California University of Pennsylvania
Pennsylvania State System of Higher Education

Technology Security Guideline Number 2011-01
Guidelines on Remote Network Access

Approved by: CITO

History: Issued 1/18/2011

Revised --

Additional History

Related Policies:

Additional References:

I. Introduction

These guidelines address the acceptable safeguards for use of privately owned and/or remote devices to access the California University of Pennsylvania network. A privately owned device is one that is not owned by California University of Pennsylvania that requires access to the network.

II. Guidelines

These guidelines apply to employees, students, or contractors who use privately owned devices to remotely access the California University of Pennsylvania network. This covers all forms of remote access including but not limited to: Access via Terminal Services (e.g., Citrix, Remote Desktop Protocol, and Virtual Private Network).

Please note that, although employees may request access for any privately owned device to remotely connect to the California University of Pennsylvania network, this in no way implies that the privately owned device will be supported by California University of Pennsylvania or connected directly to the California University of Pennsylvania network.

For instances when an employee uses a privately owned device to gain remote access to the California University of Pennsylvania network, the following guidelines apply:

- Anti-Virus (AV) software must be installed and kept current. If AV software is not already installed, it is recommended that employees utilize the AV software that may be made freely available to all employees. Patches and security updates must be kept current. For computers with a Microsoft operating system, it is recommended that the Microsoft Windows Update feature be configured to automatically receive and install updates.

- Employees who are working from any remote location must store and maintain all business-related data on the California University of Pennsylvania network. California University of Pennsylvania data should never be saved locally to a non-California University of Pennsylvania device. Confidential data should only be accessed on a California University of Pennsylvania provided encrypted device.

- "Public" and mobile devices (e.g., mobile devices and computers provided by libraries, universities, coffee shops, hotel business centers, etc. for general public use) should not be used to access confidential data on the California University of Pennsylvania network.

- If the personal computer used to remotely access the California University of Pennsylvania network is located on a home wireless network, then the wireless network should be secured based on industry best practices (renaming the default SSID and only allow authorized users to access your network and utilizing WEP/WPA encryption, etc.). For more information regarding wireless network security, please refer to *Securing Wireless Networks*, provided by the United States Computer Emergency Readiness Team (US-CERT), at the following location: http://www.us-cert.gov/cas/tips/ST05-003.html.

- Home users with a broadband connection are strongly encouraged to utilize a router, rather than connecting the computer directly to the Internet. Even low-end routers, which are often provided by many broadband ISPs, add Network Address Translation and firewall capabilities that provide a considerable amount of additional protection.