Princeton University's Commitment to Information Security

Princeton University has established a comprehensive information security strategy to insure the security, confidentiality and integrity of Princeton University information and to protect such information against unauthorized access.

Information security functions at Princeton are managed by its information security program, which is a well-staffed, well-organized, and well-managed operation designed in part to comply with regulatory mandates and guidelines. The program's responsibilities include: assessing policies and guidelines, assessing/controlling/mitigating risk, threat evaluation, monitoring, coordinating emergency response, and communicating information to Princeton University's executive leadership.

Princeton University incorporates fundamental information security functions to comply with the evolving array of regulatory mandates, which include: Gramm-Leach-Bliley Act, Health Information Portability and Accountability Act, Payment Card Industry Data Security Standard, and FACTA Red Flag Rules.

To ensure compliance with all relevant laws and regulations, the validation of all security functions is integrated into University procedure and is periodically evaluated by the Office of Information Technology, Office of Audit and Compliance, Office of the General Counsel, Risk Management, and the University's external auditors.

Princeton University concerns itself with all facets of information security, including the effective risk management of the technologies it uses. The Information Security Office (ISO) has been developed and tasked with ensuring the confidentiality, integrity, and availability of Princeton University's information. As part of the Office of Information Technology, the ISO posture and assessments address such fundamental practices as: accounts provisioning, accounts administration, access control, identity management, security governance, standards and authoring, security architecture, department security, IT security management, standards compliance, threat and vulnerability analysis, security events monitoring, and cybersecurity incident response.

Princeton University utilizes modern technology solutions to meet these information security goals. Some examples of technologies in use include: anti-virus management software, host intrusion detection, network intrusion detection, firewalls, and vulnerability scanning tools. In addition, the integrity of all such programs are reviewed for their ability to be integrated into University procedures and are routinely evaluated and adjusted, as needed.

Princeton University is committed to providing vigilant, strategic, proactive information security, employing the administrative, technical, and physical safeguards appropriate for a research institution of its size, complexity, and the nature of its activities.