Computer and Information Security Policy

<table>
<thead>
<tr>
<th>Section: Information Technology</th>
<th>Policy Number: 901</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Office: Information Technology</td>
<td>Effective Date: 10/01/98</td>
</tr>
<tr>
<td></td>
<td>Revised: 01/01/09</td>
</tr>
</tbody>
</table>

Scope
This policy applies to all members of the University Community who use the University’s computing resources or use any device containing University data, including faculty, administrators, staff, student workers, students, alumni, interns and other authorized users. Additional policy terms and conditions apply to students as part of the University’s Academic Computing Initiative, and these may be found in the Student Handbook.

Access Rights
St. John's University, New York (the "University") through the Department of Information Technology (IT) and Library initiatives, provides an array of computing resources to support the instructional, research and administrative functions of the University, including computing equipment, laptop computers distributed pursuant to the University's Academic Computing Initiative, networks (via wireless and wired access), Internet access, computers, terminals, communications networks, printers, software, data files and other relating computing equipment and devices ("Computing Resources"). Agreement and adherence to the following policies is a mandatory prerequisite to use of the Computing Resources and your use of Computing Resources constitutes your agreement to be bound by these policies. Users are prohibited from accessing any portion of a network that they have not been authorized to access, and may not provide access to any network to anyone who does not have University authorization for such access. Users are prohibited from circumventing or attempting to circumvent network security systems. Network privileges may be revoked temporarily or permanently at the discretion of the University for Violation of the Computer and Information Security Policy.

Authorized users are permitted to connect their own computing devices to the University's network or Internet connection after contacting the Department of Information Technology to arrange such access. A user's computer hardware must meet certain specific prerequisites. These specifications are subject to change. The University does not guarantee that all computers, even those that meet the specific prerequisites, will be able to access the local area network (LAN). In addition, no device will be granted access to a network unless it has current anti-virus software properly installed. In the case of an authorized user needing access from a remote site, Virtual Private Network (VPN) software will be installed on that user's computer which will allow fully secured encrypted access to the university's networks and systems.

Since rapid change is inherent to computer and information networks, the University reserves the right to modify these policies at any time. Although the University will make reasonable efforts to announce changes to policies, it is the user's personal responsibility to remain informed of the current policies by periodically checking the Human Resources Policy Manual (or the Student Handbook for students) and other University policy sources.
INFORMATION SECURITY POLICIES

The Department of Information Technology is the business unit that operates and manages computing resources at the University. IT has instituted commercially acceptable and reasonable internal mechanisms and controls to safeguard the privacy of data stored in our systems, although no system is immune from security breaches. These mechanisms require that specific privileges be given to personnel responsible for the maintenance of computer systems. These rights are afforded to ensure proper operation of the systems and will not be used as a method for accessing private information, except as necessary for maintenance of the systems or for investigation of policy violations, or as directed by appropriate legal authorities. These rights and privileges are secured and monitored in adherence to security guidelines.

These Policies are written to incorporate current technological advances. The technology installed at some units may limit immediate compliance with any policy. Instances of non-compliance must be reviewed and approved by the chief information officer or the equivalent officer(s).

Definitions: The terms “data” and “information” are used interchangeably in the document and refer to electronically stored data and information. The terms “system,” “database” and “network administrator” are used in this document. These terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty. Many students, faculty and staff members are the system administrators for their own machines and they must be cognizant of the types of data stored on their computers. The term “data owner” defines anyone who monitors and grants access to data within his or her oversight.

PURPOSE OF THESE POLICIES

By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

These information security policies serve the following purposes:

- To establish a University-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.

The Chief Information Officer, or designee, is responsible for implementing these policies.

POLICIES DEFINED:

- DATA CLASSIFICATION POLICY
- ACCESS CONTROL POLICY
- VIRUS PREVENTION POLICY
- SYSTEM SECURITY POLICY
- ACCEPTABLE USE POLICY
DATA CLASSIFICATION POLICY

It is essential that all University electronically stored data be protected. All data should be reviewed regarding its use, sensitivity, and importance before sharing or printing. When a question arises regarding the classification of data, data owners should seek assistance from the Internal Audit department. There are three data classes defined below:

**High Risk:** Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified. It is the data owner’s responsibility to implement the necessary security requirements and/or notify Information Technology if there are any questions or concerns pertaining to further protecting this or any other data.

**Confidential:** Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner’s responsibility to define and ensure the necessary security requirements.

