ITServices information technology

Queen's UNIVERSITY

Electronic Information Security Guidelines (EISG)

Reference Material for Queen's Leadership

July 2009

Objective

These Guidelines are intended to:

- help the Queen's University community understand the risks inherent in using and managing electronic information;
- recommend measures and practices that can help to safeguard the security of information in electronic form; and
- assist in planning and operational decision-making.

According to the information systems security policy, either the Head of the Department or the Principal Investigator for a research group is responsible for ensuring that all employees are aware of and are working within policy and recommended practices for safeguarding personal and confidential information.

Authoring

These Guidelines have been developed by ITServices with the input and support of the Senate Information Technology Committee (SITC) and the Security Community of Practice. Their content has been developed using leading practices in electronic information security, as well the following Queen's Senate policies:

- Information Systems Security Policy (2003)
- Network Security Policy (2002)
- Computer User Code of Ethics (2005)
- Queen's University Student Code of Conduct (2008)

The Guidelines will continue to evolve as new risks to, and measures to preserve, electronic information security emerge.

To view the full guidelines, please visit the ITServices website at www.queensu.ca/its/security.

If you have any questions regarding these Guidelines, please contact the ITS Support Center at 36666 or by using the help form at http://www.queensu.ca/its/apps/forms/itsc/helpform/ .

Background

Unfortunately, many prominent universities have endured serious incidents where personal or confidential information was exposed. One need only scan the headlines to see institutions with information security breaches: McGill, UBC, Ryerson, Trent, Florida, Berkeley, Yale, Stanford; the list goes on. The risks can be great, both for the individual whose personal information may fall into the wrong hands, and for the university in terms of reputation, legal and other costs, and embarrassment.

Because information handling practices at universities are generally believed to be more lax, universities are being increasingly targeted by persons seeking to access personal data for whatever purpose, including identity theft. Between 2006 and 2008, the number of information security incidents at universities and the number of universities affected both increased by almost 70%.

It is incumbent upon all members of the Queen's community to be aware of practices to avoid, and to understand and adopt safer information handling and management strategies.

Categorization

The Guidelines have been categorized into distinct security areas:

A: Desktop and Laptop Computer Security
B: Password Security
C: Server and Network Security
D: System and Application Administration
E: Software Development and Selection (*in development*)
F: Confidentiality Agreements
G: Reporting Actual or Suspected Security Incidents

In addition, applicability has been identified by role for each Guideline.

Roles Definitions

Please note, an individual may possess multiple roles, and, by extension, have multiple responsibilities.

Department Head[1]

Department Heads, including Directors, are responsible for ensuring that security policy is implemented within the unit.

Principal Investigator

The individual recognized by the University as having lead responsibility for a research project or area. In the context of information security, the Principal Investigator has the same responsibilities as a Department Head, but typically on a smaller scale and/or with narrower scope.

Information Steward[1]

An Information Steward is a department head, or delegate, within the university who bears responsibility for the collection, processing, and maintenance of university records.

System Administrator

The individual assigned responsibility for installing and maintaining a server or application.

User

An individual who, by virtue of their role(s) at the University, needs to access and use a defined range of systems, applications, and information to fulfill their duties or pursue their studies.

[1] *Definition taken from Queen's information systems security policy*

Guidelines by Role:

All Users	A1. Antivirus and Anti-Spyware
	A2. Security Updates and Patches
	A3. File Sharing and Remote Access
	A4. Secure Data Deletion and Destruction
	A5. Encryption
	A6. Physical Computer Locking
	A7. Account Passwords
	A8. Operating System Accounts
	B1. NetID Password Hijacking
	B2. Sharing Your Personal NetID Password
	B3. Password Changes
	G1. Actual or Suspected Unauthorized Access
Department Heads	D1. System Assessments
	D2. Permissions
	F1. Queen's Employee Requirements
	F2. Third-party Requirements
Information Stewards	D2. Permissions
Principal Investigators	D1. System Assessments
	D2. Permissions
	F1. Queen's Employee Requirements
	F2. Third-party Requirements
System Administrators	C1. Physical Location of Servers
	C2. Active Services and Open Ports
	C3. Backups
	C4. Firewalls
	C5. Remote Access
	C6. Physical Location of Network Devices

A: Desktop and Laptop Computer Security

A1 – Antivirus and Anti-spyware

All computers connected to the University network should have up-to-date antivirus and anti-spyware software installed and running at all times. Scans should be run weekly.

