OSU INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES

Remote Access Control	**6-010** **TECHNOLOGY SERVICES** **June 2021**

OVERVIEW

1.01 Remote access to OSUIT’s university network is essential to maintaining our stakeholders’ productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our university network. While these remote networks are beyond the control of OSU Institute of Technology (OSUIT) policy, we must mitigate these external risks the best of our ability.

PURPOSE

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

SCOPE

3.01 This policy applies to all OSUIT employees, students, contractors, vendors, and agents with an OSUIT-owned or personally owned computing device used to connect to the OSUIT network. This policy applies to remote access connections that access the OSUIT or OSU System networks. This policy covers all technical implementations of remote access used to connect to OSUIT networks.

POLICY

4.01 It is the responsibility of OSUIT employees, students, contractors, vendors, and agents with remote access privileges to OSUIT's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to OSUIT.

4.02 General access to the Internet for recreational use through the OSUIT university business network is strictly limited for OSUIT employees, contractors, vendors, and agents (hereafter referred to as “Authorized Users”). When accessing the OSUIT network from a personal computer, Authorized Users are responsible for preventing access to any OSUIT computer resources or data by non-Authorized Users. Performance of illegal activities through the OSUIT network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the OSUIT *6-001 Appropriate Use of Digital Technology Resources*.

4.03 OSUIT provides mechanisms to collaborate between internal users, with external partners, and from non-OSUIT systems. The only approved software for remote access are Microsoft Remote Desktop, DUO multifactor authentication, and OSU Cisco VPN. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

4.04 Secure remote access must be strictly controlled using encryption via Cisco VPN, O-Key credentials, and multifactor authentication. For further information see the *Acceptable Encryption Policy* and the *User Password Creation Policy*.

4.05 Authorized Users shall protect their login and password, even from family members.

4.06 While using a OSUIT-owned computer to remotely connect to OSUIT's university business network, Authorized 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.

4.07 Use of non-university owned resources to conduct OSUIT business must be approved in advance by Technology Services and the appropriate OSUIT supervising leader.

4.08 All hosts that are connected to OSUIT internal networks via remote access technologies must be fully patched with up-to-date patches and anti-virus software.

COMPLIANCE POLICY

5.01 Compliance Measurement
Technology Services will verify compliance to this policy through various methods, including but not limited to periodic visual inspection, scanning tool reports, and internal and external audits will provide feedback to the appropriate university leaders.

5.02 Exceptions
Any exception to the policy must be approved by the AVP of Technology Services in advance.

RELATED STANDARDS, POLICIES, AND PROCESSES

Please review the following policies for details of protecting information when accessing the university network via remote access methods, and acceptable use of OSUIT's network:

- *Appropriate Use of Digital Technology Resources*
- *User Password Creation Policy*

- *Network Security*
- *Network Devices*
- *Data Stewardship*
- *Access Control*

Approved:
Policy and Procedures Committee, 6/16/2021
Effective date: 6/16/2021