Employee Remote Access Standard

1.0 Reference

This standard supports Portland Community College (PCC)'s Privacy Policies, Oregon Identity Theft Protection Act, PCC Information Classification Standard and Virtual Private Network (VPN) Standard.

2.0 Overview

The equipment used to access PCC's network remotely could be inflected with computer viruses, worms, bots, etc. Once the compromised machine is connected to PCC's network, it can spread the inflection to other machines in the network and impair the ability for PCC to operate effectively. Additionally, unsecured communication while using remote access will allow another user to read data in transit which may contain personal and sensitive information.

3.0 Purpose

The purpose of this document is to define standards for connecting to Portland Community College's network from any host. These standards are designed to minimize the potential exposure to the College from damages which may result from unauthorized use of College resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PCC internal systems, etc

4.0 Scope

This standard applies to all Portland Community College employees, contractors, vendors and agents with a College-owned or personally-owned computer or workstation used to connect to the College network. Three basic types of remote access, whether fixed or mobile include:

- Travelling users (e.g. Staff working across campuses or are temporarily based at other locations)
- Home workers (e.g. Faculty and staff with work at home agreements)
- Non PCC staff (e.g. Contractors and other 3rd party organizations)

Remote access implementations that are covered by this standard include, but are not limited to, dial-in modems, remote desktop, WiFi, WiMax, DSL, VPN, Smart-phones, PDAs, "cloud computing," and cable modems, etc.

5.0 Standard

5.1 General

5.1.1 It is the responsibility of Portland Community College employees, contractors, vendors and agents with remote access privileges to the College's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Portland Community College.

5.1.2 The PCC employee bears responsibility for the consequences of their login credentials. At no time should any Portland Community College employee provide their login or email password to anyone, not even family members.

5.2 Requirements

5.2.1 PCC employees and contractors with remote access privileges must ensure that their PCC-owned or personal computer or workstation, which is remotely connected to the College's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

5.2.2 PCC employees and contractors with remote access privileges to PCC's network need to understand that unless specifically identified, PCC does not support third party applications and services.

5.2.3 Routers for dedicated lines configured for access to the PCC network must meet minimum authentication requirements of CHAP.

5.2.4 Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

5.2.5 Non-standard hardware configurations must be approved by Technical Services; also Technical Services must approve security configurations for access to hardware.

5.2.6 All systems that are connected to PCC internal networks via remote access technologies must use the most up-to-date security software and operating system patches installed.

5.2.7 Personal equipment that is used to connect to PCC's College's networks must meet the requirements of PCC-owned equipment for remote access. See the *Data Protection Guidelines -End Point Security*

5.2.8 PCC employees and contractors with remote access privileges to PCC's network must avoid downloading sensitive files to their personal computer or workstation unless there is an exceptional need.

6.0 Enforcement

Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment. Any non-PCC employee using PCC's network services found to have violated this standard may have their access terminated. Depending on circumstances, students may be subject to disciplinary action.

Any user who violates this standard may be held liable for damages to PCC assets, which may include and not be limited to the loss of information, computer software and hardware, lost revenue due to down time, fines and judgments imposed as a direct result of the failure of the user to adhere to this standard.

7.0 Definitions

Cable Modem: Cable companies such as Comcast Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Data breach: a deliberate or inadvertent unauthorized release of identifying information as the result of an error or deliberate penetration of a PCC system. A breach is a likely indicator of attempted identity theft.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Example: Being on a Portland Community College-provided Remote Access network, and connecting to another network, such as a spouse's remote access.

Remote Access: Any access to Portland Community College's network through a non-Portland Community College controlled network, device, or medium.

Security information: data the disclosure of which would likely substantially jeopardize the confidentiality of identifying information.

Smartphone: A smartphone is a mobile phone offering advanced capabilities, often with PC-like functionality (PC-mobile handset convergence). It is a miniature computer that has phone capability. Smartphones can have features like e-mail, Internet and e-book reader capabilities, and/or a built-in full keyboard or external USB keyboard and video connector. There is no industry standard definition of a smartphone.

Split-tunneling: Simultaneous direct access to a non-Portland Community College network (such as the Internet, or a home network) from a remote device (PC, PDA, smartphone, etc.) while connected into Portland Community College's network via a VPN tunnel.

WiFi: Term for wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."

WiMax: WiMAX is a wireless digital communications system, also known as 802.16, that is intended for wireless "metropolitan area networks". companies such as CLEAR provide Internet access over the Portland Metro area. WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100m).

***Virtual Private Network (VPN)*:** A technique of implementing secure connections over the public Internet through encryption and authentication schemes. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

8.0 Revision History

4rd draft revised Oct 23rd, 2009