Standard Title	IT Risk Management Standard
Issue Date	September 17, 2020
Effective Date	September 17, 2020
Last Updated	September 10, 2024
Responsible Office	Office of the Vice President of Information Technology and Chief Information Officer
Contact Information	Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: ocs@kennesaw.edu

Scope:

The IT Risk Management Standard applies to the tracking, management, and remediation of all significant threats to campus IT services. Significant threats are those which are identified by internal and external assessments (both deliberately or identified in the course of another project/task) and follow the process for inclusion described below.

Purpose:

IT Risk Management is a critical component of any information security program, facilitating the identification and reduction of threats by utilizing limited resources in the most effective manner. The IT Risk Management Standard was created to meet the requirements specified in the USG IT Handbook 5.5.2 to establish a uniform process for cataloging the nature of a risk, the level of the risk, the impact and frequency of the risk, the owner of the risk, and the mitigating measures in place to reduce the risk.

Standard

While IT Threats are most often identified through the ongoing vulnerability management projects conducted by the UITS Office of Cybersecurity (OCS) and incident handling investigations, effective IT Risk management necessitates other entry points in which threats are identified. These entry points include (but are not limited to) project management processes, identifying new threats or ineffective mitigation progress, employees identifying previously unknown threats to IT security, IT audit and external assessment outcomes, external notifications regarding threats, and service tickets which escalate to the point of a new IT risk.