Policy	Remote Access Guidelines
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	February 11, 2019
Reviewed	June 23, 2025
Approved by	VP for Finance and Administration
Version	25.1

WORK from HOME & REMOTE ACCESS GUIDELINES

PURPOSE

Remote access to Shepherd University networks and/or IT resources is often necessary to maintain employee and/or student productivity, but in most cases, remote access will originate from external networks that operate at a significantly lower security posture than Shepherd University's campus network. Everyone needs to take an equal part in helping to minimize and mitigate external risks.

The purpose of this guideline is to define rules and requirements for connecting to Shepherd University's network from any external host; from off-campus; or, outside of the campus network. These rules and requirements are designed to minimize the potential exposure to Shepherd University from damages which may result from unauthorized use of Shepherd University IT resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical Shepherd University internal systems, and fines or other financial liabilities incurred as a result of those losses.

This guideline applies to all Shepherd University users, including students, faculty, staff, and agents operating on behalf of Shepherd University on a university owned device or a personally owned computing devices used to connect to the Shepherd University network or internet resources. This guideline applies to remote access connections used to do work on behalf of Shepherd University, including reading/sending email, accessing core network and/or data systems, use of the virtual desktop infrastructure (i.e. Citrix), and viewing of any Shepherd University IT resources from home. This guideline covers all technical implementations of remote access used to connect to Shepherd University networks.

GUIDELINES

It is the responsibility of all Shepherd University users, including students, faculty, staff, and agents operating on behalf of Shepherd University, with remote access privileges to Shepherd University's campus infrastructure network, to ensure that their remote access connection is given the same consideration as the user's on-site connection at Shepherd University.

When accessing the Shepherd University network from a personally owned computing device, all users are responsible for preventing access to any Shepherd University IT resources, including data, by nonauthorized users. Performance of illegal activities through the Shepherd University network by any user (Authorized or otherwise) is prohibited, as outlined in BOG Policy #35 as well as the Acceptable Use Policy. Users assume the responsibility for any affiliated consequences of misuse of the campus network by usage of remote access. For further information and definitions, see the Acceptable Use Policy.

Employees who have not been issued a Shepherd University owned computer are responsible for ensuring that they have the proper IT approved software/hardware technology to perform their job duties from a remote location on a personally owned computing device. These devices may include, but are not limited to, computer, tablet, telephone, and peripherals (e.g. monitor, docking station, keyboard, mouse, headset, etc.). Equipment supplied by the employee, will be maintained by the employee. Shepherd University accepts no responsibility for damage or repairs to employee-owned equipment. Shepherd University reserves the right to make alterations to standards and/or determinations as to what qualifies as appropriate equipment, subject to change at any time. Equipment supplied by Shepherd University is to be used for university purposes only. Upon termination of employment, all Shepherd University property will be returned to Shepherd University, unless other arrangements have been made in writing and approved by the employee's Executive sponsor.

All employees will establish an appropriate work environment that is to be utilized at home or remote for school/work purposes. Shepherd University will not be responsible for costs associated with the setup of employee's home office and/or modifications to the employee home office space, network connectivity, or affiliated non-Shepherd approved/utilized software.

For additional information regarding Shepherd University's remote access connection options, including how to obtain a remote access login, anti-virus software, troubleshooting, etc., please visit the Shepherd University IT Services website.

REQUIREMENTS

- Secure, remote access must be strictly controlled with strong, data-encryption (i.e. Virtual Private Networks) and strong passwords/phrases.
- Users shall protect their username and passwords, even from family members, and will not share their login credentials with any other authorized or unauthorized user.
- While using a Shepherd University's owned computer to remotely connect to Shepherd University's network, users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct Shepherd University's operational, scholarship, research or other university business must be approved in advance.

- All hosts that are connected to Shepherd University's internal networks via remote access technologies must use up-to-date anti-virus software, exhibit regular software patches to vendor supported operating systems, and ensure secure connections whenever possible.
- Other personally owned equipment used to connect to Shepherd University's networks must meet the requirements of Shepherd University's owned equipment for remote access.
- Users shall enable a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Lost or stolen Shepherd University computing devices must be reported immediately by using the Incident Management reporting process.
- Store all Shepherd University resources, data, and documents in an approved Shepherd University location (ex: network shared drives, Microsoft OneDrive, or personal M drives on the Shepherd University network), as outlined in the Acceptable Use Policy.
- Storing any Shepherd University data and/or sensitive information, including protected, private, and nonpublic information on a local, personal computing device, storage array, personal cloud service is strictly prohibited, as outlined in BOG Policy #35 and the Acceptable Use Policy.
- Users need to consider securing Shepherd University owned laptops with the use of cable locks or locking laptops in drawers or cabinets when not in use.
- Users are encouraged to leverage the use of adequate surge protection.
- Wireless infrastructure devices that provide direct access to the Shepherd University network, must enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAPTLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point

SCOPE of AFFECTED PARTIES

These guidelines apply to all users, such as students, faculty, and staff of Shepherd University and to other persons accessing Shepherd University information assets and/or IT resources including but not limited to authorized agents or community members, regardless of whether such information asset or IT resource is accessed from on-campus or off-campus.

ROLES & RESPONSIBILITIES

All Shepherd University students, faculty, staff, and other parties with access to Shepherd University information assets and IT resources shall be responsible for:

USERS

- Adhere to these guidelines, as well as operate in compliance with all applicable laws and Shepherd University policies, standards, guidelines, regulations, and procedures.
- Physically secure and safeguard Shepherd University IT resources and/or affiliated data within the user's possession and control, including abiding with the safe handling of data.
- Report promptly to itworkorder@shepherd.edu any issue with a user's account, IT resource, or to report a lost/stolen Shepherd University owned computing device.

CIO/CISO - INFORMATION PRIVACY OFFICER

- Ensure compliance with the utilization of tools, reports, inspections, audits, to confirm users are abiding to these guidelines.
- Provide authorization and direction to IT Services staff in accordance with these guidelines.

- Develop awareness and necessary training materials as it pertains to these guidelines.

IT SERVICES STAFF

- With appropriate authorization, take directed action in accordance with these guidelines to preserve, secure, and protect the interests of Shepherd University.
- Ensure all associated procedures are followed and documented accordingly when taking any actions outlined in these guidelines.

RELATED TOOLS

RELATED POLICIES

- BOG#35: Information Technology Security
- Acceptable Use Policy
- E-mail
- Information Security & Privacy Policy
- Social Security Number Guidelines
- Work from Home / Remote Access Guidelines