I. PURPOSE:

A. This policy is required to aid in the development of a secure computing environment where unique challenges exist due to the diverse community being supported (Education, Business, and Religious).

B. With respect to members of the Saint Vincent College Faculty, this document is not meant to conflict with, alter or modify in any way the policies and procedures set forth in Section 3.4.2 (Computer Usage) of the Faculty Handbook. To the extent that there is any perceived inconsistency between Section 3.4.2 and this document, the provisions of Section 3.4.2 prevail with respect to any matter dealing with a member of the College Faculty. This policy also does not supersede any provision of the College's Acceptable Use Policy.

II. IMPACT:

A. Participants (scope): All end users (administration, faculty, staff, students, alumni with accounts, monks, and priests) of the Saint Vincent community.
B. Implementation: CIO is responsible for implementation and interpretation.
C. Other Affected Parties: All stakeholders.
D. Potential Impact: There is a substantial budgetary, legal, and logistical impact required to ensure this policy is enforced.

III. COMPLIANCE:

A. Strategic Plan (if applicable): IS Strategic Plan.
B. Applicable Laws (if applicable): Policy makes best effort to support compliance of the IS International Mobile Computing policy, Acceptable Use Policy, GLBA Safeguards Rule, DMCA, HEOA, CALEA, HIPAA, CAN-SPAM Act, Fair Credit Reporting Act, USA PATRIOT Act, FTC Red Flags Rule, Fair and Accurate Credit Transactions Act, and dozens of other privacy/security-related laws and regulations.
C. Authorization: President and CIO have authorization for approving this policy.
D. Exceptions: Any member of the President's Senior Cabinet/Council can request day-to-day policy exceptions, but notice should be provided accordingly as granted.

IV. POLICY AND PROCEDURE ELEMENTS:

A. Index: N/A
B. Definitions: N/A
C. Statement of Need, History: The College, Archabbey, Seminary, and Parish continues to change, grow and embrace an increased use of technology to support its institutional goals and mission.
D. Body of policy and procedures: As follows:

As a community of educators, students, business people, and religious leaders committed to the values and perspectives of the Catholic Benedictine tradition, we recognize the potential benefit, as well as danger, in the use of technology. Consequently, we make careful use of the products of science and technology in order that we might responsibly fulfill our callings as students,

faculty, staff, monks, and priests. We are stewards of technology and therefore, acknowledge our accountability to one another and to the mission of Saint Vincent.

Each member of the Saint Vincent community is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, mobile devices, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. This security policy is not exhaustive in coverage, but rather provides the essential framework, guidelines, and recommendations to secure computing in today's technological environment.

1. The authorized user is responsible for the proper use of the account including password maintenance guidelines (Appendix A) and file protection measures. A user should never share an account or password with anyone. For applications that do not force password changes, authorized users are expected to change their passwords frequently to help prevent unauthorized access and misuse.

2. Saint Vincent computing facilities, including the entire campus network and access to the Internet, are designed to only be used by the faculty, staff, priests, monks, current students, and former students of Saint Vincent who still hold active accounts. Under normal circumstances friends, spouses and children of faculty, staff, and students will not be given network accounts. VP level approval must be obtained for exception to this rule.

3. Users are responsible to secure their office environment to protect the technological assets in their possession and to secure any Saint Vincent owned mobile devices they are in possession of when outside of their office to ensure the hardware, software and information contained within are protected.

4. The College is responsible for installing antivirus and antispyware software on College owned equipment, utilizing Firewall technology, and keeping all O/S patches up to date to prevent from infection by a virus, Trojan, worm, or other malicious software (Appendix B). As budget constraints loosen, plans are in place to implement Intrusion Detection and Encryption solutions. It is essential that users who connect to the College network have updated antivirus and antispyware software on their "personal" device(s), utilize firewall and encryption software were feasible, and keep their O/S patches up to date (Appendix C).

5. Email is a valuable resource for communication within the community, but it can easily create security vulnerabilities. All messages and attachments created, sent or retrieved over the Internet have the possibility of getting infected before, during, and after transmittal. Refrain from sending and forwarding jokes or chain letters via email. They waste bandwidth and storage space, and can contain viruses and other malware. Care should be taken to not open any emails from unknown sources and remain cautious about opening emails and attachments from known sources.

6. Care should be taken when surfing and posting information on the Internet and especially in Social Directories and Social Media sites, such as Facebook, Twitter, etc. When using social media, a user needs to be aware that viruses are known to occur and that identity theft and Internet impersonation happens regularly. Any one of these types of compromises can cause an individual undue stress, loss of data, and loss of personal assets and reputation. It can also cause financial, data, and reputation loss to Saint Vincent. Personal identification information should be kept to a minimum and users should be very careful about the type of personal information that is being displayed and shared with others. Make sure the image you project on-line is one that accurately represents you and that you protect yourself by taking advantage of the privacy settings, which help control who can access your information.

