

---

## UB MODIFICATIONS TO NY STATE INFORMATION SECURITY POLICY

---

**Category:** Information Technology  
**Responsible Office:** Chief Information Officer  
**Responsible Executive:** Chief Information Officer

**Date Established:**  
**Date Last Revised:** 8/12/2011  
**Date Posted to Library:** 9/2/2011

---

### Summary

---

The NY State Information Security Policy sets forth the minimum requirements, responsibilities and accepted behaviors to establish and maintain a secure environment and achieve the State's information security objectives. These modifications adjust the NY State policy for UB's higher education environment.

---

### Policy

---

#### Background

A university environment is inherently open by nature, providing equal access to knowledge, with free exchange of ideas. Ownership of a university IT infrastructure is also more complex than that of other state entities, since departments and individuals within universities purchase IT infrastructure with external funding and develop web content, and students connect personally-owned devices to the university network and post web content. Unlike corporations and many state entities, "rule by edict" is not a realistic governance principle. The SANS Institute <sup>1</sup> (Templeton, 2005) has described the needs of a university environment as follows:

- To provide "...an atmosphere that encourages free exchange of ideas and an unwavering commitment to academic freedom."
- To provide a network infrastructure capable of supporting diverse network demands and expectations
- To protect the infrastructure from unwanted activity and/or restrictions; both internally and externally
- To provide cohesive, comprehensive security policies and procedures that will not become "shelfware", required to have but not used because they are too confusing to follow
- To strive to adhere, insofar as resources will allow, to all legislative requirements

The NY State Information Security Policy, based on ISO17799 standards, developed for state entities but not mandated for SUNY institutions, is a comprehensive information security policy, but requires some modifications to be appropriate for an open network environment like that of a university. The following text lists those modifications.

## POLICY STATEMENT

### *Modifications to NY State Information Security Policy for the University at Buffalo Environment*

#### 1. Part 3. Information Policy (Page 8) *NY State Information Security Policy*

All information, regardless of the form or format, which is created, acquired, or used in support of SE's (state entity's) business activities must only be used for SE business."

*Modification:* Modify "must only be used for SE business."

To "must only be used for SE business and collaborative efforts in research and education."

Rationale: University at Buffalo research faculty and scholars are involved in many research collaborations involving other institutions, and are often required to disseminate the results of externally funded research.

#### 2. Internet and Electronic Mail Acceptable Use (Page 17) *NY State Information Security Policy*

When SE employees connect to the Internet using any SE Internet address designation or send electronic mail using the SE designation, it should be for purposes authorized by SE management.

*Modification:* Strike this statement

Rationale: University at Buffalo faculty do not seek, nor should they, management approval for electronic communications with colleagues and others.

#### 3. External Connections (Page 17) *NY State Information Security Policy*

Because the Internet is inherently insecure, access to the Internet is prohibited from any device that is connected, wired or wireless to any part of a SE network unless specifically authorized by SE ISO. This includes accounts with third party Internet service providers. Users will not use the SE's Internet accounts to establish connections to these third party services, unless authorized to do so by SE management and the security of the connection is reviewed and approved by the SE ISO.

*Modification* Strike this statement

Rationale: The UB [Policy on Securing Network Connected Devices](#) defines responsibilities in connecting devices to the network and supersedes this statement.

#### 4. Security of Email (Page 18) *NY State Information Security Policy*

Users of the SE E-mail system are a visible representative of the state and must use the systems in a legal, professional and responsible manner. Unless prior management approval has been obtained, SE users must not connect to commercial E-mail systems from any SE system or workstation (i.e., AOL, Yahoo, etc.)

*Modification:* Strike this statement

Rationale: Our 28,000+ students are clearly not representatives of the state, and students and faculty frequently use non-UB email services such as AOL, Yahoo, Hotmail, et al. In addition, we are currently migrating student email to Google Apps Education Edition. Replace this section with the UB [Computer and Network Use](#) acceptable use policy.

5. Public Websites Content Approval Process (Page 20)

*NY State Information Security Policy*

The content of each public site must be reviewed according to a process that is defined and approved by the SE.

*Modification:* Strike this statement

Rationale: Our students and faculty are free to post information on UB web servers as long as they comply with UB's [Computer and Network Use](#) acceptable use policy.

6. Remote Access Control (Page 27)

*NY State Information Security Policy*

Working from a remote location must be authorized by SE management and appropriate arrangements made for this activity through written policy and procedure to ensure the work environment at the remote location provides adequate security...

*Modification:* Strike this statement.

Rationale: Our students, faculty, and staff are by the nature of their work and lives nomadic and work from remote locations without SE management approval.

---

## Procedure

---

### Applicability of Policy

This policy applies to all University information technology devices and data regardless of their medium and/or form, and to all those who handle University information (faculty, staff, students, third party contractors, and any others).

### Policy Review and Update

The Chief Information Officer or his designee will periodically review and update this policy as needed. Questions concerning this policy should be directed to the Office of the Associate VP for Information Technology.

### Compliance

Violations of this policy will result in appropriate disciplinary measures in accordance with University policies, applicable collective bargaining agreements, and state and federal laws.

## Contact Information

Information Security Officer  
CIO Office  
517 Capen  
(716) 645-3582

---

## Related Information

---

### University Documents:

Title of Related University Policy, Procedure, or Form linked when possible

[UB Computer and Network Use Policy](#)

[Policy on Securing Network Connected Devices](#)

[UB Password Policy](#)

### Other Documents:

Title of Related External Document Linked when possible

[NY State Information Security Policy](#)

---

<sup>1</sup> Templeton, Carol, "Security in an Open Environment Such as a University," *SANS Institute*, 2005.