University of CINCINNATI	*Policy Title:* **Information Security Review**	*Policy Number:* **9.1.27**
Category: Information Technology **Policy applicable for:** IT@UC	**Effective Date:** 09/26/2019 **Prior Effective Date:** 09/26/2018	**Policy Owner:** VP & CIO, UC Information Technologies **Responsible Office(s):** Office of Information Security

Background

Information security risk assessments (Information Security Reviews) are necessary to identify and document unmitigated risks that may exist on new or existing university information systems or information technology (IT) solutions and provide recommendations to mitigate the identified risk. Information Security Reviews must be performed whenever new IT services or equipment are acquired or when significant changes are made to existing systems, infrastructure or services. An Information Security Review, along with the recommended security controls, work to improve the university's security posture.

Policy

Information Security Reviews must be performed in the following scenarios:

- Implementation of new information services and systems; or significant changes to existing university information services or systems, that may store or transmit Export Controlled or Restricted data (see Data Classification and Data Types for additional information)
- Implementation of new critical infrastructure or significant changes to existing critical infrastructure.
- Implementation of a new enterprise system or significant changes to existing enterprise systems.
- Implementation of new systems or significant changes to existing systems, which permit third party access to university systems or data.
- Implementation of cloud services for the storing or processing of Export Controlled, Restricted or Controlled data.

Note: Please review the Significant Change Assessment form (Appendix A) for assistance in deciding if a change is significant. When in doubt, err in favor of completing a Security Review.

The Office of Information Security (OIS) must perform required Information Security Reviews prior to procurement process initiation, but additional review may be required prior to implementation. Any significant project must have a Security Review incorporated in the project plan. The Information Security Review enforces preventive measures and application of controls to limit 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, equipment and services ensuring reasonable protection of confidentiality, integrity and availability of university data and systems, while simultaneously enabling the university to attain its mission.

The Information Security Review form must be completed and submitted to OIS via the link https://ois-rms.uc.edu/jira/servicedesk/customer/portal/2/create/40 for preliminary review and processing.

Once the Information Security Review Form is received, OIS will evaluate and provide required remediation steps and controls. The remediation steps and controls must be completed by the project owners. Project owners are required to supply status updates during the projects.

Failure to contact OIS or failure to comply with the security requirements will result in termination of the project or service. Suspended projects or services will only be recommenced upon compliance with mandated security requirements.

After the Information Security Review has been completed, projects must follow the university Change Management process.

Contact Information

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

Related Links

Data Classification and Data Types
Information Security Review Process
https://ois-rms.uc.edu/jira/servicedesk/customer/portal/2/create/40
Appendix A: Significant Change Assessment

History

Issued: 11/01/2009
Revised: 05/01/2010
Reviewed: 02/13/2015
Revised: 02/12/2016
Revised: 04/07/2017
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019
Revised: 01/8/2021

Appendix A: Significant Change Assessment

Use the matrix below for assistance in calculating if a Security Review is required. Assess each Risk Attribute and give it a value of 1 to 4, place that value in the total column. Add the total column, if the total is greater than 7 then a Security Review is required.

Risk Attribute	4	3	2	1	Total
Dependencies	Change cannot be reversed	Requires extended hours to reverse	Moderate time to reverse	Easily reversed	
Impact to System	Affects all platforms or servers	Affects multiple systems	Affects single platform or server	very limited impact	
Criticality level	Major system(s)	Critical components	Moderately-critical components	None	
Users Affected by Change	Entire organization	One or more colleges	Select departments, units or groups	Individual or small group	
Data Type	Export Controlled data	Restricted data	Controlled data	Public data	

Significance Level	
13+	High
8 to 12	Moderate
0 to 7	Low

Total