

## **Electronic Information Security Policy Framework - For Senate Approval**

On behalf of the University, Associate Vice-Principal IT and Chief Information Officer Bo Wandschneider seeks the approval of Senate for a new policy framework which is intended to address the security of University IT and information resources, and the privacy of sensitive information in the University's care. ITServices and our partners in the faculties and departments continue to strengthen the security of the Queen's IT infrastructure. However this doesn't fully address all risks – we continue to rely heavily on every member of the Queen's community to be aware of security risks and adopt appropriate practices to address them.

We began work on these policies several years ago on recommendations from the General Research Ethics Board, and the University's FIPPA Coordinator, and they have been reviewed with numerous campus stakeholders, all of whom supported the relevance of and need for these policies. It is very important to have them approved as soon as possible, as it will take time for the Queen's community to understand and become compliant with them. ITServices and our partners in faculties and departments will continue providing support aimed at helping members of the Queen's community through this process. We cannot realistically expect immediate compliance in all areas once these policies have been approved, but we believe these policies establish the vision we should all be striving for.



## Electronic Information Security Policy Framework

This policy framework groups policies and supporting materials relating to the security and integrity of the University's information and technology resources, and information that is in our care. All members of the Queen's community have a responsibility to preserve the integrity and reliability of the University's IT infrastructure, and the confidentiality of valuable or sensitive information. These policies should be read with the following Guiding Principles in mind:

1. The University's information technology resources are intended to support the mission of the University and the academic and administrative activities of the Queen's community.
2. Ensuring the reliability and integrity of the University's IT resources is dependent upon the cooperation of the Queen's community and the broad adoption of necessary controls and practices.
3. The University and all Queen's employees and students are accountable for compliance with information privacy legislation and other applicable laws.
4. The level of protection needed for each type of IT Resource should be commensurate with its sensitivity, and the severity of risk of it being compromised, exposed or stolen.

Definitions:

<b>Term</b>	<b>Definition</b>
<a href="#">Queen's University Data Classification Standard</a>	A key element of this Framework which categorizes various types of information or data according to the level of protection or safeguarding they require.
<b>Sensitive Information</b>	An electronic set of information or data, such as a database, file or document, that is classified as <i>personal</i> , <i>confidential</i> , or <i>operationally-sensitive</i> , as defined under the <a href="#">Queen's University Data Classification Standard</a> . Whether it is stored on or off campus does not matter.
<b>IT Resource</b>	A computer, device, or network on which there is a significant operational dependency for the University, a Department or Research Group, and/or which stores, transmits, or provides access to Sensitive Information. This includes computers functioning as servers, and storage devices such as USB keys and portable hard drives, but may also be personal computers, printers, facsimile and other devices which have internal storage capability that could contain Sensitive Information.
<b>Unit Head</b>	The Department Head or Director of a Queen's department, or the Principal Investigator or Lead Researcher for a research unit or project.
<b>System Administrator</b>	The individual who has primary responsibility for installing, configuring and maintaining an IT Resource. In the absence of a designated system administrator, the primary owner or user of an IT Resource is regarded as its System Administrator.
<b>Security Controls</b>	Safeguards or measures which eliminate, counteract or minimize security risks.

The intent and scope of these policies make it necessary for there to be some technical terminology. A glossary of Electronic Information Security Definitions is provided to aid understanding.

### Purpose/Reason for These Policies:

The purpose of the Queen's Information Security Policy Framework is to establish or foster:

1. responsibility for preserving the security and privacy of electronically maintained Institutional and personal information,

2. responsibility for preserving the security, availability, and integrity of the University's information technology infrastructure;
3. authority for ensuring compliance with the Policy Framework's policies and standards; and
4. compliance with the law and federal and provincial legislation.

**Scope of this Policy Framework:**

The Framework consists of three primary Policies:

Policy	Purpose and/or Scope
<b>Electronic Information Security Policy</b>	Preserving and protecting the University's electronically maintained information assets, and the privacy of electronically maintained personal and confidential information
<b>Acceptable Use of Information Technology Resources Policy</b>	Establishing what the University's information technology resources may or may not be used for, and ensuring there is equitable access to them.
<b>Network and Systems Security Policy</b>	Preserving the security, integrity, reliability and availability of the University's information technology infrastructure.

