

University at Buffalo Enterprise Information Security Charter

Revision 1.1 (January 26, 2007)

Purpose

This document presents the basis of information security within the University at Buffalo and represents the endorsement of the University's executive management for its importance. It identifies the motivation for information security, describes information security principles and terms, and defines the scope of information security policies and responsibilities of the various security functions.

Applicability

All faculty, staff, students, volunteers and contractors of UB.

All direct affiliates and contract personnel who use any computer-related technology must be aware of the provisions and their requirements related to this charter, as well as the UB Information Security Policies and Computer acceptable use policies.

Charter Owner

Information Security Officer (ISO)

Charter Description

Objective

The University at Buffalo recognizes that information and IT resources and facilities are critical assets. It is the responsibility of all members of the University community to safeguard these assets. The University implements, maintains and monitors a comprehensive enterprise information security policy and compliance program appropriate to:

- The risks of the institution, its operation and mission
- Generally accepted information security practices; and
- Applicable legal and regulatory requirements

The security efforts at UB will be primarily managed by a risk management approach and will be as much as possible, consistent with appropriate standards such as ISO 17799, SUNY and NYS Policies.

Motivation

The University at Buffalo highly values the ability to create knowledge, provide a comprehensive learning environment, openly communicate ideas and share information. The University's information (whether managed on a UB-owned resource or held in trust and managed by a third-party service provider or partner) is an important asset that shall be protected according to its value and the degree of damage that could result from its misuse, unavailability, destruction, unauthorized disclosure or modification. The University at Buffalo is committed to preserving the confidentiality, integrity and availability of all forms of information used and maintained on behalf of faculty, staff, students, volunteers, contractors, research subjects, patients, granting agencies and other affiliated groups and individuals. Improper disclosure or destruction of these assets may result in harm to the operation of the University in support of its mission of teaching and learning, research and community service. As a result, specific procedures are developed to help administer and manage the storage and processing of computer-based information related to the proper conduct of University operations. These procedures address all computer and information management activities including materials derived from these assets such as printed copies that could constitute a threat or risk to the proper activities of the University in such a way that risk is minimized or otherwise accepted by its executive officers.

As a result, specific procedures are developed to help administer and manage the storage and processing of information related to the proper conduct of University operations. These procedures address all electronic (or computer) and non-electronic (or non-computer) information as well as all information management activities that could constitute a threat or risk to the proper activities of the University in such a way that risk is minimized or otherwise accepted by its executive officers.

Principle Goals

Information security is in part a risk management discipline addressing the preservation of information confidentiality, integrity and availability. Information assets are identified, valued, assessed for risk and protected as appropriate to the needs and risks of the University. The information security effort is established via a hierarchical set of policies and procedures that help users and administrators to define and mitigate risks, maintaining a trade-off between information value and cost of risk mitigation. Policies are high-level documents used to put information security principles into practice. Procedures are a series of related activities aimed at achieving a set of objectives in a measurable and repeatable manner. Various processes and technologies are employed to understand threats and implement security controls to protect systems, infrastructure and data.

