Minimum Security Standards and Guidance

Minimum Security Standards and Guidance
for Protection of Electronic Data

Effective: August 1, 2015
Contact: Information Technology Services

Contents

Purpose

This standard, in concert with the Data Classification policy, implements the Data Protection Requirements section of the Information Technology Security policy. Adherence to these standards is an essential safeguard for the protection of electronic university data and systems. However, compliance does not assure complete security. These standards should be incorporated into a comprehensive security plan. Additional policies and laws may also apply.

1. Scope

This standard applies to all electronic accounts, systems, devices, and networks, which access, contain or transmit any University-owned data, to the extent that such accounts, systems, devices and networks have been made accessible to employees, agents or contractors of Iowa State Universtiy.

2. Audience

This standard applies to all data users, data owners, data custodians, data stewards, and system and network administrators of such accounts, systems, devices, and networks.

3. Minimum Standards

This section lists the minimum standards that are to be enabled and enforced for the various data protection levels.

Using the Data Classification Standards and Guidance, classify each data item as restricted, high, moderate, or low.

If a reliable and effective solution is not available for a particular requirement, then a limited exception may be granted (see section 4).

top

3.1. Minimum Standards for Account Controls

These are standards related to user credentials for authentication and authorization (e.g. Net-ID, university ID).

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.1.1	All administrative accounts must use multifactor authentication if the technology is available and implemented.		Required	Recommended	Recommended	Optional
3.1.2	Each account must use a password meeting the ISU high level of strength.		Required	Required	Recommended	Optional
3.1.3	Each account must use a password meeting the ISU moderate level of strength.		NA	NA	Required	Required
3.1.4	All unused accounts must be deleted or disabled as soon as practicable.		Required	Required	Required	Recommended
3.1.5	Each account must be granted the least privilege to perform required job function(s).		Required	Required	Required	Required
3.1.6	Each account must be assigned to one individual or to one service.		Required	Required	Required	Required
3.1.7	Each account must be restricted to a single security domain [ie. data protection level].		Required	Recommended	Recommended	Optional

top

3.2. Minimum Standards for System Controls

These standards are minimum best practices for systems administration.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**

3.2.1	Local login access to the system must be restricted by access control list to those accounts with a documented business need to use the data on the system.		Required	Required	Required	Recommended
3.2.2	Remote login access to the system must be restricted to those accounts with a documented business need to use the data on the system remotely.		Required	Required	Required	Recommended
3.2.3	Accounts with access to the system will be regularly reviewed, and access removed when a business need no longer exists for that access.		Required	Required	Required	Recommended
3.2.4	Only the minimum operating system components and applications required to carry out the business function shall be installed.		Required	Recommended	Recommended	Recommended
3.2.5	Security updates to the operating system and application services for internet-accessible systems must be applied within the following timeframes: • Critical severity vulnerabilities with an active exploit: Immediately		Required	Required	Required	Required

	• Critical severity vulnerabilities without an active exploit: 15 calendar days • High severity vulnerabilities: 30 calendar days Security updates to the operating system and application services that address known-exploitable-vulnerabilities (KEVs) for non-internet-accessible systems must be applied within 30 days.					
3.2.6	If automated notification of operating system and application updates is available, it shall be enabled.		Required	Required	Required	Recommended
3.2.7	Protected data shall be stored in an encrypted form.		Required	Required	Required	NA
3.2.8	Systems operating on Microsoft Windows or macOS , must actively run an approved malware detection program, with on-access scanning and automatic updates enabled.		Required	Required	Required	Required
3.2.9	Systems must run only the services required to perform the specific business		Required	Recommended	Recommended	NA