The Policies establish *what* each person's responsibilities are. Procedures, Standards and Guidelines are intended to establish *how* one upholds their responsibilities under the Policies.

These policies apply to:

1. all members of the Queen's University community, including course instructors, principal investigators and other researchers, staff, and students;
2. persons contracted by or collaborating with a Queen's department, research group, or employee, if those persons will have access either to the Queen's IT infrastructure, or sensitive information under the care or control of the University;
3. any information, including scholarly or research information or data, that is considered personal, confidential, or operationally sensitive, as defined by the Queen's University Data Classification Standard.
4. any element of the Queen's information system and network infrastructure, regardless of who operates that element, including any personal computer or device while it is connected to the University's network, either on campus or remotely.

**Authority:**

The Chief Information Officer (CIO) or his or her designates have the authority to investigate suspected or alleged non-compliance with these policies on behalf of the University. They will assess the significance of any alleged non-compliance, and determine a course of action through consultation with appropriate University officers. Serious non-compliance will be referred to the appropriate disciplinary body or process.

Where there are reasonable and probable grounds to believe that a failure to take action to address a non-compliance situation could result in significant harm to a person or University property, the CIO or his or her designate have the authority to enact emergency measures, the sole purpose of which are to contain a serious situation or mitigate a serious risk. Examples of such situations include, but are not limited to:

- Damage to University property has occurred or is likely to occur;
- The integrity of the campus network or computing infrastructure is in jeopardy;
- An individual's personal safety, or the privacy of personal or confidential information, is threatened; or
- There has been an alleged violation of the Law;

Immediate measures can include immediate restriction in or a complete suspension of an individual's or group's access to computing and network facilities and services, and/or disconnection of a system or device which

threatens the security or integrity of Queen's IT resources or personal or confidential information. Such measures will remain in effect until it has been determined that the non-compliance has been appropriately dealt with and any risks have been mitigated or eliminated.

## **Responsibilities:**

### Unit Head Responsibilities

- a) Establish which individual has responsibility for maintaining the security of each IT resource in the unit, and maintain a contact list of these individuals.
- b) Ensure that all Unit employees and any third parties such as contractors working with the Unit's IT resources are made aware of the Queen's University's IT security policies, standards and guidelines associated with installing and maintaining IT resources.
- c) Cooperate with ITServices during investigations relating to detected or suspected IT security vulnerabilities or incidents.

### System Administrator Responsibilities

- a) Maintain the security of all IT resources for which the System Administrator is responsible in accordance with these policies and associated standards.
- b) Maintain awareness of the University's IT policies, standards, guidelines and procedures.
- c) Cooperate with ITServices during investigations relating to detected or suspected IT security vulnerabilities or incidents.

### Software Developer Responsibilities

- a) Design and develop software applications with appropriate security measures and controls, as established by this policy and associated standards, IT industry best practices, and recommendations from ITServices and/or IT and information security audits.

### ITServices Responsibilities

- a) Provide Unit Heads and System Administrators with information, advice and assistance relating to the acquisition, installation and operation of IT resources in the Unit.
- b) Monitor campus network traffic to proactively detect unauthorized or malicious activity, alert potentially affected Units, and take appropriate measures to contain or mitigate risks.
- c) Conduct network-based security scans of systems and devices connected to the Queen's network to detect common vulnerabilities and/or compromised systems, and take appropriate measures to contain or mitigate the risk. Provide notice to and seek the cooperation of System Administrators when conducting such scans.
- d) Notify System Administrators of any risks detected and the measures to be taken to address them.
- e) Report recurring vulnerabilities which are not being appropriately addressed to the Unit Head for the area.
- f) Enact emergency measures to address serious security vulnerabilities, including temporarily disconnecting an IT resource from the University's network.
- g) Respond to external reports or complaints about security issues pertaining to IT resources within the University, and conduct technical investigations of any alleged security incidents or risks.
- h) Cooperate with and assist law enforcement agencies investigating serious security incidents or risks within the University.
- i) Provide the Queen's community with the means to report security incidents, risks or abuses so that they can be investigated and addressed.