Operating Principles

- 1 The University continues to honor its commitment to academic freedom.
- 2 Legal, regulatory and contractual requirements are followed by the University at Buffalo.
- 3 The University has a responsibility to be a good Internet network citizen.
- 4 The primary accountability for information security rests with the owners/creators of the information.
- 5 Security breaches must be reported to the UB Security Office with sufficient information to determine the risks and consequences of the breach. In the event of a security breach, the UB Security Office assumes primary oversight responsibility for managing the incident and any required reporting. If the incident has to be turned over to the legal authorities, i.e. FBI, Secret Service. Then management responsibility will be transferred to Legal counsel as appropriate.
- 6 Information security policies, standards, guidelines and procedures are developed to communicate security requirements and guide the selection and implementation of security control measures.
- 7 Personal accountability and responsibility for information security are incorporated in roles and responsibilities that ensure that every individual applies the applicable information security policies, principles, procedures and practices in their daily work-related activities.
- 8 Information security education, training and awareness programs are intended to ensure that users are aware of security threats and concerns and are equipped to apply organizational security policies and principles.
- 9 Not all information has the same security requirements, therefore, information assets are classified according to their importance to the University thus enabling an appropriate level of protection. The University at Buffalo Information Classification policy is used to classify information assets.
- 10 Access is granted to information assets for an individual and for the original intended operational purpose. New uses of previously granted access to data require an explicit new request and consent of the responsible Data Custodian. Providing 3rd party access to those information assets is prohibited without the consent of the Data Custodian.
- 11 Information Security is not a static area. Changes to existing procedures necessary to reflect current technology, new threats and new methods for ensuring secure operations will be implemented as often as necessary.

Scope

This policy is applicable to all data, computer equipment, network or data communications equipment, computer programs, procedures and support software, data storage devices and media. It is intended that information is protected in whatever form, including, but not limited to, printed documents, electronic data, images and the spoken word. Information should be protected while at rest and when it is handled, transmitted or conveyed. IT assets include all devices and hardware/software components of the IT infrastructure, applications and data stores. IT assets include all data, computer equipment, network or data communications equipment, computer programs, procedures

and support software, data storage devices and media. In addition, this policy authorizes the development of standards for personnel activities, incident prevention and reporting and compliance or audit reviews directed by appropriate regulations and commonly accepted business practices.

Roles / Responsibilities **Executive Management**

Executive managers (e.g., Vice Presidents, the Provost, Deans, Vice Provosts and Associate Vice Presidents, Directors and Department Chairs, etc.) are accountable for information security and must ensure compliance with security policies, standards, procedures and practices within their respective areas of responsibility.

Information Security Leadership

The Information Security Officer (ISO) is responsible for ensuring that an appropriate security program and security controls are in existence and in force throughout the enterprise. The ISO of the information security function or his/her designated representative is the officer in charge of developing, maintaining, disseminating and measuring compliance with this policy through the procedures and standards that are generated in response to this commitment. The ISO is responsible for determining methods of implementing and enforcing security policies and for advising the enterprise on security-related issues. The ISO ensures, in particular, that information security awareness is conducted or increased, and security audits are performed and reported regularly. The ISO appoints and manages suitably skilled people to staff information security teams as deemed appropriate. The ISO oversees security planning including both IT service continuity planning and Identity management planning as part of a comprehensive security approach. The ISO will provide a periodic report, at a minimum quarterly, to the President's cabinet on the state of UB Information Security.

Security Policy and Governance

Security risk and policy governance is provided by a multidisciplinary group (Information Security Risk and Policy Committee - ISRP) that reviews, advises and endorses information security policy objectives and strategies. They agree to the roles and responsibilities for information security across the enterprise as defined in specific policies. They visibly promote and provide support for information security initiatives throughout the enterprise. The ISRP is led by the ISO and includes representatives from many academic and academic support units. In addition, two other standing groups are chartered and maintained. One with the University Data Custodians and one focusing on IT security technology. (See charters and membership for these groups)

Individuals

It is the general responsibility of all UB community members to protect UB IT facilities and information resources. They are obligated to follow security related policies, use best practices to protect their IT facilities and university information, follow appropriate regulations, and maintain their security awareness by taking advantage of training and security information. It is the duty of all employees and contractors to report any actions or conditions that appears to violate the spirit of this policy.

Enforcement

To ensure that the importance of this policy is communicated uniformly throughout the organization, the CIO, the Executive Vice President and Provost of the University at Buffalo ratify, at least annually, this policy as it relates to regulatory compliance, legal privacy protection and information protection. ***Violations of this policy will be subject to disciplinary action, up to and including termination of employment or criminal prosecution.***

Changes

1st Edition: January 26, 2007