Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Updates Made By</th>
<th>Updates Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>03/17/2020</td>
<td>IT GRC</td>
<td>Creation of document</td>
</tr>
</tbody>
</table>

Overview

The University of Oklahoma (OU) permits staff and faculty the ability to work remotely in support of University business processes. Individuals who are authorized to perform tasks remotely, on behalf of OU, must comply with the specific Rules of Behavior (RoB) listed below.

All individuals granted remote access, must read and acknowledge the Remote Access Rules of Behavior. This acknowledgement must be completed annually thereafter, should remote services be required. By connecting to OU Remote Access Services, users reaffirm their knowledge of, and agreement to adhere to, the Remote Access RoB. The Remote Access RoB may be presented to the user in hardcopy or electronically.

The Remote Access RoB cannot account for every possible situation. Therefore, where the Remote Access RoB does not provide explicit guidance, users must use their best judgment to apply the principles set forth in the RoB for ethical conduct to guide their actions.

End User Responsibilities

A. You have no reasonable expectation of privacy regarding communications or data transiting or stored on OUP Information Systems, including communications or data allowed for limited personal use. At any time, and for any lawful University purpose, the University may monitor, intercept, and search any communication or data transiting or stored on OUP Information Systems may be disclosed or used for any lawful University purpose. Unauthorized or improper use of OUP Information Systems may result in disciplinary action up to and including removal of access.

B. All Individuals:
   a. Must comply with all OU Policies and Standards as implemented.
   b. Must use OU Information Systems for lawful, official use, and authorized purposes only, with limited personal use permitted.
c. Must protect all privileged user account passwords, passcodes, Personal Identity Verification (PIV), personal identification numbers (PINs), etc. from unauthorized use, disclosure, or access.

d. Must secure all OU data in all areas and in any form (e.g. digital, paper, etc.), to include mobile media and devices that contain OU data, and ensure that all OU data is encrypted using FIPS 140-2 approved encryption.

e. Must properly dispose of OU data, in either hardcopy, softcopy or electronic format in accordance with the *Electronic Data Disposal and Reuse Policy*.

f. Must ensure that Remote Desktop Protocol (RDP) Sessions are locked or logged off before walking away and will not allow another user to access that RDP Session while an individual is logged on to it.

g. Must not share privileged account access, passwords, PINs with anyone.

h. Must not install or remove any system hardware or software, or modify any system setting that has not been reviewed or approved in accordance with the *Information Security Risk Assessment Policy*.

i. Must not provide anyone (including yourself) with privileges or access greater than is necessary to accomplish assigned roles and responsibilities.

j. Must not delete or modify audit logs, or prevent the auditing of privileged actions.

C. Physical Security

- Individuals must take personal responsibility for the security and protection of equipment provided to them, the systems they access, and the information contained on those systems while conducting remote administrative tasks.

- Access to endpoints authorized users only.

D. Acceptable Use

- Remote access into OU Information Systems is granted for OU Information Systems only.

- Remote access into OU Information Systems must be from authorized endpoints, complying with OU Minimum Baseline Configuration or Portable Device Baseline Configuration expectations. This includes, but is not limited to:
  - Protection from malicious software using OU Campus Approved AV (McAfee or Dell Data Protection);
  - Protection from unauthorized disclosure of information subject to regulatory or privacy requirements, by employing full disk encryption of all devices used to initiate remote access sessions with OU Information Systems;

- Remote access into OU Information Systems must use an approved OU Remote Access Service that includes:
  - OU Virtual Private Network (VPN);
  - OU Virtual Desktop Infrastructure (VDI);
  - Web-accessible Information Systems (HTTPS); and
  - OU Bomgar Remote Support
• Use of OU endpoints must not be shared with non-OU individuals.

• OU data must be stored in an OU data storage location, and not on an administrative (personal) endpoint. Services available for storage include:
  • OU Network Storage, requires VPN
  • OU Sync & Share, requires internet access only
  • OU Office 365 (OneDrive and DropBox), requires internet access only and is not suitable for regulated or privacy data

E. Incident Response

Remote access users must report the following types of event, when conducting remote access, to the Director of IT Governance, Risk, and Compliance (IT Security GRC) at grc@ou.edu:

• Any event in which access to OU data has been gained by an unauthorized person,

• Any event in which a device containing OU information has (or might have been) lost, stolen or infected with malicious software (viruses, Trojans, etc.),

• Any event in which an account belonging to a person that has access to the data might have been compromised or the password shared with an unauthorized person (responding to phishing emails, someone shoulder surfing and writing down your password, etc.),

• Any attempt to physically enter or break into an area where OUP data is or might be stored,

• Any other event in which OU data has been or might have been lost or stolen, and

• Any event in which OU IT information security policies, standards, or practices are violated.