*Contact Officer:*

*Related Policies, Procedures and Guidelines:*

Information Systems Security Manager, ITServices

Policies as listed in Scope section



## Acceptable Use of Information Technology Resources Policy

Category:

Approval:

Responsibility: Associate Vice-Principal IT / Chief Information Officer

Date:

### Definitions:

The following are definitions for key terms used in this policy:

<b>Sensitive Information</b>	An electronic set of information or data, such as a database, file or document, that is classified as <i>personal</i> , <i>confidential</i> , or <i>operationally-sensitive</i> , as defined under the <a href="#">Queen's University Data Classification Standard</a> . Whether it is stored on or off campus does not matter.
<b>Unit Head</b>	The Department Head or Director of a Queen's department, or the Principal Investigator or Lead Researcher for a research unit or project.

For other definitions, please see Electronic Information Security Definitions.

### Purpose/Reason for This Policy:

The purpose of this Policy is to establish the responsibilities of members of the Queen's community with respect to their use of Information Technology (IT) resources, and those actions necessary or that should be avoided in order to fulfill these responsibilities.

### Scope of this Policy:

This Policy applies to all Queen's faculty, staff and students, as well as to contractors or agents engaged by a department or employee, or any individual using Queen's IT Resources, whether on-campus or remotely.

### Policy Statement:

***The use of Queen's University information technology (IT) resources must be consistent with the academic mission of the University. These IT resources are provided to support the teaching, learning, research and administrative activities of the Queen's community. As a member or guest of the Queen's community, you may have access to valuable internal and external networks and resources, and Sensitive Information, and you are expected to use these resources in a responsible, ethical, and legal manner. Your actions should not adversely affect the ability of others to use these resources, or compromise the security and privacy of sensitive information.***

### Responsibilities:

**You will use Queen's IT resources for the academic and administrative purposes for which they are intended.**

**You will:**

- a) use only those IT Resources that you have been authorized to use, unless those resources are intended to be generally available to the Queen's community; and
- b) not use IT Resources for commercial activities unless such activities have been authorized in writing by the University, and do not adversely impact other users, or introduce risk to the security of personal or confidential information or the Queen's IT infrastructure.

**You will not adversely affect the ability of others to use IT resources within or external to Queen's, or compromise the integrity or reliability of those IT resources. You will:**

- a) ensure that your personal computer or workstation is maintained in accordance with [Electronic Information Security Guidelines](#); and
- b) not use Queen's IT resources in a manner that interferes with the normal operation of IT resources within or external to Queen's, or hinders or encroaches on the ability of others to use those resources.

**You will not compromise the security and privacy of sensitive information. You will:**

- a) keep your user authentication credentials, such as user accounts and passwords or similar authentication credentials, secure, such that they cannot be used by others;
- b) choose secure passwords for your user accounts;
- c) preserve the confidentiality of any University information to which you have access in the course of your employment or academic activities at Queen's;
- d) preserve the privacy of any personal or confidential information about or belonging to other individuals, to which you have access in the course of your employment or academic activities; and
- e) take the necessary precautions to prevent theft or unauthorized use of computers, storage devices, and information.

**You will use IT resources in a manner which is consistent with all University policies and does not cause damage to the University. You will:**

- a) maintain familiarity with Queen's Information Security Policies, Standards and Guidelines, and seek clarification from ITServices about any elements that are unclear; and
- b) adhere to the terms of any contractual agreements or arrangements between Queen's University and external service providers or organizations, and use such resources for the intended academic and/or administrative purposes only.

**You will not violate the rights of others or contravene the laws of Canada and/or the Province of Ontario in your use of IT resources. You will:**

- a) respect the copyright and intellectual property rights of others, whether at Queen's or elsewhere;
- b) respect the licensing agreements and terms for all software, and only install and use software as permitted in the license agreement for that software;
- c) respect the licensing agreements and terms for all electronic resources including databases, journals, books and other print, audio and video content;
- d) not use Queen's IT resources for any activities or actions which are illegal or do not comply with Canadian or Ontario legislation; and
- e) not use Queen's IT Resources to do anything that is a violation of the rights of others, such as displaying or distributing obscene, harassing, defamatory, or discriminatory material or messages.

