Policy

Title:	**Remote Access Policy**
Effective Date:	August 21, 2017
Approved By:	Chief of Staff
Responsible Party:	Chief Information Officer

I. PURPOSE

Salus University provides network access for faculty and staff from physically remote locations (remote access). Remote access is provided so that university activities can be performed without requiring the employee to be at specific geographical locations. By providing remote access, there are additional risks that must be taken into consideration that exist outside of the university network campus. This policy is provided to allow Salus to appropriately handle these risks.

II. POLICY

Remote access is reserved for those individuals who have a demonstrable university need for such access. Only those services approved by the University will be provided via remote access.

III. PROCEDURE

1. Remote access can be arranged for by contacting the help desk at extension 1444. The help desk will require access to the approved individual's university-issued or personal computer, as applicable, to install remote access capability. 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 granting such university access.
2. 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.
3. During the initiation of a remote access session, the individual will be required to provide verification credentials. These credentials are the property of Salus 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.

4. 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.
5. 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.
6. Upon request, Salus reserves the right to inspect computers that are being used to initiate remote access connections. Such inspections will be limited to verifying that such computers are using appropriate protections, including but not limited to running current anti-virus protection and having a properly configured personal firewall. If a computer does not meet Salus' standards, remote access will not be permitted.
7. Salus reserves the right to monitor remote access use, and to restrict or deny access at any time and for any purpose.