Queen's University Electronic Information Security Policy Framework

Draft for Comment – January 2014

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:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queen's University Data Classification Standard</td>
<td>A key element of this Framework which categorizes various types of information or data according to the level of protection or safeguarding they require.</td>
</tr>
<tr>
<td>Sensitive Information</td>
<td>An electronic set of information or data, such as a database, file or document, that is classified as personal, confidential, or operationally-sensitive, as defined under the Queen's University Data Classification Standard. Whether it is stored on or off campus does not matter.</td>
</tr>
<tr>
<td>IT Resource</td>
<td>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.</td>
</tr>
<tr>
<td>Unit Head</td>
<td>The Department Head or Director of a Queen’s department, or the Principal Investigator or Lead Researcher for a research unit or project.</td>
</tr>
<tr>
<td>System Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Security Controls</td>
<td>Safeguards or measures which eliminate, counteract or minimize security risks.</td>
</tr>
</tbody>
</table>

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:

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

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.

In situations where it is determined that there is significant risk to the University or individuals, the CIO or his or her designate have the authority to enact emergency measures, the 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 a risk.

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: Information Systems Security Manager, ITServices

Date for Next Review: TBD

Related Policies, Procedures and Guidelines:

Policies as listed in Scope section

Associated Standards, Guidelines, Procedures, etc.

Policies Superseded by This Policy: None