**You will report suspected, known or observed IT or information security risks or exposures of a serious nature by following the Procedures for Reporting IT or Information Security Incidents or Risks.**

Unit Heads are responsible for ensuring that all supervisors, employees, students, guests and contractors are made aware of their responsibilities under the Queen's University Electronic Information Security Policy Framework.

Failure to comply with these responsibilities will be considered a violation of this policy.

*Contact Officer:*

Information Systems Security Manager – ITServices

*Related Policies, Procedures and Guidelines:*

- 1) *Electronic Information Security Policy*
- 2) *Network and Systems Security Policy*
- 3) *Various related Standards, Procedures and Guidelines*



## Network and Systems Security Policy

Category:  
Approval:  
Responsibility: Associate Vice-Principal IT / Chief Information Officer  
Date:

### Definitions:

The following are definitions for key terms used in this policy:

<b>Sensitive Information</b>	An electronic set of information or data, such as a database, file or document, that is classified as <i>personal</i> , <i>confidential</i> , or <i>operationally-sensitive</i> , as defined under the <a href="#">Queen's University Data Classification Standard</a> . Whether it is stored on or off campus does not matter.
<b>IT Resource</b>	A computer, device, or network on which there is a significant operational dependency for the University, a Department or Research Group, and/or which stores, transmits, or provides access to Sensitive Information. In general this refers to computers functioning as servers, and storage devices such as USB keys and portable hard drives, but also extends to personal computers, printers, facsimile and photocopiers which have internal storage capability that could contain Sensitive Information.
<b>Unit Head</b>	The Department Head or Director of a Queen's department, or the Principal Investigator or Lead Researcher for a research unit or project.
<b>System Administrator</b>	The individual who has primary responsibility for installing, configuring and maintaining an IT Resource. For the purposes of this policy, in the absence of a designated system administrator, the primary owner or user of an IT Resource is regarded as its System Administrator.
<b>Security Controls</b>	Safeguards or measures/countermeasures which prevent, counteract or minimize security risks.

For other terminology, please see Electronic Information Security Definitions and the [Queen's University Data Classification Standard](#).

### Purpose/Reason for This Policy:

The purpose of the Network and Systems Security Policy is to ensure the security, integrity and reliability of the University's information technology resources, and the confidentiality of sensitive information, by establishing responsibility for ensuring that IT Resources are installed and maintained in accordance with appropriate security controls, standards and practices.

### Scope of this Policy Framework:

This policy applies to all employees of Queen's University who manage IT resources where:

1. There is a significant operational or strategic dependency on an IT resource, at the University, Faculty or Department level; or
2. The IT resource plays a role in storing, accessing or transmitting personal, confidential or operationally-sensitive information.

This policy also applies by extension to external contractors or agents who are involved in deploying and managing IT resources for the University, a department, or a research group.

There is a wide range of IT Resources used across the University. The following policy statement establishes responsibility for ensuring the required security measures are implemented or used for IT Resources:

### **Policy Statement:**

***Members of the Queen's Community who are responsible for managing IT Resources on which the University or a Faculty, Department or a research group depend, OR which are used to collect, store or provide access to Sensitive Information, must ensure that those Resources are acquired, installed, configured, maintained and disposed of in a manner that is consistent with Queen's Electronic Information Security Policies, Guidelines and Standards, such that those Resources are not compromised, and sensitive information is appropriately protected. More specifically:***

