# 8.2.2 Remote Access Standard

I. Purpose:

Remote access to the University of Oklahoma (OU) network is essential to maintain productivity and support University missions. Remote access provides a way for university users and support staff to share screens, access Information Technology (IT) services from home, and vice versa. Remote access is defined as access to "non-public" University Information and IT services from outside of the University's hard wired and/or wireless networks. Remote access tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the University's network that can be used for theft of, unauthorized access to, or destruction of assets.

The purpose of this standard is to define the security controls required for deploying and using remote access tools.

II. Scope:

This policy applies to:

- All University staff, faculty, students, contractors, vendors, and agents with remote access privileges.
- All remote access connections used to do work on behalf of the University, including reading or sending email and viewing web resources.
- All technical implementations of remote access used to connect to university networks.

III. Accountability:

This standard is approved and enforced by the Chief Information Officer (CIO). Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this Standard. IT Security Exception requests can be submitted at https://itsupport.ou.edu, search for IT Security Exception. Exceptions require the approval of the the Cybersecurity and Infrastructure Advisory Council depending upon the level or risk introduced with the exception.

IV. Standard:

| REMOTE ACCESS MATRIX | | | | | | | |
|---|---|---|---|---|---|---|---|
| SERVICE/SOLUTION | OU VPN | OU VDI | RDP | SSH | Zoom | Bomgar | RemotePC |
| STUDENT USE | Yes | Yes | No | No | No | No | No |
| STAFF & FACULTY USE | Yes | Yes | No | No | No | No | No |
| RESEARCH AND LAB USE | Yes | Yes | Yes | Yes | No | No | No |
| STUDENT LAB ACCESS | Yes | Yes | Yes | Yes | Yes | No | Yes |
| IT REMOTE SUPPORT | Yes | Yes | No | No | Yes | Yes | No |
| DEVICE ADMINISTRATION | Yes | Yes | Yes | Yes | Yes | No | No |
| THIRD PARTY/VENDOR | Yes | Yes | Yes | Yes | Yes | No | No |
| SUPPORTED BY OU IT | Yes | Yes | No | No | Yes | Yes | No |

1. **Remote Access Security:** IT must establish good practices for secure remote access to reduce the risk of information or information resource compromise. Secure practices include but are not limited to:

1. Remote access services must authenticate to OU Authentication services (e.g., Single-Sign-On, Lightweight Directory Access Protocol [LDAP], or Federated Authentication).
2. All remote access must utilize OU Multi-Factor authentication.
3. All remote access firewalls must send logs, including all authentication logs, to the OU IT central log repository for monitoring.

2. **OU Virtual Private Network (OU VPN):** Staff, faculty, students, contractors, vendors, or agents must use one of the OU VPN options to access protected on-campus resources. The OU VPN service is available for Microsoft and macOS systems.

   1. Protected On-Campus Resources
      The list below provides a sample of systems considered to be protected.
      Norman Campus
      - ❑ Laserfiche
      - ❑ CQ5 Content Management System
      - ❑ PeopleSoft Admin tools
      - ❑ Virtual Labs
      - ❑ Network file shares
      - ❑ Certain licensing servers

Health Sciences Center Campus

- ❑ EMR
- ❑ GE Centricity Business
- ❑ Peoplesoft Admin tools
- ❑ Network file shares

Tulsa Campus

- ❑ Peoplesoft Admin Tools

Network file share**VPN Services**

**ouvpn.ou.edu**
OU VPN for Norman campus staff, faculty, students, contractors, vendors, or agents.

**connect2.ouhsc.edu**
OU VPN for Health Sciences Center staff, faculty, students, contractors, vendors, or agents.

**vpn.tulsa.ou.edu**
OU VPN for Tulsa Health Sciences Center staff, faculty, students, contractors, vendors, or agents.

**soonervpn.tulsa.ou.edu**
OU VPN for Tulsa campus staff, faculty, students, contractors, vendors, or agents.

3. **OU Virtual Desktop Infrastructure:** The OU VDI delivers a clean desktop with secure, encrypted access to network services. Use OU VDI to access protected, on-campus applications using a secure, encrypted virtual desktop while using personally owned devices that do not meet University security standards are while accessing web-based resources from the public Internet.

