Policy

Title:	**Virtual Workplace Technology**
Effective Date:	February 16, 2022
Approved By:	President's Council
Responsible Party:	Chief Information Officer
History:	8/21/17; 6/30/20;

I. PURPOSE

Salus University permits faculty and staff to work virtually, using personal and university provided computers. Such permission may include:

- the issuance of a university-provided laptop;
- the use of web-based applications;
- the use of downloaded software; and/or
- the provision of network access from physically remote locations.

Working remotely can create additional technology risks that must be taken into consideration. This policy is provided to allow Salus to appropriately handle these risks.

II. POLICY

The appropriate technology shall be provided to those individuals designated to work remotely who have a demonstrable university need.

III. PROCEDURE

1. Technology needs may be requested through an individual's supervisor and the help desk by submitting a help ticket.
2. If approved, a university-provided laptop shall be configured with the requested and approved software and network access. Individuals are responsible for damage or loss to their university provided laptop, ordinary wear and tear excepted. Without the permission and/or assistance of the help desk, individuals are not to reconfigure their university-provided laptop, modify or delete any pre-loaded software or to download any additional software.
3. The use of web-based applications, such as Blackboard, Panopto and NextGen RDGateway do not require preapproval or any additional technology beyond a web browser.
4. If approved, any software to be downloaded on an individual's personal computer, may be downloaded by the individual or, if possible, the help desk will coordinate the download. If

the individual downloads the software, the individual shall pay for the software and submit for expense reimbursement (or may use a university-issued credit card). Individuals waive any claims they may have against the university due to loss of files from, or inadvertent functionality issues caused to, their personal computers as a result of downloading software for approved university use.

5. If approved, remote access via an individual's personal computer shall be arranged by the help desk. Individuals waive any claims they may have against the university due to loss of files from, or inadvertent functionality issues caused to, their personal computers as a result of providing remote access. Upon request, the university reserves the right to inspect personal computers that are being used to initiate remote access connections. Such inspections will be limited to verifying that such personal computers are using appropriate protections, including but not limited to running current anti-virus protection and having a properly configured personal firewall. If a personal computer does not meet the university standards, remote access will not be permitted.

6. Individuals are responsible for the use of the remote access issued to them, and are required to take reasonable precautions to prevent unauthorized use of their remote access. These precautions should include measures to avoid damaging or compromising Salus' information assets. For instance, avoiding the use of software or other networks that may introduce computer viruses into Salus' network. For help with determining appropriate use, users should contact the help desk.

   During the initiation of a remote access session, the individual will be required to provide verification credentials. These credentials are university property and are issued to the individual for approved university purposes only.

   Individuals shall not share, lend or give their credentials to, or allow the use of their remote access by any other person

   Individuals shall not attempt to reconfigure, disable or otherwise change any software or configuration settings associated with establishing or using remote access unless instructed to do so by the remote access support team.

   Remote access uses encryption technologies. These and other technologies may be restricted or prohibited in foreign countries, and may result in confiscation of the computer on which the software resides. Criminal action may also result. Before travelling internationally, individuals shall contact the help desk to disable remote access.

   If unauthorized use is suspected or if their credentials are suspected lost or stolen, individuals are required to immediately report the situation to the help desk.

   The university reserves the right to monitor remote access use, and to restrict or deny access at any time and for any purpose.

IV. ACCOUNT TERMINATION

1. **User VPN Account access may be temporarily or permanently suspended based upon any or all of the following best practice(s) criteria:**
    a. **User no longer requires VPN access to perform their job duties.**
    b. **Employee termination, resignation or leave of absence.**
    c. **Continued user access has identified potential risk(s) to Salus University electronic assets and resources.**
    d. **User has violated the Electronic Usage Policy.**
    e. **Ninety (90) days of inactivity on the VPN user account, resulting in temporary disabling of VPN access and further review.**