N.B.: Seton Hall University reserves the right to amend or otherwise revise this document as may be necessary to reflect future changes made to the I.T. environment. You are responsible for reviewing this Policy periodically to ensure your continued compliance with all Seton Hall University I.T. policies.

1. **Policy Title**: Remote Access (VPN) Policy

2. **Audience/Scope**: This policy applies to all SHU, employees, contractors, consultants, temporary employees, and all personnel affiliated with third party employers utilizing the VPN to access the SHU Network.

3. **Policy Statement:** Use of a VPN allows members of SHU to securely access University network resources as if they were on the campus. Consequently, it is extremely important to impose strict safeguards on such access to protect Personally Identifiable Information and Confidential University Information.

4. **Definitions:**

   a. VPN: Virtual Internet Protocol "tunnel" into the SHU network, as though the "remote" user was connected to a Seton Hall network jack.

   b. Remote Access: Not physically connected to an on SHU campus network connection; "on the internet", apart and away from SHU.

   c. Personally Identifiable Information - (including, but not limited to, dates/places of birth, social security numbers, credit card information, maiden names, home addresses and home/personal cell phone numbers)

5. **Policy Statement: Guidelines for VPN use**

   a. VPN gateways will be set up and managed only by UITS Network and Telecom group.
   b. VPN must use strong authentication. Password should expire every 90 days.
   c. Only VPN software that is approved by and/or distributed by UITS may be used to connect to the SHU Internal Network.
   d. All requests for VPN accounts must be routed through the UITS Help Desk ticketing system. Access will be granted only to authorized users on a strict business need with prior approval required from Department Head and the University Information Security Officer.
   e. Use of VPN service should only occur from trusted service which does not include Internet cafes and other public places.
   f. Users are bound by policies not limited to those listed in Paragraph 7, below.
   g. VPN access is available using University owned and approved laptops installed with a VPN client distributed by UITS. It is highly recommended that an SHU owned laptop be used for VPN Access and by using VPN technology with personal equipment, users must understand that their machines are a de facto extension of SHU's network, and as such must comply with SHU's Information Technology Policies.

h. All computers connected to SHU’s internal networks via VPN or any other technology must use the most up-to-date anti-virus, anti-spyware, operating system patches, and firewall software.
i. Sponsored third parties such as software consultants or vendor support personnel, are prohibited from using SHU’s VPN. Exceptions may be made on a case-by case basis by the Information Security Officer.
j. It is the individual responsibility of the users with VPN privileges to ensure that unauthorized persons are not allowed access to SHU internal networks.
k. The VPN connection provides secure access into the SHU Network. VPN does not, by itself, provide Internet connectivity. When off campus, users are responsible for providing their own Internet service in order to use SHU’s VPN service.
l. VPN users will be automatically disconnected from SHU's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Artificial network processes should not be used to keep the connection open.
m. Only one active VPN connection is allowed per user.
n. VPN account should not be shared with others. Users should not download any confidential information pertaining to the University on personal equipment. While connected to the VPN, access Internet resources external to SHU is a high Risk and not recommended.
o. For security reasons, each VPN user should disconnect from the VPN server when access to the SHU network is no longer required.
p. Procedure must be in place to deactivate accounts of terminated users or those who longer require access. User re-certification will be on a quarterly basis.

6. **Notification:** If Confidential Information is inadvertently disclosed or lost to any 3rd party, or is suspected to have occurred due to the use of VPN service, The University Information Security Officer, Department Supervisor and the Helpdesk should be notified immediately so that appropriate action can be taken.

7. **Related Policies and Standards:**
   a. P-01 Information Security Policy
   b. P-02 Information Technology Appropriate Use Policy

8. **Enforcement.** Any user found to have violated this policy may be subject to loss of certain privileges or services, including but not necessarily limited to loss of VPN services. The Information Security Officer is charged with the responsibility to periodically review the policy and propose changes as needed.

9. **Comments or Suggestions.** Questions concerning this Policy can be directed to or the University Information Security Officer or UITS Help desk.

10. Disclaimer

Access to VPN Service

Seton Hall University may, at any time and for any reason, change, terminate, limit or suspend this Service, in whole or in part. Your access to the Service is completely at the discretion of Seton Hall University, and your access to the Service may be blocked, suspended, or terminated at any time for any reason including, but not limited to, violation of these Terms and Conditions, disruption of access to other users or networks, or violation of applicable laws or regulations.

Acceptable Use of Service

You are fully responsible for your activities while using this Service (including for any content, information and other materials you access or transmit via this Service), and you agree not to use this Service to engage in any prohibited conduct. Broadly stated, prohibited conduct is any conduct that is unlawful, infringing, tortuous or that is harmful to (or puts at risk) Seton Hall University or any other party or property; that violates another party's intellectual property, privacy or other rights; or that otherwise interferes with the operation, use or enjoyment of any service, system or other property.

By continuing to use this Service, you agree to abide by Seton Hall University Appropriate Use and Technology Usage Policy.

As User of SHU Technology assets, I understand the above and will comply to the best of my ability.

Username: ____ *(please print)*

SHUID # ____ *(If Applicable)*

Sign and date: ____