Security Policies

Table of Contents

✓ **Getting Started**

The initial process in developing an information security policy is to work with appropriate offices across campus to identify which laws, regulations, and information security drivers are applicable to your institution.

1. **Perform** a high level gap analysis of each regulatory requirement and driver that is applicable to determine where policy is needed.
2. **Develop** a prioritized action plan that will help you organize your efforts.
3. **Prepare** a summary document of the impact that the information security policy or policies will have on the institution. The document should:
    a. Describe the policy
    b. Communicate the reason or business justification for the policy, as well as the risks and negative impact of not implementing the policy
    c. Identify regulatory, technical, cultural, and organizational dependencies for implementation of the policy
    d. Identify milestones and possible roadblocks of implementation, compliance, and enforcement
    e. Identify impacted stakeholders
4. **Develop** the policy in collaboration with other key stakeholders at your institution.
5. **Ensure** the policy is vetted by impacted subject matter experts and business owners, including information security, legal counsel, human resources, operational staff, and any other applicable steering committees.
6. **Review** resources in the Guide such as the GRC FAQ, as well as standards and regulations that address specific requirements (e.g., PCI DSS 3.0, HIPAA, GLBA, GDPR).
7. **Publish**, communicate, train, and implement.

Top of page

Overview

⚠ This chapter includes two components. The first is information about the **process of creating information security policies**. The second component is a **listing of sample information security policies** from higher education institutions.

The adoption of one or more information security policies is the first step that institutions of higher education take to express their commitment to the protection of institutional information resources and the information entrusted to them by constituencies and partners. At institutions of higher education, institutional policies, including information security policies, are often drafted through a consensus building process with solicitation and feedback from all identified stakeholders. Once approved and published, its effective communication and periodic reviewing and updating ensures that the policy's stated intent and corresponding expectations are consistent and relevant over time to reflect changes in technology, laws, business practices, and other factors.

Information Security Policy Development

A policy for information security is a formal high-level statement that embodies the institution's course of action regarding the use and safeguarding of institutional information resources. The policy statement should clearly communicate the institution's beliefs, goals, and objectives for information security. It also provides institutional leaders with an opportunity to set a clear plan for information security, describe its role in supporting the missions of the institution, and its commitment to comply with relevant laws and regulations. To be effective an information security policy must:

- Require compliance (i.e., it should be mandatory to the intended audience)
- Be implementable (e.g., impact on legacy systems and current infrastructure)
- Be enforceable. (i.e., failure to comply should result in disciplinary actions)
- Be brief and easy to understand
- Balance protection with productivity

Also, the information security policy should:

- State why the policy is needed (i.e., business reasons, to ensure compliance with laws, regulations, contracts, and/or other policies)
- Express leadership support for the role of information security in the carrying out of the institution's missions,
- Focus on desired behaviors (e.g., acceptable use) and outcomes
- Define roles and responsibilities
- Outline the standards and procedures to be followed.

A careful balance must be reached to ensure that the policy enhances institutional security by providing enough detail that community members understand their expected role and contribution but not so much detail that the institution is exposed to unnecessary risk.

Some elements to be included in information security policies include the following:

- **Policy statement**: Statement of expected behavior, actions, or outcome. The policy statement may also list exclusions (e.g., people or activities that are specifically excluded from the application of the policy).
- **Who the policy applies to**: This section states the people, units, or departments affected by the policy. This section may also list users who are required to follow the policy as part of their job responsibilities.
- **Policy rationale**: The reason for the policy, including any business rationale or legal or regulatory reasons for the policy.
- **Policy definitions**: This section should define any words of art that are used in the policy.
- **Compliance language**: This section states how the institution will enforce the policy.
- **Person responsible**: This section states who is responsible for answering questions about the policy.
- **Related documents**: This section lists any other documents related to the policy, such as standards, guidelines, or procedures, that must be consulted in order to follow the policy.
- **Policy history**: This section lists the revision history of the policy and any substantial changes that have occurred over time.

Information Security Policy Frameworks

There are a number of frameworks that can be used as a foundation for the subject matter included in an institution's information security policy. These frameworks can be used as the basis of one large, overarching information security policy, or for smaller policies devoted to discrete information security topics. Higher education institutions have found success following either model. The Standards box at the end of this page lists a few popular industry frameworks/standards that may be consulted when drafting information security policies. The 2016 EDUCAUSE Core Data Service found that the following information security frameworks/standards are most popular in higher education:

- ISO 27001 (Used by 22% of responding institutions)
- NIST 800-53/FISMA (Used by 20%)
- CIS Critical Security Controls (Used by 18%)

Choosing the right policy framework is all about what will work best for the institution and its missions. Institutions of higher education should consider the following when selecting a framework for their information security policy:

- What works for the institution?
- What has not worked before?
- What fits the institution’s culture?
- What regulatory requirements must be met?
- What are the organizational drivers?
- What future technology is on the institution's roadmap?
- What resources (staff, budget, skill sets) are needed to obtain the desired outcomes?

Top of page

Policy Review and Update Process

Most institutions of higher education will have a documented periodic policy review process in place (e.g., annually) to ensure that ensure that policies are kept up to date and relevant. In some institutions, a policy owner or manager would be the individual who would determine the need for a new policy or the update to an existing policy. In other institutions, the role of policy manager may be played by the Business Owner (e.g., the Chief information Security Officer may be the owner/manager of the information security policy.) We use the term policy manager in this section.

