University at Buffalo
Information Technology

Exception Request Form: Minimum Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices

Directions: Under appropriate circumstances, a user may be granted an exception to adherence to the Minimum Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices. Academic and clinical units are responsible for identifying and implementing their exceptions process and for documenting their exceptions.

Exceptions are valid for one calendar year from date of approval.

Section A: Employee Information

Employee Name	
Employee Position/Title/Role	
Employee Signature	
School/Unit/Department	
Date	

Section B: Exceptions Requested

University-owned desktop, laptop, and notebook computers that have access to, store, and/or process university data.

By checking the box(es) below, you are requesting an exception to compliance with the standard(s). The form can be for multiple exception requests.

	Standards for Low Risk Data
	2.1 Security Patching
	2.3 Malware Protection
	2.4 Supported OS
	2.5 Supported Software
	2.6 Firewall
	2.7 Limit Administrative Account Privileges
	2.8 Whole Disk Encryption

Please note that exceptions are not permitted for 2.2 Password Authentication

	Standards for Moderate Risk Data
	2.9 Scan for Personally Identifiable Information (PII)
	2.10 Inventory
	2.11 Inactivity Timeout
	2.12 Hard Drive and Printer Sharing
	2.14 Disposal/Re-use of Hard Drives and Storage
	2.15 Remote Desktop Access

Please note that exceptions are not permitted for 2.13 Login Banner

Exception Request Form: Minimum Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices

Standards for High Risk Data	
	2.16 Application Whitelisting
	2.17 Account Lockout
	2.18 Vulnerability Scanning
	2.19 Physical Security
	2.20 Security Benchmarking

Section C: Exceptions Requested

University-owned mobile and other endpoint devices that have access to, store, and/or process university data.

Standards for Low Risk and Moderate Risk Data	
	3.2 Inactivity Timeout
	3.5 Disposal/Re-use
	3.6 DO NOT Store Category 1 Data

Please note that exceptions are not permitted for 3.1 PIN or Passcode, 3.3 Encryption, or 3.4 Remote Location and Erase

Section D: Rationale

Section E: Approval

Dean/Vice President/Designee Name (please print)

Dean/Vice President/Designee Signature Date