.
    a. Is there is a legal requirement to have documented guidance?
    b. Are there operational issues that require clear statement of direction?
    c. Is there new technology (such as cloud computing) that requires University-or campus-wide guidance?
    d. Will documenting (and implementing) this guidance mitigate risks?
2. **What are the consequences/risks of having documented guidance covering this topic?** If the guidance is necessary but not implementable across the University or campus within a reasonable time frame, starting with standards (rather than a policy) is preferable. If there is a contradiction or inconsistency between the proposed standards and existing policies or laws, further analysis is necessary with the participation of appropriate stakeholders to determine how to handle. An existing policy may be obsolete or substantially out-of-date; therefore, updating or retiring the existing policy may be the appropriate option.
    a. Is this guidance implementable?
        1. Is there a technical enforcement mechanism available for this policy?
        2. What are the financial costs for implementing this policy?
        3. Does OUHSC have the necessary staff available to implement this policy?
    b. Does this guidance represent a strategy that OUHSC would like units to plan for, although it may not be currently implementable?
    c. Is there an existing policy that already addresses this topic?
3. **Should this guidance be mandatory? Is it technology-dependent?** If the guidance is mandatory, implementable, and applicable across the University or campus, and technology-independent, it should be stated as a policy. If it is mandatory, implementable, and applicable across the University or campus, but specific to a particular technology, it should be stated as a standard. Another option is to create a combination of a short, high-level policy statement, and a detailed, technology-dependent standard.

a. Is there a federal or state law requiring the University to follow this?
b. Is there a contractual obligation for the University or campus to follow this?
c. Is there another reason why this should be mandatory?
d. Will this change when new technology is implemented? If yes, what part of the guidance is technology-dependent and what part can be stated as a general policy?

4. **Can the essence of this guidance be summarized in no more than one page?**
   Short, high-level policy statements will typically be documented as a policy. More detailed documentation can be provided as standards or procedures. If the guidance cannot be summarized succinctly it may need to be represented as a combination of a policy and standards or procedures.
5. **How often do policies, standards, and procedures need to be reviewed in order to stay current and applicable?**
   Policies should be reviewed every two (2) years at a minimum to ensure that policies continue to meet legal and regulatory obligations and best practices and keep up with technological change. Standards and Procedures should be reviewed every two (2) years at a minimum and must be reviewed when the associated Policy undergoes a change.
6. **Are policy exemptions or exceptions allowed?**
   Exemptions to policies and related guidance are generally not allowed. If an exemption is necessary, then the requesting party must comply with the policy exception process. This process is maintained and coordinated by the Director of Information Security.
7. **What determines whether a policy is University-wide, campus-wide or unit-level?** These questions do not determine the category (policy, standard, procedure) but rather the scope for applicability.
   a. Should this guidance apply University-wide to all users of University information resources?
   b. Should this guidance apply University-wide to all IT providers?
8. **Is this guidance specific to information technology? What other campus domains are involved and who should be included in policy drafting and decision-making?**
   Sometimes, the implementation of an IT service may trigger the need for a policy that relates to multiple domains (HR, student, other), and it may or may not involve IT decisions. It is important to assess this situation with the appropriate stakeholders and determine who should be the primary owner of the policy. There may be cases where an HR or Compliance Office policy, for example, should be implemented and supported by an IT Standard or Procedure (e.g., Preferred Name Policy; Web Privacy Policy or Web Accessibility Policy).

2.6 Policy Governance and Approval



The OUHSC Information Technology governance structure sets campus-wide priorities for IT services, resources, and facilities.

The IT policy function resides with the Chief Information Officer, with delegated responsibilities to Information Security for policy development, coordination, education, and maintenance.

3. Roles and Responsibilities

1. **OUHSC Information Technology Managers** are responsible for the following:
    a. Review and provide feedback for proposed or modified OUHSC policies, standards, or procedures.
2. **OUHSC Information Technology Research Committee (ITRC)** is responsible for the following:
    a. Review and provide feedback for proposed or modified OUHSC policies.
3. **OUHSC Subject Matter Experts** are responsible for the following:
    a. Review and provide feedback for proposed or modified OUHSC policies, standards, or procedures.
4. **OUHSC Legal Office** is responsible for the following:
    a. Review and provide feedback for proposed or modified OUHSC policies.
5. **OUHSC Office of Compliance** is responsible for the following:
    a. Review and provide feedback for proposed or modified OUHSC policies.
6. **Information Security Review Board (ISRB)** is responsible for the following:

a. Review, provide feedback for, and approve/reject proposed or modified OUHSC policies.
b. Determine if OUHSC Information Security policies or standards require the review and approval of Dean's Council.
c. Present OUHSC Information Security policies or standards to Dean's Council when required.

7. **Dean's Council** is responsible for the following:
   a. Review, provide feedback for, and approve/reject proposed or modified OUHSC policies, as determined by the ISRB.
8. **OUHSC Information Security Services** is responsible for the following:
   a. Review and modify policies, standards, or procedures at least every two (2) years, and more often if needed.
   b. Propose new OUHSC Information Security policies or standards based on the applicable triggers.

4. Enforcement

This policy is authorized and approved by the OUHSC's Senior Vice President and Provost and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

5. Scope

This policy is applicable to all OUHSC Information Security policies, standards, and procedures.

6. Regulatory References

- HIPAA 45 CFR 164.308
- HIPAA 45 CFR 164.310
- HIPAA 45 CFR 164.312
- Gramm-Leach-Bliley Act Safeguards Rule
- Payment Card Industry Data Security Standard (PCI DSS)
- U.S. Department of Education, Data Security Checklist
- HITRUST 04.a Information Security Policy Document
- HITRUST 04.b Review of the Information Security Policy
- HITRUST 05.a Management Commitment to Information Security

7. Review Frequency

This policy is scheduled to be reviewed, updated, and modified as necessary every two (2) years.

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	03/15/2017	OUHSC IT	Baseline Version
1.1	03/30/2017	Randy Moore	
1.1	01/26/2018	April Lee	Added decision tree.
1.1	2/22/2018	Randy Moore	Added language regarding technical enforcement of policy.

1.2	02/23/2018	April Lee	Replaced references to guidelines with procedures to support OUHSC's practice.
1.3	03/26/2018	ISRB	Minor revisions.
1.4	09/10/2018	ISRB	Minor revisions.
1.5	09/11/2018	Jill Raines	Minor revisions.

8.2 Approval History

Version	Date	Approved By
1.5	11/13/2018	Information Security Review Board

8.3 Review History

Date	Reviewed By
02/22/2018	Randy Moore, Chad Miller, Jill Raines
03/05/2018	Subject Matter Experts