

**History of Related Legal Requirements for University Information Security Management**  
*Appendix D, Information Security Guidelines, Part 1, Campus Programs & Preserving Confidentiality*, Document #6608.

Responsible Office: Administrative Services and Technology  
February 1, 2008

*These statements are managers' informal summaries and are not for legal interpretations.*

The 1974 US Federal Privacy Act (5 USC Sec. 552a) required US agencies to manage their use and disclosure of personal identifying information with public notices and “appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”

The 1974 NYS Freedom of Information Act (FOIL) required NYS agencies, including the University (University Procedure #6601) to manage their use and disclosure of personal information. While its main purpose was to ensure that most classes of agency-maintained information would be released to the public under due process, it also prohibited the release of personal information when that would be an “unwarranted invasion of personal privacy.”

The 1974 US Federal Family Educational Rights and Privacy Act (FERPA) required educational institutions, including the University (University Procedure #6600), to manage their use and disclosure of student personally identifiable information.

The 1984 NYS Personal Privacy Protection required NYS agencies, including the University (University Procedure #6603) to manage their use and disclosure of personal information. Agencies must “establish appropriate administrative, technical and physical safeguards to ensure the security” of most forms of personal information under its “actual or constructive control” irrespective of the physical form or technology used.

The 1996 Health Insurance Portability and Accountability Act (HIPAA) required a wide range of healthcare-related organizations, including the University and several of the Campuses, to manage their use and disclosure of personal information related to health transactions and to meet several security standards of electronically transmitted healthcare records. The HIPAA analysis and implementation process involving each Campus was established by the Chancellor in a memorandum to Campus presidents March 2002.

The 1999 Gramm-Leach-Bliley Act (GLBA) with its associated Federal Trade Commission Safeguards Rule required financial institutions, including the University and all State-operated Campuses, to manage their use and disclosure of personal information related to customers, which for the University includes their financial aid recipients. The Act requires Campuses to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” The regulations went into effect in 2003 and were presented in memorandum to University presidents by University Counsel.

The 2003 New York State Information Security Policy describes nearly 300 practices which are “the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment.” These are mandatory for state agencies and “best practices” for the University. The Policy closely aligns with the international standard for governance of information security, ISO 27001 and the ISO’s related codes of practice, ISO 17799.

In 2004, the University established the Information Security Initiative (ISI) and hired a University Information Security Officer to assist campuses in meeting the requirements of law and the State policy.

In 2005, the payment card industry converged on a single standard, *PCI-DSS* (payment card industry data security standard) that defines 12 standards for securing payment card information and systems and applies to any merchant, including those within the University, that store information when doing transactions with credit and debit cards. Specifically, "PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply." If these standards are not met, the credit card companies and banks can stop services to a specific campus merchant or an entire campus.

The 2005 New York State Information Security Breach and Notification Act required businesses and agencies to make timely notification to citizens regarding any breach of a system containing non-encrypted personal information, such as names with Social Security Numbers and to notify “in the most expedient time possible and without unreasonable delay.”

The 2006 New York State Disposal of Personal Records Law required businesses and agencies use diligence in destroying records containing personal identifying information.

The 1999 updating of the 1987 NYS Governmental Accountability, Audit and Internal Control Acts and the related 2002 University Policy (#7500) and Procedure (#7501) for internal controls and the related 2007 *Standards for Internal Control in New York State Government* issued by the State Comptroller, require information security. The OSC standards states that one of four purposes of internal controls is to “safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud. It further requires an organization-wide security management program” that “includes a comprehensive, high-level assessment of risks to information systems.” It requires a “plan that clearly describes the organization’s security management program and policies and the procedures that support it, including procedures for the secure storage and disposal of sensitive information” and “a structure to implement and manage the security program with security responsibilities clearly defined.” It requires protection of “the organization's equipment, information, documents and other resources that could be wrongfully used, damaged or stolen” by “limiting access to authorized individuals only.”

In 2007, the ISI wrote, with Campus collaboration, a description of the minimal actions required of a Campus information security program that protects the confidentiality of sensitive information. The 13 Actions became the 13 standards in the current Procedure.