


| | | |
|---|---|--|
|  <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p> | <p><i>Policy Title:</i> Acceptance of Risk</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 27001/17799, COBIT 4.0, HIPAA, FERPA, GLB</p> | <p><i>Policy Number:</i> 9.1.6</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p> |
|---|---|--|

Background

It is understood that it is not possible to eliminate all business work from an organization. However, for the University of Cincinnati, there exists a legal duty to mitigate risk to a level that is prudent or that would be acceptable to a “reasonable person”.

It is therefore the general policy of UC that all organizations are required to take steps to reduce risk to a level established as best practice.

Where an organization elects not to institute a control or process to reduce the risk any further and they feel that there is still a question as to whether the risk they are going to leave in place is reasonable the associated risk or vulnerability left unaddressed must be clearly communicated and accepted by UC Senior management or their designate.

Policy

- All organizations within the University of Cincinnati are required to follow the best practices for their industry with respect to the mitigation of risk except where there exists a strong business reason to exempt an organization from a particular recommendation or practice.
- Any such Risk Exception must be documented and approved by senior management.
- The approval will be granted or denied via the completion of the Risk Acceptance Form (RAF).
- The RAF must be initially signed by a UC Manager and then forwarded to the Director of Information Security for review and approval/denial or escalation to more senior management.
- UC Information Security is responsible for the maintenance of the Risk Acceptance Form. The form may be obtained from UC Information Security by sending an email to InfoSec@uc.edu or by visiting the InfoSec web site at www.uc.edu/infosec

Audience:

This policy applies to all organizations belonging to the University of Cincinnati.

Definitions:

Prudent: Wise in handling practical matters; exercising good judgment or common sense.

Best Practice: A concept which asserts that there is a technique, method, process, or activity that is more effective at delivering a particular outcome than any other. Descriptions of best practices are normally available from a certifying or regulating authority for an industry.

Risk: A concept that denotes a potential negative impact or something that increases the probability of a loss.

Risk mitigation: Actions taken to reduce the probability that the loss represented by the risk will occur. Mitigation recognizes that the purpose of an organization is to deliver services and goods to their respective customers to meet business goals. It provides for cost/benefit analysis of a mitigating action prior to implementation.

Procedure:

| | |
|------------------------|---|
| ISO 27001/17799 | International Standards Organization for Information Security |
| COBIT 4.0 | ISACA Audit Controls Objective for IT |
| HIPAA | Health Insurance Portability and Accountability Act |
| FERPA | Family Educational Rights and Privacy Act |
| GLB | Gramm-Leach-Bliley Act |

Related links:

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [Health Insurance Portability and Accountability Act](#)
- [The Family Educational Rights and Privacy Act](#)
- [Gramm-Leach-Bliley Act](#)

Phone Contacts:

| | |
|--------------------------------|--------|
| UC Information Security | 8-ISEC |
| Director, Information Security | 6-9177 |
| UC Office of the CIO | 6-2228 |

Disciplinary Actions:

Violation of this policy may result in revocation of network access for the effected system(s). Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants and dismissal for interns and volunteers. Additionally, individuals are subject to loss of University of Cincinnati Information Resources, access privileges, civil, and in some cases criminal prosecution.

Appendix A: Risk Acceptance Process

InfoSec Risk Acceptance Process