- 1. IT Resources should be installed in locations with physical access controls which limit access to only those individuals who must have it.***
- 2. All servers connected to the Queen's network and providing services should be installed, configured and maintained in accordance with the Server Security Standard and the [Electronic Information Security Guidelines](#).***
- 3. Those individuals involved in configuring and maintaining IT Resources must do so in accordance with the Authentication and Access Control Standard and the [Electronic Information Security Guidelines](#).***
- 4. Those individuals who manage IT Resources which store, access, or transmit Sensitive Information must do so in accordance with the Queen's University Electronic Information Security Policy, the Sensitive Information Protection Standard, and the [Electronic Information Security Guidelines](#).***
- 5. Any new system or software application, whether developed or acquired, that will be used to gather, store, or provide access to sensitive information must undergo a system security assessment prior to being used with real data. This includes both new software applications and when applying major releases/upgrades of those applications.***
- 6. All individuals who manage IT Resources are required to monitor the availability and security of those resources to detect any risks to their regular operation, and to detect any attempts to compromise or access the resource by unknown or unauthorized parties. Logging of access and activity should occur and logs should be reviewed regularly.***
- 7. All software on which there is a significant operational dependency, or which is used to gather, store, process, provide access to, or transmit Sensitive Information, must be acquired or developed in accordance with relevant policies and standards in the Queen's University Information Security Policy Framework.***
- 8. All suspected or confirmed security incidents must be reported in accordance with Procedures for Reporting IT or Information Security Incidents or Risks.***

Contact Officer:

Information Systems Security Manager – ITServices

Related Policies, Procedures and Guidelines:

- 1) Acceptable Use of Information Technology Resources Policy
- 2) Electronic Information Security Policy
- 3) Various related Standards, Procedures and Guidelines



## Electronic Information Security Policy

Category:  
Approval:  
Responsibility: Associate Vice-Principal IT / Chief Information Officer  
Date:

### Definitions:

The following are definitions for key terms used in this policy:

<b>Sensitive Information</b>	An electronic set of information or data, such as a database, file or document, that is classified as <i>personal, confidential, or operationally-sensitive</i> , as defined under the <a href="#">Queen's University Data Classification Standard</a> . Whether it is stored on or off campus does not matter.
<b>IT Resource</b>	A computer, device, or network on which there is a significant operational dependency for the University, a Department or Research Group, and/or which stores, transmits, or provides access to sensitive information. This includes computers functioning as servers, and storage devices such as USB keys and portable hard drives, but may also be personal computers, printers, facsimile and other devices which have internal storage capability that could contain Sensitive Information.
<b>Information Steward</b>	The University officer or employee having primary responsibility for establishing policies and procedures relating to access, use, retention and destruction of Sensitive Information, and for ensuring that it is protected from unauthorized access or modification, and inappropriate use or disclosure, whether intentional or unintended.
<b>Information Custodian</b>	A Unit Head or individual assigned responsibility by the Steward for collecting, storing or enabling access to the Sensitive Information, and for maintaining appropriate controls to guard against unauthorized access or modification, and inappropriate use or disclosure, whether intentional or unintended.
<b>Unit Head</b>	The Department Head or Director of a Queen's department, or the Principal Investigator or Lead Researcher for a research unit or project.
<b>User</b>	Any individual within the scope of this policy who is granted or has access to Sensitive Information.

For other definitions, please see Electronic Information Security Definitions and the [Queen's University Data Classification Standard](#).

### Purpose/Reason for This Policy:

The purpose of the Queen's Electronic Information Security Policy is to establish responsibility for preserving:

1. the confidentiality, integrity and availability of electronically maintained Queen's University information or data; and
2. the privacy of electronically maintained personal information in the custody or control of the University or members of the Queen's Community, whether stored on premises or external to the University

### Scope of this Policy Framework:

This Policy applies to all members of the Queen's University who, in the course of their employment or academic activities, will gather, manage, distribute or use Sensitive Information. This includes departments, research groups,

faculty, staff, students, and volunteers, and extends to external vendors, suppliers, contractors or collaborators engaged in the gathering, management and use of Sensitive Information.

**Policy Statement:**

***Members of the Queen's Community who have care and control of or use Sensitive Information, are responsible for accessing and using only that information required for their academic or administrative role(s), for protecting the information from disclosure or unauthorized use by others, and for safeguarding the privacy of personal information about or belonging to others.***

**Responsibilities:**

Responsibility for preserving the security and privacy of information rests with each member of the Queen's community involved in the collection, management, and use of information. While it may be possible to delegate responsibility to others, one cannot delegate their accountability for preserving the security and privacy of information. Responsibilities vary according to each person's role in relation to the Sensitive Information, and in some circumstances a person may have multiple roles. Any person who has care and control of Sensitive Information is a Custodian for that information while it is in their care and control. Where Sensitive Information is stored on a personal computer or mobile device, the owner or holder of that IT Resource is a Custodian for that information. The following establishes the responsibilities of each of the primary roles associated with electronic information.

