Disclaimer: The purpose of this document is to support compliance with the UB Minimum Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices, section *2.7 Limit Administrative Account Privileges*.

User Agreement for Administrative Access Utility

You have been granted an exception to the endpoint security standard, **2.7 Limit Administrative Account Privileges**, which states, "Restrict administrative privileges to device administrators only." The administrative access utility allows temporary use of administrative privileges. It has been installed on your system for the following reason(s):

- ☒ Installation of non-standard research or instructional software.
- ☐ Use of software specifically requiring administrative privileges.
- ☐ Interfacing with external hardware devices.
- ☐ Other: _____

By requesting this exception, you assume all risk and responsibility for potential security issues that may arise through improper use of this software. Your IT support staff will assist when appropriate.

Please note the following guidelines:

- The administrative access utility is to be used only for the purpose expressly specified in the exception. It is not to be used for any other purpose, including creating local administrative accounts, elevating privileges for other accounts, modifying group policy settings, or modifying the system registry.
- System modifications, updates, and similar activities that fall outside of the granted exception should continue to be performed by your IT support staff.
- If it is discovered that the software has been used for any action outside of the intended purpose, it will be removed and full administrative control of the computer will revert to your IT support staff.
- It is intended only for the use of the faculty or staff member who has been granted permission to use it.
- The administrative access utility may not be used to remove or restrict IT support staff accounts and access to the device.

Careful and appropriate use of the administrative access utility meets the requirement 5 of the CIS Critical Security Controls ("Controlled Use of Administrative Privileges") and directly maps to HIPAA, NIST, ISO, FISMA, PCI, and ITIL regulations and standards. It protects UB Category 1, 2, and 3 data and promotes responsible use of computing by normally running as user, not with administrative privileges.

Thank you for your support of the University security standards. For more information, please review the UB Minimum Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices.