University of CINCINNATI	**Information Security Policy and Compliance Framework**	
Category: Information Technology	**Effective Date:** 11/21/2016	**Owner:** VP & CIO, UC Information Technologies
Policy applicable for: IT@UC	**Prior Effective Date:** N/A	**Responsible Office(s):** IT@UC Office of Information Security

Background

The University of Cincinnati Information Security Policy and Compliance Framework (Framework) allows for a formal process to develop and review policies that support the confidentiality, integrity, availability, and accountability of university data and critical technology resources. The Framework embraces the university's mission by application of unified information security architecture and by establishing the necessary policies and procedures to secure institutional information and technology resources. The Framework promotes effective data governance and facilitates active engagement of policy sponsors, stakeholders, faculty, staff, and student representatives.

Policy Development and Revision Process

The need for new policy, or revision of existing policy, is driven by one or a number of compelling factors including evolving security threat/vulnerability information, regulatory compliance requirements, technological developments, operational considerations, organizational change or policy expiration.

While the procedural flow for policy development needs to remain agile, there is a core procedural flow for policy creation and development that includes four tiers:

1. IT@UC Office of Information Security (OIS)
2. Information Security & Compliance Committee (IS&CC)
3. Information Technology Council (IT Council)
4. Integrated Decision Making Process (if recommended by IT Council)

At each point in the tiered policy process the decision will be made to:

- Return the draft recommendation to the lower tier for development or revision;
- Redirect the draft recommendation to another committee for additional review and input;
- Escalate the draft recommendation to the next higher tier for additional review and input;

The IT@UC Office of Information Security will initiate or receive the recommendation for new policy or revision of existing policy. After appropriate development/revision, OIS will forward the draft to the IS&CC for input and feedback. Communication regarding the draft will be sent to members of the IT Managers Committee, allowing for the opportunity to provide feedback.

IT Council will determine if the draft: 1) requires additional work by the IS&CC and/or collaboration with appropriate subject matter experts or university entities, 2) can be approved by the IT Council, or 3) requires vetting via the Integrated Decision Making (IDM) process.

The IT@UC Office of Information Security will maintain all information security policies and serve as a central repository for such policies. Any policy or procedure related to an investigatory process will be referred to the Office of General Counsel.

Policy Publication

The policy document, once approved, will be published to the university community at large via the OIS web site.

Policy Support Documentation

To further clarify policy, it may be warranted to use supporting documentation including procedures, standards, and guidelines to fully implement the governing policy statement. The development of new procedures, standards, and guidelines supporting approved policies will be performed by OIS.

Annual Policy Review

Policy review will be conducted by OIS on annual basis and any significant revisions will require appropriate vetting via the Policy Development and Revision Process as explained above.

Definitions

Policy – a high-level management directive that is mandatory and contains basic components including purpose, scope, responsibilities, and compliance.

Procedure – a low-level directive that is mandatory and includes specific step-by-step guides for accomplishing a task.

Standard – describe a specific use of technology that is mandatory and often applied to hardware and software.

Guideline – a recommendation, which is not mandatory, used to support policy, procedures, and standards.

Contact Information:

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History

Issued: 11/21/2016