

## **I.T. VPN Remote Access Policy**

Policy Number:

Owner Department: Information Technology Department

Approved/Effective Date: February 24, 2011

Approved By: President's Council

### **I. POLICY STATEMENT/PURPOSE**

Remote access to electronic information of Sonoran University computer resources must be secure and prohibit unauthorized access by using virtual private network (VPN) or similarly securable connectivity protocols. The purpose of this policy is to protect electronic information from being compromised by unauthorized remote access connections.

### **II. POLICY STATUS**

Revised (to new format)

### **III. HISTORY/BACKGROUND**

N/A

### **IV. DEFINITION(S)**

**Virtual Private Network:** a mechanism for creating a private computer communication or providing a secure extension of a private network into an insecure network such as the Internet or corporate network.

**Anti-Virus Definitions:** a file regularly updated by anti-virus companies to combat virus attacks. These files are automatically applied to computers with active fee-based subscriptions and employ multiple methods of virus detection analysis including signature-based, malicious activity, heuristic-based, file analysis, and file detection.

### **V. SCOPE/KEY STAKEHOLDERS**

The scope of this policy is to define appropriate VPN access and its use by authorized personnel. Employees and authorized third parties (customers, vendors, etc.) may use VPN connectivity to gain access to the Sonoran University network resources from off-site locations. Stakeholders are defined as staff and faculty permitted VPN access

### **VI. POLICY ITEMS**

- A. Access is strictly controlled, using network and password authentication.
  - a. Permission from the employee's Vice President is required for all VPN access.
  - b. Access is reserved for:
    - i. Employees that need 24-hour access to network resources.
    - ii. Employees required to work from an external location
- B. Employees with access privileges must ensure that the VPN connection to Sonoran University's network is not used by non- employees to gain access to any Sonoran University resources.
  - a. An employee who is granted access privileges must remain constantly aware that VPN connections between their location and Sonoran University are literal extensions of Sonoran University's network, and that they provide a potential path to the university's most sensitive information.
  - b. The employee and/or authorized third party individual must take every reasonable measure to protect Sonoran University's assets.
- C. Only Sonoran University configured laptops are considered secure enough for connection to Sonoran University's network.
- D. Users granted VPN access must comply with IT's accepted VPN access methods.
  - a. VPN software is setup and configured by IT.
  - b. Tampering or altering of the VPN client software will result in disciplinary action, up to and including revocation of VPN account privileges and disciplinary action up to and including employment termination.
  - c. VPN client software will not be installed on non- Sonoran University computers (no personal home computing devices will be accepted).
- E. Enforcement
  - a. Connection activity may be monitored. Unauthorized moving of files across the VPN that contain sensitive or private patient or student information will result in revocation of account access privilege OR extended disciplinary actions when warranted. Violations of this policy may be subject to disciplinary action, up to and including termination of employment.

## **VII. RESPONSIBILITY FOR IMPLEMENTATION**

Network Administrator

## **VIII. RELATED POLICIES**

IT Acceptable Use Policy

## **IX. RELATED DOCUMENTS**

Form: User/Employee Agreement for VPN Access

## **X. NEXT REVIEW DATE**

As needed

**XI. VERSION CONTROL AND CHANGE HISTORY**

Version Control	Approved By/Date	Date Effective	Amendment
1	President's Council/ February 23, 2011	February 24, 2011	
2			

**XII. POLICY AUTHOR/CONTACT**

Paul Collins – Senior Director of IT