**As an Information Steward, you are responsible for ensuring:**

- a) that Sensitive Information for which you are primarily responsible is appropriately classified according to the [Queen's University Data Classification Standard](#);
- b) that all Custodians and Users provide appropriate protection for Sensitive Information in their care;
- c) that all Custodians and Users involved in gathering, managing or using the Sensitive Information, understand and accept their responsibilities under this Policy;
- d) that a review of who has access to the Sensitive Information is conducted regularly to ensure that only those still requiring access continue to have it;
- e) that a security assessment for the Sensitive Information be conducted on a regular basis;
- f) that in a situation when the security of Sensitive Information has or may have been compromised:
  - i. that immediate corrective measures are taken to eliminate the risk or exposure
  - ii. that the situation is reported in accordance with Procedures for Reporting IT or Information Security Incidents or Risks;
  - iii. that all affected individuals are notified when it is determined that the privacy of their personal information has been compromised; and
  - iv. that a security assessment be conducted immediately.

**As an Information Custodian, you are responsible for ensuring:**

- a) that access to the Sensitive Information is provided only to Users who require such access for legitimate University purposes, as established by the Steward, and that each user's access is approved by the associated Unit Head or designate;
- b) that a User's access to the Sensitive Information is limited to only those data subsets or elements that the User requires;
- c) that access to the Sensitive Information is revoked as soon as a User no longer requires access;
- d) that those responsible for installing and maintaining the hardware and software that is used to collect, house, manage or provide access to the Sensitive Information, do so in accordance with the Network and Systems Security Policy;
- e) that any new system or application that will house or provide access to the Sensitive Information undergo a system security assessment prior to being used;

- f) that subsequent system security assessments are conducted on a regular basis; and
- g) that the Steward is immediately notified if it is determined that the security of the Sensitive Information may have been compromised.

**As a Unit Head, you are responsible for ensuring:**

- b) that members of your unit are aware of and maintain compliance with these policies where applicable, fulfill their responsibilities as Steward, Custodian or User, and have signed confidentiality agreements where required by the Steward;
- c) that you have approved appropriate access only for those members of the Unit who require such access to fulfill their role in the Unit;
- d) that when an individual (staff, faculty, contractors, etc.) leaves the Unit, or her or his role changes, this is communicated to Information Custodians where appropriate and without delay;
- e) that all desktop, laptop or server computers which are used to collect, store or access the Sensitive Information are installed and maintained in accordance with the Network and Systems Security Policy and with the Sensitive Information Protection Standard.
- f) that any new system or application which will be used to collect, manage or provide access to the Sensitive Information has undergone a system security assessment prior to being used;
- g) that any visitors, suppliers, contractors, or collaborators who will require or have access to the Sensitive Information are made aware of this Policy and that they are subject to it; and
- h) that a secure means of information erasure or destruction is used prior to disposing of or donating any IT Resource in the Unit which contains or which at one time did contain Sensitive Information.

**As an Information User, you are responsible for ensuring:**

- a) that you access only the Sensitive Information you are authorized to use, and only for the academic or administrative purpose for which that Sensitive Information is intended;
- b) that you not disclose any portion of the Sensitive Information to another person not authorized to receive it;
- c) that you not disclose your user account and password (or similar authentication credentials) which you use to access Sensitive Information;
- d) that you notify your Unit Head immediately if the security or privacy of some or all of the Sensitive Information you use, or that is in your care or control, may have been compromised;
- e) that you maintain the personal computer or device which you use to store or access the Sensitive Information in accordance with Queen's University's Information Security Guidelines and Standards;
- f) that any Sensitive Information being transported on a portable computer or device, or sent to others electronically, be encrypted in accordance with the Sensitive Information Protection Standard and with the Electronic Information Security Guidelines.

*Contact Officer:*

Information Systems Security Manager – ITServices

*Related Policies, Procedures and Guidelines:*

- 1) *Acceptable Use of Information Technology Resources Policy*
- 2) *Network and Systems Security Policy*
- 3) *Associated Standards, Procedures and Guidelines*