**Public:** Information that may be freely disseminated

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.

- Data owners must acknowledge the data classification and must validate that they are protecting the data in a manner appropriate to its classification.
- No University-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Data owners are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- High risk data and confidential data must be encrypted during transmission over insecure channels.
- High risk data and confidential data must never be downloaded to laptops, flash drives or mobile devices.
- Backups of data must be handled with the same security precautions as the data itself.

ACCESS CONTROL POLICY

- Data may be accessed only by authorized users and disseminated based on need and job requirements.
- Users must not share usernames and passwords. All users must secure their username or account, password, and system access from unauthorized use.
• All users of systems that contain high risk or confidential data must have a strong password; the strength of a password is a function of length, complexity and randomness, usually requiring a combination of letters, numbers and capitalization.
• Passwords must not be placed in emails unless they have been encrypted.
• The Department of Information Technology may take all reasonable actions to ensure the integrity of its Computing Resources, including prevention of damage to data and equipment, irrespective of any asserted privacy interests.
• All computer-related equipment must be returned when one leaves the University. In addition, all licensed software on non-university equipment or devices must be erased.

VIRUS PREVENTION POLICY
• The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators will be subject to prosecution.
• All computing devices that connect to the network must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor’s recommendations. This includes non-university computing devices as well.
• All university supplied computing devices must have their university supplied anti-virus software enabled and accepting automatic updates.
• It is the responsibility of every employee to notify the Information Technology Department in the event that the anti-virus software on their university computing device detects a virus.

SYSTEM SECURITY POLICY
• All systems connected to the Internet should have a vendor supported version of the operating system installed.
• All systems connected to the Internet must be current with security patches.

ACCEPTABLE USE POLICY
• University computer resources must be used in a manner that complies with University policies and State and Federal laws and regulations. It is against University policy to install or run software requiring a license on any University computer without a valid license.
• Uses that interfere with the proper functioning or the ability of others to make use of the University’s networks, computer systems, applications and data resources are not permitted.
• Use of University computer resources for personal profit or non-university purposes is not permitted except as addressed under other University policies.

USER RESPONSIBILITY
Below, the University sets forth terms and conditions for the use of Computing Resources. Listings of specific acceptable and unacceptable uses are illustrative examples and are not meant to be exhaustive. The University is the sole and conclusive authority on questions
relating to acceptable uses of its resources. If a question about use arises, the use should be considered "prohibited" until Information Technology directs otherwise.

**Acceptable Uses**

Computing resources are available for use only by University faculty, administrators, staff, student workers, students, alumni, interns and other authorized users. Moreover, use of such resources is restricted for tasks related to the instructional, research, and administrative objectives of the University and the University's mission. When conducting University business via email communications, University email accounts and not personal or other non-University email accounts are to be used.

The University makes networks and the Internet available to users via wired and wireless connections. The University does not guarantee the privacy of wireless transmissions, and does not guarantee that the network will provide uninterrupted and/or error-free wireless communications.

**Prohibited Uses**

Computing resources may be used only for purposes that are legal, ethical, and consistent with the University's mission. The following activities are examples of prohibited behaviors with respect to the use of University Computing Resources:

- **Improper Usage**
  - Tampering with the anti-virus software installed on University owned or provided devices or networks or failing to use updated anti-virus software when accessing a University network.
  - Circumventing or attempting to circumvent software or hardware security systems.
  - Altering system software or hardware configurations, or disrupting or interfering with the delivery or administration of computer resources.
  - Intentionally or negligently distributing malicious software, such as computer worms, viruses, or Trojan horses.
  - Creating programs that secretly collect information about users.
  - Using computing resources, including electronic mail, to send nuisance messages such as chain letters, junk mail and profane, obscene, threatening, libelous or harassing messages.
  - Attempting to access or accessing the University's or another user's account, private files, or email without the owner's permission.
  - Attempting to access or accessing systems outside of the University without authorization of that system's owner.
  - Misrepresenting one's identity in electronic communication.
  - Using computing resources to engage in conduct which intentionally interferes with others' use of shared computing resources. This includes consuming gratuitously large amounts of system resources (e.g., Internet bandwidth, disk space, CPU time) and exceeding time limits where they have been established in University facilities such as computer labs and libraries.
- Using computing and/or electronic mail resources for commercial or personal profit-making purposes or for solicitation or for activities that violate local, state, or federal law.
- Intercepting or monitoring, or attempting to intercept or monitor, network communications or other communications not intended for that user's access without prior authorization.
- Displaying, posting, printing, or sending material that is contrary to the mission or values of the University

