Office of Cybersecurity CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY UNIVERSITY OF WISCONSIN–MADISON	# Restricted Research Drive Endpoint Checklist			Page **1** of **1**
Document Number: GRC-0001	**Document Owner:** Research Cyberinfrastructure Team	**First Published:** 8-1-25	**Revision Date:** 8-1-25	**Version:** 1.0

Overview

All users of Restricted ResearchDrive are required to use endpoints that comply with UW-526 Endpoint Management and Security Policy. Please complete this endpoint checklist to verify that your endpoint meets this requirement. You may need the assistance of IT staff in your department to answer these questions.

Endpoint Hostname(s): ______________________ Primary User(s): ________________________

Endpoint Primary Location(s): ______________________ User's Organization: ________________________

Operating System(s): ______________________ 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: ________

**Once this form is completed, it should be sent to the Office of Cybersecurity, Risk Management & Compliance (RMC) for review and overall evaluation of risk.   Please forward to rmc-cybersecurity@cio.wisc.edu.