|  |  |
| --- | --- |
| **[Insert Practice Name]** | Approval Date: \_\_\_\_\_\_\_   Revision Date/No: \_\_\_  Approval Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Policy Name: Remote Access to [Insert Practice Name]  Information Systems Policy Number: Admin - 105 | Page **1** of **3** |

# Purpose

* To promote effective provision of high-quality care by expanding the range of settings in which staff members can perform their duties.
* To define requirements for connecting to **[Practice Name]** IT systems from a remote host and to assist users in following proper and secure remote access usage and practices in order to comply with applicable privacy and security requirements.

# Definitions

O365 - a suite of applications offered by Microsoft to support Microsoft Office applications in a distributed and remote work environment.

# Scope

This policy applies to all **[Practice Name]** employees, contractors, vendors, and agents using any computing device to remotely connect to [Practice Name]’s IT systems or network for the purposes of doing work on behalf of **[Practice Name]**, including reading or sending email and viewing intranet web resources.

# Procedures

* + **[Practice Name]** IT will provide reliable and secure remote access to [Practice Name] IT systems and provide detailed standards and configuration information for remote access users.
  + Remote access users must use only [Practice Name] IT–approved remote access methods.
  + Remote access users will comply with all policies that apply to **[Practice Name]** computing practices while connected to [Practice Name] IT systems. Key points of compliance include:
    - Safe computing practices
    - Appropriate system and Internet use
    - Preventing unauthorized network access and data transfer
    - Protecting patient confidentiality and privacy
  + Remote access devices are to be used only by the approved user and not by family members, friends, or other persons while any remote access sessions are in progress.
  + Remote access privileges will be granted, maintained, and revoked based on continuing need.
  + Remote access may be terminated without warning if **[Practice Name]** management or IT determines there is a risk to the confidentiality and/or integrity of the data or network environment.

# Remote Access Methods

There are three standard methods of remote access to **[Practice Name]** IT systems:

* + **Outlook Webmail** – this method utilizes a web browser to securely connect to **[Practice Name’s]** O365 email server.
  + **Virtual Private Network (VPN) client** – this method utilizes a VPN client to connect to **[Practice Name’s]** IT systems over an encrypted virtual private network. It can provide access to all or a subset of [Practice Name] IT systems.
  + **WebEx, Live Meeting, & Similar –** these methods enable the user to participate in live web- based meetings. Because they are not HIPAA compliant the user must determine, before the

meeting begins, that no PHI will be presented or discussed. If PHI is presented, the user must terminate the meeting as soon as possible.

# Remote Access System Requirements

Remote access users accessing **[Practice Name]** IT systems with a VPN client must configure their host as follows while connected to the **[Practice Name]** network:

* + Install and maintain a current operating system set to apply all operating system updates regularly.
  + Install, use, and maintain current antivirus software and definitions.
  + Disable peer–to–peer software.
  + Disconnect from all networks other than the user’s ISP.

# Remote Access Approval Process

* + The individual requesting remote access completes the **[Practice Name]** Remote Access Request Form (Admin – 136 F) and submits it to the administrator.
* As part of the application, the individual requesting remote access will supply a photograph of the intended location, demonstrating a secure work environment.
  + The administrator has final approval relating to all remote access requests.
  + Related paperwork is retained electronically in the user’s employee file or contract file as

appropriate.

# Safe Computing Requirements

Remote access users accessing **[Practice Name]** IT systems much to use the following safe computing practices always in addition to all other **[Practice Name]** policies that apply to **[Practice Name]** computing practices.

* + Remote access devices must always use up-to-date approved antivirus protection.
* Antivirus protection must run in real time.
* Antivirus library definitions must be updated at least daily.
* Antivirus full scans must be performed at least on a weekly basis and any time the [Practice Name] administration or IT support announces a major threat risk.
  + Remote access PCs must:
* Have current, updated protection for spyware and malware.
* Have current operating system updates and patches applied regularly.
* Turn on web browser pop-up blocking.
  + Remote access users may only use devices that follow these safe computing requirements. No other devices may be used. Public PCs and public Internet access devices are specifically prohibited.
  + Passwords and/or PINs should never be written down or stored on the remote access device in an unencrypted format.
  + The remote user will adhere to standard [Practice Name] policy about password changes and strength.
  + Remote access users are prohibited from personal and recreational computer use while connected remotely to **[Practice Name]** IT systems and networks. Recreational computer use includes any Internet activity such as personal email, social networks, Internet gaming, etc.
  + Remote access devices should be disconnected from **[Practice Name]** IT systems and networks before being left unattended.
  + Installation and use of un-trusted software should be avoided.
  + Remote access devices network capabilities, such as Bluetooth, must be deactivated when in public areas.
  + No PHI or **[Practice Name]** confidential or trade information may be stored locally on the remote access device or on removable media such as flash drives or CDs.
  + PHI or **[Practice Name]** confidential or trade information printed on a remote access device must be handled, stored, and disposed of according to **[Practice Name]** HIPAA privacy guidelines.
  + Installation or use of pirated, reverse engineered, or otherwise illegal software is strictly prohibited.
  + The remote access user must take all reasonable precautions to prevent others from viewing PHI or confidential trade or operational information.

# References / Citations [complete per practice HIPAA policies]

* + **[Practice Name]** HIPAA Privacy Policy
  + **[Practice Name]** HIPAA Security Policy
  + Admin 109 – Passwords
  + Admin 107 – Destruction of Devices Containing PHI
  + Admin 110 – Physical Security of Devices Holding PHI

**CREDIT STATEMENT**

The Remote Access Policy was adopted from policies provided by:

* Peter D Berger, MBA, Administrator, Orion Eye Center, LLC, Redmond, Oregon.

