WRIGHT STATE
UNIVERSITY

MINIMUM STANDARDS
CATS - INFORMATION TECHNOLOGY

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.1	6-26-2008	Mike Persina	Initial Publication
1.2	7-2-2010	Mike Natale	Annual Review – minor grammar correction.
1.2	10-3-2011	Michael Persina	Annual review
1.3	11-15-12	Mike Persina	Annual review – added language exempting systems connected to AD domain.
1.4	4-8-2013	Mike Natale	Added critical security patch language for PCI compliance.
1.4	4-9-2014	Ken Nelson	Annual Review
1.5	6-29-2015	Mike Natale	Removed broken links.
1.5	08-01-2016	Mike Natale	Annual Review
1.5	10-01-2017	Mike Natale	Annual Review – Desktop Matrix updated
1.5	02-01-2019	Mike Natale	Annual Review
1.6	2-06-2020	John Remley	Minor modifications to anti-virus and full disk encryption
1.6	9-21-2021	John Remley	Annual Review
1.6	4-21-2022	Mike Natale	Annual Review
1.6	02-23-2024	Mike Natale	Annual Review

Wright State University

Information Security

Controls	
Policy Title:	Minimum Standards Policy
Category:	Information Technology
Audience:	WSU Faculty, Staff, and Students
Reason for Revision:	*N/A*
Created / Modified Date:	6-26-08
Location:	http://www.wright.edu/security/policy/

Responsible Parties	
Author	Mike Persina
Technical Reviewer/Mgr	
Security Reviewer	Michael Natale

TABLE OF CONTENTS

Policy Purpose

Policy Description

The following minimum standards are required for devices connected to the University network.

Software Patch Updates

University networked devices must run software that has security patches available. They also must have all currently available security patches installed. PCI-DSS systems should have the latest vendor security patches installed - critical security patches must be installed within one month of release. Exceptions may be made that compromise the usability of critical applications, such as research equipment. "Request for Exception" may be requested on the Minimum Standards for Networked Device Security Configurations. See University Desktop Compliance Matrix below.

Anti-Virus Software

Anti-virus software is made available for University owned computer systems. The CaTS Helpdesk also has a list of recommended anti-virus software for personally owned computer systems. All systems connecting to the University's network must be running up-to-date anti-virus software. See University Desktop Compliance Matrix below.

Host-Based Firewall Software

Host-based firewall software for any particular type of device currently listed on the University software distribution website must be running and configured according to the implementing guidelines on every device connected to the University network. While CaTS implements firewalls as part of the security strategy, those firewalls do not exclude the need for host-based firewalls. See University Desktop Compliance Matrix.

Spyware

Spyware or malware is any type of technology that collects and transmits information about a person or their browsing. Anti-spyware software for any particular type of device currently listed below on the University Desktop Compliance Matrix must be running and up-to-date on every device connected to the University network.

Passwords

University electronic communications systems or services must identify users and authorize access by means of passwords or other secure authentication processes. All default passwords for access to network-accessible devices must be modified. Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device unless device is joined to an Active Directory domain.

Full Disk Encryption

All university owned laptops must utilize full disk encrypted unless an exception is granted. Contact the CaTS Help Desk to make an exception request.

No Unencrypted Authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the campus network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all campus devices must use only encrypted authentication mechanisms unless otherwise authorized.

In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

Physical Security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent e-mail use, or any number of other potentially dangerous situations. When reasonable and appropriate, devices must be configured to authenticate upon logon. When reasonable and appropriate, devices must be configured to "lock" and require a user to authenticate if left unattended for more than ten minutes. Laptops, tablets and other mobile devices must be secured from unauthorized access.

Unnecessary Services

If a service is not necessary for the intended purpose or operation of the device that service should be disabled.

University Desktop Compliance Matrix

Required Software	Microsoft OS (Windows)	Macintosh OS X	UNIX - Solaris, SUSE, Red Hat
OS Updates	X	X	X
Anti-Virus	X	X	X
Spyware/Malware	X	X	
Personal Firewall	X	X	X

Enforcement

Failure to comply with this policy may result in disciplinary action and/or the loss of use of university computing resources. The university also may refer suspected violations of applicable law to appropriate law enforcement agencies.