   **mydesk.ou.edu**
   Users can connect to a virtual desktop and University applications by using a VMWare Horizon Client or through the web browser. The VMWare Horizon Client offers better performance and features.
4. **Zoom:** Zoom is a communications software that combines video conferencing, online meetings, chat, and mobile collaboration. Zoom delivers the ability for any user to leverage Zoom's meeting features to establish a remote support session. Zoom remote support sessions allow the meeting host to remotely control and restart a Windows or macOS computer.

   All faculty, staff, students, and affiliates receive a Zoom Pro Licensed account.

   **oklahoma.zoom.us**
   Zoom for Norman and Tulsa campus faculty, staff, students, and affiliates.
5. **Secure Shell (SSH):** SSH is a network protocol that provides administrators with a way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol. SSH remote access is accessible from the OU IT VPN or OU VDI.

   **SSH Remote Access**
   Using SSH public key authentication to connect to a remote system is a robust, more secure alternative to logging in with an account password or passphrase. SSH public key authentication relies on asymmetric cryptographic algorithms that generate a pair of separate keys (a key pair), one "private" and the other "public". You keep the private key a secret and store it somewhere secure. Conceivably, you can share the public key with anyone without compromising the private key; you store it on the remote system in a .ssh/authorized_keys directory.
   - ❑ Windows: Use the PuTTY SSH client. Download and install PuTTY for free from the PuTTY download page.
   - ❑ macOS and Linux: Use OpenSSH, a suite of command-line SSH tools integrated with macOS (accessible from the Terminal) and most Linux operating systems.

   **Encryption Key Management**
   Always keep the private key stored somewhere secure.
   - ❑ Encrypted USB: You can store the private key offline by using an encrypted USB drive. Use hardware encrypted USB drives for Category D1 data.
   - ❑ LastPass: You can store the private key in your OU LastPass account for Category D2 and F data.
   - ❑ CyberArk: You can store data center server private keys in the OU CyberArk service for Category A, B, C, and E data.

6. **Microsoft Remote Desktop (RDP):** Remote Desktop allows users to connect to a computer located on the OU network. Remote Desktop access is accessible from the OU IT VPN or OU VDI.
7. **OU Bomgar:** Bomgar is a third-party hosted remote support tool, managed and maintained by the Office of Information Technology, that allows administrators to support all their systems over the web, even if they are behind firewalls outside of their control. Bomgar provides remote control and screensharing, unattended access (for an additional license fee), file sharing and camera sharing. Bomgar works across Windows, MacOS, Linux, Android, and iOS, and ChromeOS. Request access to use Bomgar at https://itsupport.ou.edu.
8. **RemotePC:** RemotePC is a third-party hosted remote access tool, managed and maintained by the Office of Information Technology, that can be used to permit remote access to:
    - Software that requires a dedicated graphics processing unit (GPU).
    - Processes that require high video frame rate speeds.

    RemotePC works across Windows, MacOS, and Linux. Request access to use RemotePC at https://itsupport.ou.edu.

V. References

- National Institute of Standards and Technology Cybersecurity Framework (CSF), PR.AC-3
- National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information: 3.1.1, 3.1.2, 3.1.15, 3.1.14, 3.1.18, 3.1.20, 3.13.9, 3.13.12
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Security Rule §164.308(a)(4), 164.308(b)(1), 164.312(a)(2), 164.310(b), 164.310(c)
- National Institute of Standards and Technology Special Publication 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems, AC-17, AC-19, AC-20
- Payment Card Industry (PCI) Data Security Standards
- OU Cybersecurity Policy
- OU Information Classification Standard

| | |
|---|---|
| Policy Level: | Information Technology |
| Approval Authority: | Chief Information Officer |
| Date of Approval: | March 15, 2023 |
| Subject Matter: | Remote Access |
| Date of Last Review: | March 7, 2023 |
| Date of Next Review: | March 7, 2025 |
| Signature: | |