7. To reduce security risk, "personally" owned laptops, macbooks, etc. are not to be connected to the network jacks via a patch cable in the classrooms, computer labs, or offices, unless it is under the direction of the IS Department. Mobile devices should only use the wireless network provided by the College or the 3rd party Resnet provider. Laptops and other mobile devices that are "property of the College" should be connected by patch cable to the network jack when the device is in an office or classroom and a network jack is available because it allows for more efficient processing and better security. However, if wireless is the only feasible option, College owned devices should connect to the SVC_Private wireless network, which requires an ID and password. Connecting via a network jack or SVC_Private ensures the device will receive auto-updates of the latest antivirus and O/S patches. Additionally, the wireless signal should be turned off when the device is connected by cable. Having both connections active can cause problems with the laptop or mobile device, and it can also cause problems on the network.

8. Users are responsible for following established security guidelines for any networks or systems used outside of Saint Vincent. For any work on networks outside of Saint Vincent, through the Internet, users should follow and use those facilities according to that network's security guidelines. Users are responsible for reporting to the IS Department any violation of security guidelines by another individual. Users are also encouraged to report any information relating to a flaw in, or bypass of, computer facilities security.

9. Requests for service regarding any security concerns, to report network security incidents, or to get answers to your questions about network security or this policy, please call the IS Service Desk at (724) 805-2297, or stop by the IS Service Desk on the ground floor of Alfred Hall, or send an email to servicedesk@stvincent.edu. Each request will be logged through the IS Service Request database to insure a proper response.

APPENDIX: N/A

A. Password policy as established in Active Directory:
   - Enforce Password History = 6
   - Maximum Password Age = 120 days
   - Minimum Password Age = 0 days
   - Minimum Password length = 8

- Password Complexity = ON
- Character Complexity = 3 of 4 required (Capital, Lowercase, Number, and/or Special Character, such as ?, *, #, !)
- Account Lockout Threshold = 5 invalid login attempts
- Account Lockout Duration = 30 minutes

B. IS Department security responsibilities:
- Remain knowledgeable and current regarding relevant security best practices, requirements, and guidelines
- Analyze potential threats and the feasibility of various security measures in order to provide recommendations and solutions to all stakeholders
- Implement security measures that mitigate threats, consistent with the level of acceptable risk established by Senior Administration, such as remote VPN connectivity, password managers/vaults, virtual desktops, encryption, etc.
- Establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements
- Communicate the purpose and appropriate use for all technological resources
- Establish acceptable levels of security risk by assessing factors such as:
    i. how sensitive the data is, such as research data or information protected by law or policy
    ii. the level of criticality or overall importance to the continuing operation of the campus as a whole, individual departments, research projects, or other essential activities
    iii. how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources
    iv. how likely it is that a resource, such as Peer-to-Peer file sharing or illegal downloading web sites, could be used as a platform for inappropriate acts towards other entities
    v. limits of available technology, programmatic needs, cost, and staff support

C. User security best practices:
- Keep all "personal" devices patched and up to date with the latest O/S and application security patches
- Use antivirus and antispyware software to protect "personal" devices from malware (be aware that most all technology devices are susceptible to viruses)
- Use some type of personal firewall software
- Educate yourself about security vulnerabilities, security best practices, etc.
- Minimize network and system services by only running needed applications
- Backup your personal files on multiple secondary storage devices (DVD, Jump drives, external hard drives, cloud storage options, etc.)
- Do not store work related files on the hard drive of your Saint Vincent-issued device, rather save them on your provided network space, which is backed up regularly and protected through network access permissions
- Secure your home network and your mobile connection
- Protect the assets of the College and also your own personal devices by keeping them locked up and out of sight when not in use

- Be especially careful to protect sensitive intellectual property that has research and/or commercial value because it is a prime target of hackers
- Be cautious when clicking on update pop-ups, especially while using untrusted hotel Internet connections. Some pop-ups are actually scams designed to trick people into installing malicious software
- Assume that any computer you use other than your own is not secure, including those of friends you are staying with, at cyber-cafes, in libraries, restaurants, hotels, etc.
- When using any shared computer, don't enter sensitive information such as passwords, bank account numbers, or credit cards numbers
- Anything you send over the Internet from a public access point may be intercepted and logged by unknown parties. To avoid compromising sensitive data when using public Internet access, only enter confidential information on secure web pages. Secure web pages have addresses beginning with https
- Make sure your personal device auto screen locks after a short period of time
- Use passcodes on all mobile devices (smartphones, iPads, tablets, etc.)
- Use strong passwords:
    i. General guidelines to follow for creating and using a strong password:
        1. Don't use an easily guessed password, such as names of family, pets, friends, co-workers, birthdays, and other personal information
        2. Don’t use simple word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, 123456, etc.
        3. A password should be as long as possible, while still being easy-to-remember. One way to do this is create a password based on an easy-to-remember phrase. For example, the phrase might be: "I Can Remember My Password" and the password could be: "1CNr3mMyPwd!" or "1cR3Myp*d." or some other variation
        4. You should change your passwords on a regular basis, at least monthly, and try not to use the same password for all your applications.
        5. You should also change your password any time you suspect that your account has been compromised or tampered with