TITLE: **IT Security Remote Work Procedure**
NUMBER: **751**
AUTHORIZED BY PRESIDENT: **3/30/2021**

1.0 PURPOSE

Remote working conditions offer unique challenges and concerns, which require additional security precautions and communication tools to navigate. The purpose of this procedure is to outline required security measures that employees must take to secure Whatcom Community College (WCC) IT equipment and data when working remotely and what additional assistance they can expect from the College.

2.0 SCOPE

This procedure applies to employees who work primarily from any location other than WCC campus. All other WCC policies, procedures, and state or federal laws must be followed when working remotely in addition to this procedure. Failure to adhere to these guidelines may result in loss of information access privileges.

3.0 PHYSICAL EQUIPMENT SUPPORT

WCC Owned Technical Equipment: Equipment owned by the college may be checked out to an employee when needed. In the event of an equipment failure or malfunction, it is the responsibility of the WCC IT department to repair or replace the equipment.

Employee Owned Technical Equipment: An employee may elect to take advantage of cloud resources offered by the College from a personally owned computer. In the event of an equipment failure or malfunction, it is the responsibility of the employee to repair or replace their personally owned equipment.

4.0 SECURITY

Employees conducting college business remotely must connect to secure Wi-Fi. If an employee cannot password protect their home network, they may not conduct college business from that network. WCC can provide cellular devices for checkout that can serve as an employee’s internet connection if approved by their vice president. WCC will not pay for an internet connection to an employee’s home. Alternatively, an employee could choose to save work to a WCC owned, encrypted storage device.

If an employee is viewing or editing WCC data from their own computer and not through VMware, the computer must have a supported operating system and antivirus with up-to-date malware definitions. If the computer doesn’t meet these basic security requirements, it poses an unacceptable risk to the College and the employee may not conduct WCC business from that computer. Instead, the employee can check out a laptop from WCC, or use VMware, to use a WCC supported desktop and applications.

Employees must log off to prevent unwanted access by others when not actively working in VMware. Computers must be locked to prevent unwanted access by others when employees are not actively working. WCC-owned devices must be physically secured unless they are actively being used. Equipment will not be left in a vehicle, even if it is locked. If equipment must be left in a vehicle, it cannot be visible to the public and the vehicle must be locked.

4.1 SEGREGATION OF DATA

Personal data will be kept separate from WCC data at all times. WCC equipment will not be used for personal internet surfing, installing of employee owned software, or personal data storage, unless considered de minimis as defined in WAC 292-110-010. Any data generated by employees or existing on WCC-owned equipment is property of WCC and is subject to public records requests (Public Records Act, 1972). Employees will not store WCC data on personal devices. If employees need to access WCC data or information systems from a personal computer and an internet connection is available they should use VMware to conduct business. If no internet connection is available, all WCC data will be stored in a separate location from personal data (i.e. an encrypted USB drive) and be copied back to the WCC network (My Documents, Desktop, Burrows folder or other folder) to meet backup, archiving, and e-discovery requirements as soon as possible.

5.0 REMOTE WORK TOOLS

Remote working tools are provided and institutionally supported by the College. Primary tools used for remote work include, but are not limited to:

5.1 VMware

To access files and other software necessary to operate normally, an employee can access a virtual desktop by going to https://desktop.whatcom.edu. If documents or applications are not available via the virtual desktop, employees should contact the helpdesk (360-383-3420 or helpdesk@whatcom.edu) and they will help resolve technical issues.

5.2 CANVAS

To support teaching and learning at Whatcom Community College, employees can take advantage of our learning management system, Canvas. Employees can post information, assignments, quizzes, videos, and more for students, faculty, and staff. Canvas is the primary tool used to support online instruction. Faculty are encouraged to use Canvas to communicate regularly with students by using announcements, conversations, and posting assignments. The WCC Canvas Training shell is for employees who want to learn more about the functionality of Canvas.

5.3 ZOOM

To facilitate remote communication, employees may request a Zoom account. If an employee chooses to participate in a screen-share while conducting a Zoom conference, their desktop will be clear of sensitive information and their email client should be closed to prevent unintended sharing of confidential information. If an employee chooses to participate in a video conference call, they will ensure their surroundings are clear of sensitive information (i.e. no confidential information is written on whiteboards or posted on corkboards in the background of the video). Alternatively, an employee could use a Zoom background to obscure their surroundings. For best performance, Zoom should not be used via VMWare, but from the local computer.

5.4 JABBER

Jabber is a software based remote telephone that will run on a computer or smartphone. It is connected to the College's phone system; and, therefore callers are not aware that an employees is off campus or of an employee's personal phone number. To facilitate remote communication, some employees and departments will be authorized to use Jabber.

Related Policies and Procedures

Procedure 1189	Use of College Computing Resources
WAC 132U-276 (Policy 2150)	Access to Public Records and Documents at Whatcom Community College
WAC 292-110-010	Use of state resources