Policy Summary

Where appropriate, information security personnel will conduct risk assessments of technologies/processes that are being evaluated and/or used at Georgia State University.

Full Policy Text

Where appropriate, information security personnel will conduct risk assessments of technologies/processes that are being evaluated and/or used at Georgia State University. The purpose of these assessments is to quantify the impact and probability of potential threats and vulnerabilities. Furthermore, information security personnel may recommend which security controls, if any, are commensurate with the risks to which the university would be exposed.

Administration of Policy

Mandating Authority:
Administrative Council

Responsible Office(s):
Information Systems and Technology, 13th floor, Commerce Building, 3-4357

Responsible Executive(s):

Policy History

Approving Body: Administrative Council

Rationale or Purpose

Managing the security risks associated with Georgia State University’s ever changing information technology infrastructure presents an enormous challenge. Although some risks can be assessed and managed locally, there are many that cannot be easily understood and/or controlled. In these situations, information security personnel should perform security reviews to determine the threats, the likelihood of such events taking place, the estimated impact if they were to occur and recommend controls.

Additional Information

Standards
**Threats.** Things that can go wrong or that can ‘attack’ the system. Examples might include fire, system failure or hacking. Threats are present in every system.

**Vulnerabilities.** These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, a hacking vulnerability would be the lack of patches on a computer operating system.

**Controls.** These are the countermeasures for vulnerabilities. There are four types: --Deterrent controls reduce the likelihood of a deliberate attack --Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact --Corrective controls reduce effect of an attack --Detective controls discover attacks and trigger preventative or corrective controls

Policy originally approved and made effective November 2, 2005

**Additional Helpful Resources**