In most instances, the information security policy manager will review and update the policy at the required intervals or when external or internal factors require the review and update of the policy. The following are the most common factors that would prompt a review of the institution's information security policy.

- Changes in Federal or State laws and regulations
- Changes in technology (e.g., increased use of mobile devices on campus)
- Major information security project deployments (e.g., deployment of Mobile device Management (MDM)
- Audit findings
- Policy format changes (e.g., new policy management function and process)
- Increased reliance on third-party service providers (e.g., outsourcing, cloud)
- New business practices (e.g., online education, telecommuting, telemedicine)

The process to review and update the information security policy should include many of the steps identified in the Getting Started section of this chapter. Many institutions have a “policy on policies,” or a process to follow to implement institution-wide policies from inception to maintenance and review. That document may also list steps to follow in order to properly update an institutional policy. At a minimum, the policy manager must:

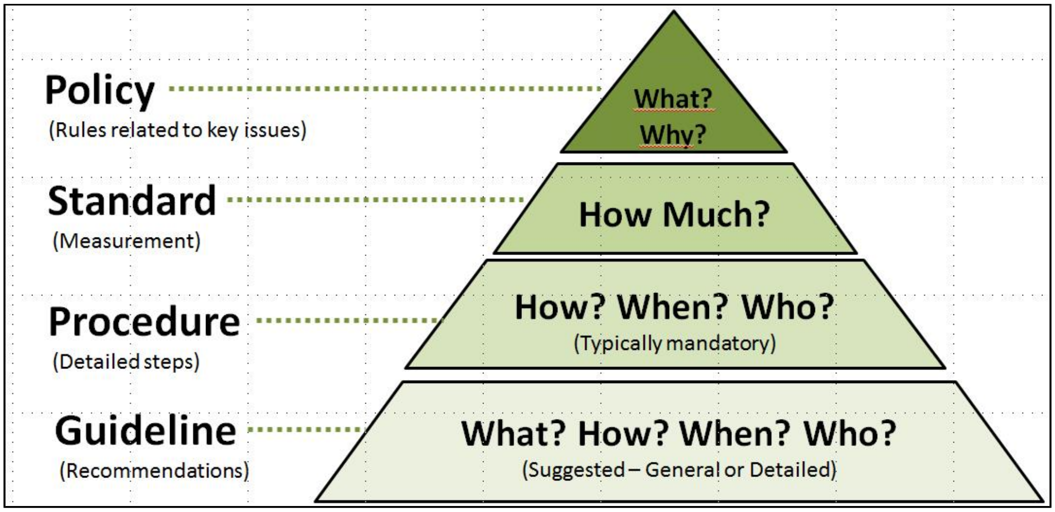
1. Document needed changes
2. Make changes to a draft version of the policy
3. Ensure stakeholder review if necessary. For instance, if the policy changes are significant or alter the intent of the original policy, then the policy manager will want to ensure the changes are vetted by impacted subject matter experts and business owners, information security, legal counsel, human resources if applicable, any other applicable steering committee
4. Publish, communicate, train, and implement according to the institution’s policy management process.

Top of page

Standards, Guidelines, and Procedures

Policies are not the only documents that end users should look to when trying to understand an institution's information security stance. While policies may state the high-level institutional goals around expected information security behaviors and outcomes, other documents may be used to state a threshold of acceptable behavior, step-by-step processes to follow, or recommended (but not required) actions to take. You may see these other types of documents used in an institution's information security program to supplement information security policies. The hierarchy for institutional governance documents is typically:

- **Policies**: The highest level of a governance document. Policies typically have general applicability and they rarely change (or are hard to change). They are leadership's high level statement of information security goals and expectations.
- **Standards**: Standards state the actions needed to meet policy goals. They are more specific than policies and easier to update in response to changing circumstances. Often standards set the minimum level of action needed to comply with a policy.
- **Procedures**: Procedures are often step-by-step checklists that are particular to a task, technology, or department. They are easily updated in response to changing technical or business influences.
- **Guidelines**: Guidelines are documents that specify recommended actions and advice. Institutional employees may not be required to follow guidelines as part of their jobs, but the guidelines are shared in order to promote good information security hygiene practices. Guidelines are flexible and easily updated.



Top of page

Resources

EDUCAUSE Resources

- Sample Information Security Policies, an EDUCAUSE library collection of sample policies from colleges and universities, including policies on privacy, passwords, data classification, security, email, and many more.
- Information Security Policy Examples (*companion page to this chapter on Security Policies*)
- EDUCAUSE Policy
- FERPA
- Gramm-Leach-Bliley Act (GLBA)
- Higher Education Compliance Alliance Matrix
- HIPAA
- ID Theft Red Flags
- PCI DSS
- Policy and Law
- Policy and Law: Campus
- Policy and Law: State
- A Framework for IT Policy Development, an *EDUCAUSE Review* article

Initiatives, Collaborations, & Other Resources

- Higher Education Compliance Alliance
- SANS Information Security Policy Templates (*Note: These templates may need customization for the higher education environment.*)
- Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs (*includes several sample policies*)

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security

27002:2013 Information Security Management **Chapter 5**: Information Security Policies	**800-53**: Recommended Security Controls for Federal Information Systems and Organizations	**APO01.03** **EDM01.01** **EDM01.02**	**Req 12**	**ID.GV-1**	**45 CFR 164.316 (a)** **45 CFR 164.316 (b)**

Top of page

Questions or comments? Contact us.