I. PURPOSE:

A. This policy is necessary to aid in the protection of the data and physical (technological) assets that faculty, staff, students, monks, or priests carry with them when traveling internationally. The policy covers the mobile computing devices and electronic storage devices that are provided by the College and the users "personal" devices that are used for business, education, or religious purposes, which have the potential of connecting to international networks and then the College network upon return. A college environment is very different from a corporation or a government agency, because of the openness and free flow of information that is promoted among professors, researchers, religious leaders, and students. The requirement to provide a balance between openness and security restricts the IT Department from implementing strict computing standards, regulations, and travel security requirements, which creates a higher risk of vulnerabilities that are especially heightened during international travel.

B. The use of mobile devices extends the boundary of Saint Vincent systems and adds risk that must be properly mitigated. Mobile devices provide the ability to transmit or receive information via networks, which presents security risks due to the susceptibility to the interception of transmitted information and introduction of malware. Such risks are higher while on international travel; especially in locations where telecommunication networks are owned or controlled by host governments that choose to monitor transmissions.

C. 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 (administrators, faculty, staff, students, monks, and priests) of the Saint Vincent community who travel internationally.
B. Equipment (scope): This policy covers all Saint Vincent-issued mobile devices and users "personal" mobile devices that have the potential of connecting to the College network upon return from international travel. This includes laptops, Macbooks, notebooks, tablets, iPads, USB drives, Blackberries, smartphones, cell phones, external drives, compact disks, DVDs, PDAs, digital cameras, audio recording devices, GPS devices, etc.
C. Implementation: CIO is responsible for implementation and interpretation.
D. Other Affected Parties: All stakeholders.
E. Potential Impact: There is substantial budgetary, legal, and logistical impact required to ensure this policy is enforced.

III. COMPLIANCE:

A. Strategic Plan (if applicable): IT Strategic Plan.

B. Applicable Laws (if applicable): U.S. export control laws prohibit or restrict taking laptop computers or other electronic mobile devices into certain countries, so users who travel internationally should educate themselves, as will the IT staff, on such laws pertaining to their travel location and must ensure that they comply with such laws. This policy makes best effort to support compliance of the IT Security 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, travel-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: Mobile device - portable disk-based, removable storage media (e.g., floppy disks, compact disks, DVD, USB flash/jump drives, external hard drives, and other flash memory cards/drives). Portable computing and communications device with information storage capability (e.g., notebook/laptop/tablet computers, personal digital assistants, cell phones, smartphones, digital cameras, and audio recording devices).
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, while at the same time the amount of international travel also continues to increase.
D. Body of policy and procedures: As follows:

Before departure:

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

2. The authorized user who is scheduled to travel internationally should submit an IT Service Request informing the IT Department that plans have been made to travel internationally with a mobile computing device.

3. At least a minimum of one week notice should be given to take a look at the device(s) to ensure it is currently clean of viruses and updated with the necessary software (antivirus, antispyware, encryption, and O/S patches).

4. One week notice is also required if the user would prefer to have a loaner device made available in place of their standard device. Laptops and USB storage devices

are available by the IT Department as loaners. To obtain "specially configured" loaner devices the user should make mention of that in the IT Service Request and provide more notice if possible.

5. Appropriate notice is necessary to allow the Service Desk Analyst sufficient time to work with the user to transfer all work related files needed for the trip to the loaner laptop or ensure the user's device is virus free and properly protected prior to departure.

6. The user can bring their device(s) to the IT Service Desk or arrange a time for a Service Desk Analyst to come to the user's office space or location of choice to evaluate and process the device. If a loaner device is preferred, the user can either come to the Service Desk to pick up the device or it can be delivered to the user, but this all depends on the amount and type of work that needs done and the status of the device in question.

7. The IT Department will do its best to ensure that certain IT staff who provide support for standard mobile devices and specially configured devices held as loaners are trained to develop and publish documentation about international travel with mobile devices. It will also ensure that certain IT staff are technically competent for configuring devices and collecting, sanitizing, and transferring data, and are as knowledgeable as possible about U.S. export control laws and manufacturer repair information in the countries that are frequented by users from Saint Vincent.

