Policy Title: Information Security Design & Architecture Review Policy

Policy Number: 9.1.27

Policy Owner: CIO, IT@UC

Responsible Office(s): Office of Information Security

Background

In order to provide adequate risk assessment of information technology services and equipment the Office of Information Security (OIS) administers an Information Security Service Review (ISSR) to improve secure business processes in the early stage of a project or purchase. The review enforces preventive measures and application of control procedures on the probability of potential threats and vulnerabilities that are likely to occur during the design and architecture phase of a project. It also aligns the security requirements of IT projects, applications, and equipment, ensuring the protection, preservation, and availability of the university’s information.

Policy

All information technology projects and services shall be subject to review by IT@UC OIS prior to implementation. New projects or significant changes to existing infrastructure will necessitate an IT@UC OIS design review.

Security review of existing infrastructure components is implemented through Change Management in which the change requester indicates the necessity for a security review executed prior to the change event.

The Information Security Service Review Form (Appendix A) must be filled out and submitted to OIS for preliminary processing and ISSR number assignment.

The OIS will evaluate and provide a recommendation regarding the equipment or service with related analysis tracked via the ITSR form.
Following approval, project owners shall be required to supply status updates at progressive stages of project development in alignment with security requirements provided by OIS.

Failure to comply with the security requirements could result in termination of the project and/or service.

Suspended project and/or service shall only be recommenced upon compliance with mandated security requirements or with the approval of the CIO.

**Audience:**

This policy applies to all IT@UC divisions, units and departments.

**Definitions:**

**Information Security Service Review:** coordination and assessment of purchases on information technologies projects and services in order to meet specific security requirements to ensure that any intolerable threat will be eliminated.

**Threat:** An action that can cause harm to systems, data or other resources.

**Vulnerability:** A weakness in a system allowing an attacker to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system.

**Procedure:**

<table>
<thead>
<tr>
<th>ISO 27001/17799</th>
<th>International Standards Organization for Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT 4.0</td>
<td>ISACA Audit Controls Objective for IT</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>GLB</td>
<td>Gramm-Leach-Bliley Act</td>
</tr>
</tbody>
</table>
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

Contact Information:
IT@UC Office of Information Security 513-558-ISEC infosec@uc.edu

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 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.

History:
Issued: 11/1/2009
Revised: 5/1/2010
2/13/2015

Appendix A:
See form below.
To be filled in by IT@UC OIS

IT Service Review # 0001
Date Received 1 November 2014
Date Processed

A. CONTACT INFORMATION

Project Name UniverSIS SSNs for the Bursar
Project Owner Jane Smith
Department IT@UC Software Development
Telephone 6-9xxx
E-Mail Address madeup@uc.edu

B. Describe the Project and the proposed architecture if known
(Attach additional information if needed)

The bursar has the need to have bulk transfers of SSNs from UniverSIS to their shared drive.

Universis

BizTalk

Encrypted Space

C. VENDOR INFORMATION

Vendor Name BizTalk and PGP on top of WinOSXXX
Contact Person
Address
City, State, & Zip
<table>
<thead>
<tr>
<th>Telephone</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail Address</td>
<td></td>
</tr>
</tbody>
</table>

*To be filled in by IT@UC OIS*
### Comments/Recommendations:

*This project has sufficient security controls to recommend moving forward. The following controls are those that must stay in place throughout the project:*

- Encryption in sending storage:  Encryption in transit:  Encryption in receiving storage
- Principles of least privilege for who gets access to the data throughout its life cycle
- Adequate logging that tracks who accesses the data

### AGREEMENT:

*I hereby certify that all the information given above is true and correct to the best of my
knowledge. I understand that failure to provide information as requested in this form may result in delays in processing and/or may not be processed.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date (mm/dd/yyyy)</th>
</tr>
</thead>
</table>