- **Willful Infringement**
  - Allowing or assisting unauthorized users to gain access to computing resources.
  - Installing software (including games) on University-provided computing equipment without obtaining authorization in advance. The University reserves the right to remove software that violates this policy without advance notice to the user.
  - Infringing upon the intellectual property rights of others in computer programs or electronic information, including plagiarism and unauthorized use or reproduction in violation of patents, trademarks and copyrights and/or software and other licensing agreements. (See “Copyrighted Material” provision)
  - Failing to comply with all applicable laws concerning the transmission, receipt or monitoring of wireless and wired communications.

- **Copyright Infringement**
  - The use of Computing Resources in violation of international and federal copyright laws is strictly prohibited. These federal laws provide to the author of an original work, whether that work is a video, a sound recording, software, or printed material, the exclusive rights to reproduce, adapt, publish, perform and display that work. Anyone other than the copyright holder is required to obtain the express permission of the copyright holder to use the work for any of these purposes.
  - The University prohibits the use of its computing resources for Internet downloading and sharing of copyrighted music and video in violation of copyright laws. In addition to violating University policy and the law, file-sharing programs (such as Grokster, KazaA, Gnutella, and Limewire) that permit these activities also may impair the University's broadband system because their use causes a strain on the University's broadband capabilities and other network resources. For these reasons, the downloading, or making available for others to download, a copyrighted movie, television show or sound recording without permission of the copyright holder is a violation of University policy. In furtherance of this policy, the University has, and will continue to create, technologies to identify and disable access to file-sharing websites that facilitate the violation of applicable law and University policy. In the event that you desire to legally download any file that may strain the University's broadband capabilities, please contact the Department of Information Technology to arrange for a time and place to do so.
*** UNIVERSITY RIGHT OF ACCESS ***

The University reserves the right to access data files, information files and messages stored in user accounts, including email, text messages or other electronic communications on university supplied devices; therefore, users do not have a legitimate expectation of privacy with regard to these files or communications.

Fair Use of Copyrighted Material
Creation of internet content and other materials for educational, research and administrative purposes must be in full compliance with current copyright laws.

Internet / Intranet Content and Publishing
Consistent with the purposes for which University computing facilities are intended, web content may be created and posted only in support of the instructional, research, and administrative objectives of the University. Web content may not include any advertising, nor may it be used in support of any commercial or business activities.

The University reserves the right to restrict web content or remove any part of such content for violation of these or any University policies, including for causing excessive traffic to the University's web servers.

Indemnification
Each user is responsible for his or her own activities in using the University's computing resources, and will indemnify and hold harmless the University from any liability to the user or any third party arising out of the use of the computing resources by the user, or any loss of information existing or stored on the University's computing equipment or resources, including all files and electronic mail.

Intellectual Property Ownership Rights
Ownership of intellectual property (with the exception of traditional works of scholarship or creativity, such as textbooks and instructional material) produced through significant use of the University's computing equipment, networks, and information resources shall reside with St. John’s University. In instances where such materials are sold, licensed or otherwise marketed, royalties on revenue shall be shared between the University and the authors of such materials in accordance with the University's patent and intellectual property policies.

Information Security Requirements
- Education should be implemented to ensure that users and data owners understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, database administrator and users.

- Violation of the Computer and Information Security Policy will result in disciplinary actions as authorized by the University in accordance with University and campus disciplinary policies, procedures, and codes of conduct.

- University data classified as high risk or confidential must never be downloaded to laptops, flash drives or mobile devices.
The Computer and Information Security Policy is updated on a regular basis and published as appropriate.

Every six months, the Department of Information Technology mandates that users change their system password to protect the privacy of their information.

Sanctions
Violations of this policy constitute unacceptable use of Computing Resources. Violations may result in a loss of computing privileges and may subject users to the University’s regular disciplinary processes, including suspension or dismissal from the University. In instances where alleged violations of this policy could result in harm to or otherwise compromise the University’s computing resources, the University reserves the right to immediately suspend computing privileges pending an investigation of the validity of the charges.

In addition, illegal acts involving University computing resources may also subject violators to prosecution by local, state and/or federal authorities. Suspected or known violations should be reported to the appropriate University authority, in accordance with current disciplinary procedures. Violations will be processed in accordance with these procedures and/or law enforcement agencies.