Georgia State University Policy

7.10.06 Information Security Management System

Policy Summary

The University selected the Information technology--Security techniques--Information security management systems--Requirements (ISO 27001) as a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS was a strategic decision which was influenced by the needs and objectives, security requirements, and processes employed at the University. ISMS implementation has been incremental and will continue to be scaled in accordance with University requirements.

Full Policy Text

- **Document Control.** Relevant versions of applicable documents will be available at points of use. When a new procedure, or version of a procedure, is issued for inclusion in the University’s Information Security Management System it will include (at a minimum):
  - A revision level showing the new document(s)/version(s)
  - Point(s) of contact for questions or comments
  - Date of last update or issuance
  - Data classification (if sensitive or confidential)

- **Internal Audit.** Internal audits of the ISMS shall be conducted at planned intervals at least annually or as the need arises (internal audits do not necessarily involve University Auditing and Advisory Services).
  - Personnel who are independent of the current work or project shall perform the internal audits.
  - Auditors shall possess personal attributes to enable them to act in accordance with the principles of auditing and have successfully completed at least 32 hours of formal ISMS training or possess internationally recognized certifications such as the Certified Information Systems Auditor (CISA) or Certified Internal Auditor (CIA).

- **Management Review.** Semiannual meetings will be held and at a minimum the input to the management reviews shall include:
  - Results of ISMS audits and reviews
  - Feedback from interested parties
  - Techniques, products or procedures, which could be used at the University to improve the ISMS’s performance and effectiveness
  - Status of preventive and corrective actions
  - Vulnerabilities or threats not adequately addressed in the previous risk assessments
  - Results from effectiveness measurements
  - Follow-up actions from previous management reviews

- **Records Retention.** Unless specified otherwise, ISMS records will be maintained in the
department or college in which they were produced for a minimum of 30 days.

- **Training.** All relevant personnel shall be made aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

**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**

Information security is not an "IT problem," it is a business issue. Organizations that are within the scope of the University’s ISMS must establish, operate, and continuously ensure the appropriateness of safeguards against security threats. Beyond technology, crucial elements of the ISMS include managed planning, the creation of and adherence to policy/procedures, and properly recorded activities. The University’s ISMS depends on people who, with appropriate training and awareness, are its greatest strength.

**Additional Information**

- Digital Millennium Act
- Family Educational Rights and Privacy Act (FERPA)
- FTC Red Flag rule
- Health Insurance Portability and Accountability Act (HIPAA)
- VISA Payment Card Industry (PCI) Compliance

Policy originally approved by Administrative Council May 4, 2009

**Additional Helpful Resources**