University of CINCINNATI	*Policy Title:* **Information Security Review**	*Policy Number:* **9.1.27**
Category: Information Technology **Policy applicable for:** Faculty/Staff/Affiliates	**Effective Date:** 07/21/2023 **Prior Effective Date:** 06/24/2021	**Policy Owner:** VP & CIO, Digital Technology Solutions **Responsible Office(s):** Office of Information Security

Background

Information security risk assessments (Information Security Reviews) are necessary to identify and document information security risk that may exist related to 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 for a variety of scenarios which are identified below. 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 IT services or systems; or significant changes to existing university IT services or systems, including critical infrastructure, enterprise systems, systems that integrate with critical infrastructure, enterprise systems, or systems that process, transmit, or store Controlled, Restricted, or Regulated data.
- Implementation of new IT services or systems; or significant changes to existing systems, which permit third party access to university systems or data.
- Implementation or changes to cloud or vendor hosted services for the storing or processing of university data.
- Development of new or significant changes to applications, websites, or databases that will process, transmit, or store Controlled, Restricted, or Regulated data, or that integrate with existing university systems.
- Research projects (will involve engagement with the Office of Research).
- IT related contracts or agreements, including software purchases and licensing.
- Contractor or Professional services where the user/entity will access critical infrastructure, enterprise systems, or systems that process, transmit, or store Controlled, Restricted, or Regulated data.
- Instances where the university is providing services to another organization.
- Proof of Concepts involving technology.

Information Security Reviews may be initiated at:
https://mailuc.sharepoint.com/sites/OIS/SitePages/Information-Security-Review.aspx

Contact Information

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

Related Links

Information Security Review Process
Information Security Review Link
Data Governance & Classification Policy