U of A Policies and Procedures On-Line (UAPPOL)

Approval Date: June 25, 2010

Information Technology Security Policy

Office of Accountability:	Provost and Vice-President (Academic) Vice-President (Finance and Administration)
Office of Administrative Responsibility:	Vice-Provost and Associate Vice-President (Information Technology)
Approver:	Board of Governors
Scope:	Compliance with University policy extends to all members of the University community.

Overview

The University of Alberta is critically dependent on its **information technology resources** to fulfill its academic and business responsibilities. Breaches or compromises of these resources can negatively affect the University's ability to fulfill these responsibilities and can be damaging to the University's reputation.

Use of the University of Alberta's information technology resources must comply with all applicable laws, University of Alberta policies, procedures, appendices and guidelines.

Purpose

The purpose of this policy is to protect the integrity of the University's information technology resources against threats that include, but are not limited to, unauthorized intrusions, malicious use, and inadvertent compromise.

POLICY

1. GENERAL

Use of University information technology resources is permitted only to authorized **members of the University community**, and other **authorized guests**, who must follow the requirements set out in the Information Technology Use and Management Policy and related procedures. All members of the University community are responsible for the security and protection of information technology resources, including, but not limited to, any networks, computers, software, and data, over which the member has use or control. Use of University information technology resources off campus must comply with the same requirements as on campus use.

2. DATA CLASSIFICATION AND SECURITY

Data protection and safeguards must be implemented in a manner that is commensurate with its value and sensitivity.

3. NETWORK SECURITY

Each faculty, department, and unit is responsible for the activity of its users and for educating users on the proper use of the University of Alberta Campus Network and the Internet. The following may be used to determine whether or not a particular use of the Campus network is appropriate:

a. The faculty, department, and unit, and their **Local Area Network (LAN) administrator** must ensure that no hosts connected to the LAN create malicious or negligent network activity, or adversely affect the Campus Network.

b. It is the faculty's, department's, and unit's responsibility to ensure that all users of the LAN who access the University of Alberta Campus Network or the Internet are identifiable from their network traffic. Network traffic must be traceable to users in the event that the University is required to identify the source of network activity. If this is not possible from some hosts on the LAN, then it is the department’s responsibility to filter or otherwise prevent those hosts from having access to the Campus Network and the Internet.

Access to any wired or wireless network connected information technology resource must be via a logon process identifying and authenticating the user, except where read access is permitted (for example, the library catalog and browsing public University websites), or unprivileged access is normal and appropriate safeguards are in place (for example, an Intranet site or kiosk mode web browser). The mandate of the University’s Campus Area Network is defined in the University Campus Network Policy.

4. PHYSICAL SECURITY

Appropriate controls must be employed to protect physical access to information technology resources, commensurate with the identified level of acceptable risk.

5. DISPOSAL OF ELECTRONIC EQUIPMENT

All electronic equipment must be **sanitized** prior to disposal in accordance with University Information Technology security standards.

6. SECURITY AWARENESS TRAINING

All users of the University information technology resources must undergo security training.

7. INCIDENT RESPONSE

Anyone witnessing or suspecting an information technology security incident and/or unacceptable use of University information technology resources in a manner that contravenes this Policy, is obligated to respond and report in accordance to the Responding to and Reporting of Information Security Breaches Procedure.

Support and assistance can be obtained from IST at 780-492-9400 | ist@ualberta.ca.

Assistance from the Office of the Chief Information Security Officer (CISO) is available through ciso@ualberta.ca.

8. NON-COMPLIANCE AND MISCONDUCT

Non-compliance with this policy constitutes misconduct and may be pursued under the applicable collective agreements, University policy, or law. The University’s actions under this policy will be taken in accordance with the *Ethical Conduct and Safe Disclosure Policy*.

DEFINITIONS

A**n**y definitions listed in the following table apply to this document only with no implied or intended institution-wide use. **[▲ Top]**	
Information technology resources	Information technology resources refer to all hardware, software, and supporting infrastructure owned by, or under the Custodianship of, the University that is used to create, retrieve, manipulate, transfer and store electronic information. This includes (but is not limited to), central and non-centrally supported computers, file systems attached to these computers, operating systems running on these computers, software packages supported by these operating systems, wired and wireless networks, telecommunication and hand-held devices, data stored on or in transit on the above, as well as electronic identities used to identify and authenticate the users of the aforementioned resources.
Members of the University Community	University staff, faculty, students, and other holders of valid CCID.

Authorized guests	Other authorized users of information technology resources may include, but are not limited to, conference attendees, prospective students, and users of University public domain resources.
LAN administrator	Local Area Network (LAN) administrator refers to the person or persons responsible for configuring, installing, maintaining, and supporting the network components of information technology resources for a faculty, department, and unit. In some cases the LAN administrator and the system administrator (as defined in the *Information Technology Use and Management Policy*) will be the same individual.
Sanitized	Proper erasing of any residual data from an electronic storage device.
Information Technology Security Incident	Events where there is suspicion that: • the confidentiality, integrity, and availability of University data has been compromised • information and information technology resources are used for, or violated by, illegal or criminal activity • information technology resources has been attacked, is currently under attack, or is vulnerable to attack.

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. **[▲ Top]**

Access to Information and Protection of Privacy Policy (UAPPOL)

Information Services and Technology (IST) (University of Alberta)

Code of Student Behavior (University of Alberta)

Copyright Act (Department of Justice)

Ethical Conduct and Safe Disclosure Policy (UAPPOL)

Freedom of Information and Privacy Protection Act (Government of Alberta)

UofA Code of Practice for Learning Analytics (University of Alberta)

PUBLISHED PROCEDURES OF THIS POLICY

There are no published procedures of this policy.