STANDARD: Minimum Security Standards

Overview

This document addresses the minimum standards required under data categorization and ensure the confidentiality, integrity, and availability of university data and technology resources.

Policy Reference

APM 30.11 Data Classifications and Standards

Scope

These standards are the minimum baseline for all university faculty, staff, students, and affiliates accessing, storing, and processing UI data or using UI technology resources at the Low, Moderate, or High risk levels. Effective date: August 20, 2016.

Standards

Standards	Requirements	Low	Moderate	High	Reference*
Access Control	Use separate privileged accounts for administrative or security access, and audit the use of privileged access.		x	x	3.1.5,6,7
Access Control	Require authentication (or verify identity) to access non-public information and limit information access to authorized users and processes.	x	x	x	3.1.1,3.1.2,3.5.2
Access Control	Require ITS-approved and centrally logged authentication for access to data.			x	3.1.3
Access Control	Store data only on the ITS shared drive or ITS-approved locations.			x	3.1.3
Access Locks	Limit unsuccessful logon attempts by locking accounts after 20 unsuccessful attempts in 10 minutes.	x	x	x	3.1.8
Access Timeout	Lock workstation or session after 5 minutes of inactivity. Automatically			x	3.1.10,3.1.11

	terminate session when appropriate.				
Access Timeout	Lock workstation or session after 15 minutes of inactivity. Automatically terminate session when appropriate.		x	x	3.1.10,3.1.11
Antivirus	All systems capable of running Antivirus must install and run with up-to-date definitions and periodic scans.	x	x	x	3.14.2,4,5
Antivirus	Installed antivirus must be managed or approved by the ITS Security Office (Sophos).			x	3.14.6
Audit	Log system access to enable analysis, investigation, and reporting of unlawful or uauthorized activity, and ensure invidual users can be uniquely identified.	x	x	x	3.3.1,3.3.2
Audit	Ensure logs for data and systems access is centrally logged for at least 1 year. All systems should be time synchronized to assure accuracy. Logs must be protected from unauthorized access or modification, and access changes limited to a subset of privileged users.			x	3.3.7,3.3.9
Configuration Management	Establish baseline configuration and hardware and software inventory through ITS configuration management. Baseline configuration must establish and enforce security settings. Inventory, control, and monitor user software.		x	x	3.4.1,3.4.2,3.4.9

Configuration Management	Establish least functionality, by disabling unneeded access, services, or functionality. Restrict local admin rights on workstations.		x	x	3.4.6,3.4.7
DNS	All systems must use ITS-approved Domain Name System (DNS) servers.	x	x	x	NFO SC-20,21,22
Encryption	All data must be encrypted in transport, and at rest. Endpoint or mobile devices must be encrypted with ITS-managed encryption.			x	3.8.6,3.13.10,3.13.11, 3.1.19
Encryption	All authentication must happen over encrypted transport mechanisms.	x	x	x	3.5.10
Encryption	All data for remote access must be encrypted in transport.		x	x	3.1.13,3.13.8
Firewall	All systems capable of running a host-based firewall, must have it turned on and configured consistent with the principles of least privilege.	x	x	x	3.1.5,3.1.20
Identification and Authentication	Identify users, user processes, or devices accessing data or systems. Require authentication before system or data modification.	x	x	x	3.5.1
Identification and Authentication	Authenticate users or user processes before they can access information systems.		x	x	3.5.2
Identify Management	Ensure each user has a unique account. Account names cannot be re-used after they have been established for 1 business day.	x	x	x	3.5.5

Incident Response	Report all suspected technology security incidents to the ITS Security Office and cooperate with assigned investigators. All reports will be categorized, tracked, and reported per the Technology Security Incident Response Plan.	x	x	x	3.6.1,3.6.2
Inventory	All networked devices, except on designated and restricted guest networks, must be registered in the ITS Network Management System.	x	x	x	3.4.1
Logon Banner	Where possible, provide an approved system use notification at every logon to university controlled systems.	x	x	x	3.1.9
Maintenance	Limit maintenance on information systems to authorized personnel. Sanitize media of university data before any off-site maintenance is performed.		x	x	3.7.1,3.7.2
Media Protection	Protect paper and digital media from physical access except by authorized users.		x	x	3.8.1,3.8.2
Media Sanitization	Sanitize or destroy by an approved method (DBAN or similar) any media with university data, before media is disposed or reused.	x	x	x	3.8.3
Multifactor Authentication	Use multi-factor authentication for local and network access to privileged accounts, and network access to non-privileged accounts.			Targeted for 2017	3.5.3

Patching	Only run operating systems which are currently supported and patched. Apply security patches to address flaws in systems and applications automatically, or within 10 days. Alternatively, patches may be applied in a timeframe approved through a risk-based vulnerability assessment process approved by the ITS Security Office and all affected data and system owners.	x	x	x	3.14.1
Physical Protection	All university data centers must be limited in access, that access be logged and monitored, and all visitors escorted and logged.	x	x	x	3.10.1,3.10.2,3.10.3,3.10.4
Public Data	Information to be published external to the university must be approved by an appropriate authority or process.	x	x	x	3.1.22
Remote Access	Monitor and control remote workstation access, and limit to access via ITS-managed VPN.		x	x	3.1.12,3.1.14,3.1.15
Removable Media	Removable media or storage devices which may contain university data must be restricted from external use by mandating ITS-managed encryption.			x	3.1.21,3.8.6
Risk Assessment	All devices on the university network are subject to vulnerability scanning, and proactive measures taken (APM 30.14) by the Computer Security Incident Response Team in accordance with assessment of risk.	x	x	x	3.11.2,3.11.3

Security Assessment	Security controls must be periodically assessed and action plans implemented to address any vulnerabilities and to ensure continued effectiveness.		x	x	3.12.1,2,3
Security Awareness	All users shall receive routine security awareness training appropriate for their role.		x	x	3.2.1,2,3
System and Communication Protection	Incoming and outgoing communications must be monitored, controlled, and protected where it enters and leaves university controlled systems. Architecture and design shall promote effective information security. This includes email as well as interfaces with external vendors.	x	x	x	3.13.1,3.13.2
System and Communication Protection	Publicly accessible systems shall be on separate networks from internal-only systems.	x	x	x	3.13.5
Vendor Security Assessments	A Risk Assessment must be completed by the ITS Information Security Office before the University acquires or utilizes external information systems.	x	x	x	NFO SA-9
Wireless Access	Limit access to university systems and data to approved wireless network that use encryption and authentication (AirVandalGold).		x	x	3.1.17

Other References

NIST SP800-171 (January 2016) http://dx.doi.org/10.6028/NIST.SP.800-171

NIST SP800-53r4 (April 2013) http://dx.doi.org/10.6028/NIST.SP.800-53r4

*Numbers are 800-171, otherwise SP800-53 is the reference.

*Glossary**

Data at Rest	For the terms of this standard, "at rest" data will be considered to be data outside of the ITS-managed or approved data centers.
Privileged Access	Authorized access to perform security-relevant functions that ordinary users are not allowed to perform.
Remote Access	Access to an information system communicating through an external network (Internet).
Local Access	Access to an information system directly and not through a network.
Multifactor Authentication	Two or more factors to achieve authentication, including something you know (password); something you have (cryptographic device, hardware or software token); or something you are (biometric).
Security functions	Hardware and software of an information system responsible for enforcing system security controls or policy and supporting the isolation of code and data.

*For further glossary and clarification, refer to NIST SP800-171.

Standards Owner

UI Information Technology Services (ITS) is responsible for the content and management of these standards.