A2 – Security Updates and Patches

All computers connected to the University network should have security patches and other critical software maintenance applied as promptly as possible. Server administrators and computer lab administrators should ensure that they are following a patch management schedule.

A3 – File Sharing and Remote Access

Any file sharing or remote access software should be configured to allow only secure access to files required for University business.

A4 – Secure Data Deletion and Destruction

Computer storage media (hard drives, CDs, tapes, etc.) should be disposed of in a secure manner. Before re-selling, donating or giving away a computer or storage device, all personal and confidential data must be deleted using a secure deletion process.

A5 – Encryption

Where there is any risk that data, especially personal or confidential information, may be accessible by unauthorized individuals, lost or intercepted, the data should be encrypted.

A6 – Physical Computer Locking

All computers should be secured with a physical locking device when left unattended.

A7 – Account Passwords

All accounts should be secured with a strong password, including the main Administrator account on Windows computers which is blank by default. Computers should be configured to require a password when use is resumed after a period of inactivity.

B: Password Security

B1 – NetID Password Hijacking

If you believe that your Queen's NetID is being used by an unauthorized person or that the password associated with it has become known to an unauthorized person, you should change your NetID password immediately and report the breach to ITServices.

B2 – Sharing Your Personal NetID Password

Never disclose your personal NetID password.

B3 – Password Changes

Passwords for systems which contain or provide access to personal and confidential information should be changed every 6 months.

C: Server and Network Security

C1 – Physical Location of Servers

All critical servers and its storage devices should be in a location that is accessible only to authorized individuals with appropriate keys or access privileges.

C2 – Active Services and Open Ports

Prior to putting a server into production, the system administrator should ensure that only the necessary ports are open and that only required internet services are enabled. System administrators should also regularly review the server's configuration.

C3 – Backups

All critical servers should be backed up on a regular basis. All backups should be stored in a separate secure location.

C4 - Firewalls

All servers which store or process personal and confidential information should be protected behind a firewall that uses an intrusion detection and prevention system.

C5 – Remote Access

Off-campus remote administration access to critical servers must be available only through encrypted and secure connection methods (e.g., SSH, SSL/VPN).

C6 – Physical Location of Network Devices

All network components (switches, hubs, routers, etc.) should be in a location that is accessible only to authorized individuals with appropriate keys or access privileges.

D: System and Application Administration

D 1 – System Assessments

Any new system or application which will store or provide access to personal and confidential information and will be connected to the Queen's network, should be subjected to a system assessment prior to being put into production.

D 2 - Permissions

All users of a system should be given access only to the functions that are required for their job. Users that no longer require access to the system should have their permissions revoked immediately. An annual review should be performed to verify and correct all permissions.

D 1 – System Assessments

Any new system or application which will store or provide access to personal and confidential information and will be connected to the Queen's network should be subjected to a system assessment prior to being put into production.

F: Confidentiality Agreements

F1 – Queen’s Employee Requirements

All employees whose position at the University requires that they have access to personal or confidential information should be required to sign a statement of confidentiality and non-disclosure.

F2 – Third Party Requirements

All parties who will have access to the University's personal and confidential information should be required to sign a confidentiality and non-disclosure agreement before they are given access.

G: Reporting Actual or Suspected Unauthorized Access

G1 – Actual or Suspected Unauthorized Access

Any member of the Queen's community who discovers or suspects that personal or confidential information has been stolen, exposed to unauthorized access, or is somehow vulnerable, should report such situations to abuse@queensu.ca without delay.