

| | | | | | |
|---|--|---|-------------------------------------|--------------------------|--|
|  Office of Cybersecurity <small>CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY UNIVERSITY OF WISCONSIN-MADISON</small> | | <h1 style="margin: 0;">Endpoint Security Checklist</h1> | | Page 1 of 1 | |
| Document Number: GRC-0001 | Document Owner: secure-box-admins@office365.wisc.edu | First Published: 1/1/2019 | Revision Date: 10/14/2024 | Version: 1.1.1 | |

Overview

External collaborators must complete this form attesting to security controls on the endpoint used to access a UW-Madison secure Box folder.

| | |
|---|---|
| Endpoint Hostname(s): _____ Endpoint Primary Location(s): _____ Operating System(s): _____ | Primary User(s): _____ User's Organization: _____ User's IT Support Org: _____ |
|---|---|

Please review the following cybersecurity controls. If a control is present on the endpoint, initial in the corresponding box. If the control is not present, DO NOT initial.

| Security Control | Initials |
|---|----------|
| 1. Host-based vulnerability management and configuration compliance software is installed and enabled. | |
| 2. Vulnerability scans of the endpoint are completed (at least) monthly. | |
| 3. All available operating system and application security patches are installed. | |
| 4. Anti-virus / anti-malware software is installed and enabled. | |
| 5. Host-based firewall is installed and enabled. | |
| 6. Host-based Intrusion Prevention System (IDS/IPS) is installed and enabled. | |
| 7. Primary user DOES NOT have administrative rights on the workstation. | |
| 8. Whole-disk encryption solution (hardware or software) is installed and enabled. | |
| 9. Encryption solution and policies are managed centrally, not by the primary user. | |
| 10. Primary user logs off or locks the endpoint when it is unattended. | |
| 11. Endpoint is configured to automatically lock the screen when inactive for 15 minutes. | |
| 12. Password policies are enforced that adhere to best practices (length and complexity minimum requirements, no password reuse permitted). | |
| 13. Primary user completes (at least) annual cybersecurity awareness training. | |
| 14. Other security practices and compensating controls, please list: | |

Completed by (print): _____ Signature: _____ Date: _____

****In the event the workstation or user becomes compromised (via malware, exploited vulnerability, leaked credentials, etc.), or the workstation is stolen/replaced, contact the UW-Madison Office of Cybersecurity at cybersecurity@cio.wisc.edu.**