8. Before traveling internationally, it is preferred that:
    - If possible, the user utilizes a Saint Vincent-issued mobile device(s) for Saint Vincent-authorized travel rather than "personal" devices
    - Mobile devices not be taken if the trip can be accomplished without them
    - Only the minimum amount of information necessary (electronic and paper) be taken to accomplish the trip
    - The user saves all information from their mobile device(s) to the appropriate Saint Vincent network systems prior to travel
    - The user assists the IT staff by becoming as informed as possible about how to troubleshoot basic technical issues regarding their device and where to go on the manufacturer's website for repair information in the country to which they are traveling. This is particularly important for those who will be traveling with their "personal" device(s), which may not be a brand that the IT Department utilizes and supports
    - The user assists the IT staff by educating themselves on U.S. export control laws pertaining to their travel location so they know if laptop computers, encrypted devices, or other electronic mobile devices are prohibited or restricted

- The user remembers to take along the documentation, contact information, and a copy of this policy provided by the IT Department to be utilized in case they experience any hardware or data compliance problems

While traveling:

9. In case of the loss, theft, compromise, or suspected compromise of "personal" devices, Saint Vincent-issued mobile devices, or Saint Vincent information during travel, users should *immediately* while still traveling report the event to the IT Service Desk. It is preferred that this be done via a phone call if at all possible. If after EST daylight hours, the user should send an email to servicedesk@stvincent.edu to report the incident or if *immediate* after-hours attention is needed, get in contact with the CIO and/or Director of Technical Services.

10. Users should be aware of the following:
    - Manually turn off the wireless access and Bluetooth capabilities, and lock an SD card if possible to prevent writing to the card when not in use. Turn these capabilities on, or unlock, only when needed
    - Government security agencies in some countries may log your Internet activity without informing you that they are doing so
    - In some countries it is common practice for the government or businesses to copy data from your computer without your knowledge or consent
    - Sensitive intellectual property that has research and/or commercial value is a prime target for 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

11. Users should also physically secure all mobile devices and information while traveling, for example:
    - Do not store devices in checked baggage
    - Do not leave devices or sensitive information unattended in public places, e.g., airports, restaurants, taxi cabs, limos, conference meeting rooms, waiting rooms
    - Guard against eavesdroppers and shoulder surfers

- Secure laptops in hotel rooms with a locking device or in a hotel provided safe
- Use digital signature and encryption capabilities if made possible by the IT Department and allowed by the host government

Upon return:

12. Upon return from international travel, users should *immediately* contact the IT Service Desk to arrange for the pickup, scanning, and sanitizing of loaner devices, their Saint Vincent-issued work device(s), or "personal" device(s).

13. It is imperative that users not connect the device(s) they traveled with to any Saint Vincent system or network (wired or wireless) until the device is scanned and sanitized by the Service Desk.

14. If there is information on loaner devices that the user needs, the user must request the information be removed and provided to them via an IT Service Request and notice must be given prior to the device being sanitized so the data is not lost. The Service Desk Analyst will ensure the information is malware free prior to giving it back to the user.

15. If malware is detected and cannot be removed or it is "suspected" that it has not been removed after sanitization, the Service Desk Analyst will quarantine the device and contact the user of such event. The Service Desk Analyst will consult with IT management to determine if outside consulting assistance is needed. If the device was a "personal" device or a Saint Vincent-issued work device (not a loaner), the user will be notified of the issue and a loaner device will be provided to the user until the original device is certified as clean.

16. Users should consider changing their passwords upon returning from international travel. If your password was compromised while abroad, changing it will render the stolen password useless.

APPENDIX:

1. The Higher Education Information Security Council (HEITC) has developed a resource page, Security Tips for Traveling Abroad: https://wiki.internet2.edu/confluence/display/itsg2/Security+Tips+for+Traveling+Abroad

2. The FBI has also developed a helpful brochure, Safety and Security for the Business Professional Traveling Abroad: http://www.fbi.gov/about-us/investigate/counterintelligence/business-travel-brochure