	function of the machine.					
3.2.10	Systems must not run client applications that are common attack vectors, e.g., email, instant messaging, web browsers.		Required	Recommended	Recommended	NA
3.2.11	Systems must have session timeouts and screen locks enabled.		Required	Required	Required	Optional
3.2.12	Where available, systems must run an integrity checker on critical system and configuration files.		Required	Recommended	Recommended	NA
3.2.13	All file systems containing critical system files or protected data must require authentication and support access control.		Required	Required	Required	Recommended
3.2.14	All privileged access must be logged, e.g., administrator, root.		Required	Recommended	Recommended	Recommended
3.2.15	All logins and logouts must be logged.		Required	Recommended	Recommended	Recommended
3.2.16	Logging of all security events is required.		Required	Recommended	Recommended	Recommended
3.2.17	Security logging must include remote logging.		Required	Recommended	Recommended	Recommended
3.2.18	Security logging must be monitored 24x7.		Recommended	Recommended	Recommended	Optional
3.2.19	Storage media and systems must be clearly labeled with		Required	NA	NA	NA

	Restricted Data Stickers.					
3.2.20	Systems must be running an operating system and apps that are actively supported for security fixes.		Required	Required	Required	Required

top

3.3. Minimum Standards for Network Controls

These standards define network access that connect systems.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.3.1	System must be on a firewall protected network shared only with systems in the same security domain.		Required	Recommended	Recommended	Optional
3.3.2	All network transit of Protected Data across the network must be encrypted.		Required	Required	Required	NA
3.3.3	No cleartext transmission of passwords shall be permitted.		Required	Required	Required	Required
3.3.4	Network access shall be restricted to the minimum necessary to perform required functions. Example: firewalls		Required	Required	Required	Optional

top

3.4. Minimum Standards for Physical Controls

Best practices for physical securing of equipment.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.4.1	Systems must be located in a locked room with limited access.		Required	Recommended	Recommended	NA

3.4.2	Systems must be located in a locked rack or cage.		Required	Optional	Optional	Optional
3.4.3	Backup media must be physically secured from unauthorized access.		Required	Required	Required	Recommended
3.4.4	Backup media must be stored in a physically diverse location.		Required	Recommended	Recommended	Recommended
3.4.5	Systems must be provided with power protection--conditioning, uninterruptable power supply UPS, and backup generator.		Required	Recommended	Recommended	Optional
3.4.6	Systems must be located in a room with appropriate environmental controls, e.g., heat, humidity.		Required	Recommended	Recommended	Recommended
3.4.7	Systems storage media must be securely erased or disposed of when system function/role changes including equipment disposal.		Required	Required	Required	Recommended
3.4.8	Storage media must be physically destroyed when system function or role changes to a lower classification or at equipment disposal.		Required	Recommended	Recommended	NA

top

3.5. Minimum Standards for Training and Compliance

These are the steps necessary to ensure security policy and standard awareness.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.5.1	All system users must be notified of what protected data exists on a system and its protection requirements.		Required	Recommended	Recommended	NA
3.5.2	At least annually all system users must sign the *Protected Data*		Required	Recommended	Recommended	NA

	Confidentiality Agreement. Link is pending.					

top

3.6. Minimum Standards for Change Management

Standards related to approved changes to systems.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.6.1	System administrators must establish, document and use an approved change control process for system configuration.		Required	Recommended	Recommended	Recommended
3.6.2	System changes and patches must be evaluated and tested prior to installation in a production environment.		Recommended	Recommended	Recommended	Recommended

top

3.7. Minimum Standards for Business Continuity

This ensures the availability of university data and information processing systems.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.7.1	System administrators must establish, document, and follow a regular backup schedule.		Required	Recommended	Recommended	Recommended
3.7.2	The ability to restore from backup must be tested at least once a month--automated verification, user-initiated, or trial restores are acceptable methods.		Required	Recommended	Recommended	Recommended
3.7.3	Contact the ITS Security team by emailing security@iastate.edu upon discovery of		Required	Required	Required	Required

	possible compromised data.					

top

3.8. Minimum Standards for Lifecycle Management

These ensure that university devices are tracked and managed consistently.

			Data Protection Level			
	Standard		**Restricted**	**High**	**Moderate**	**Low**
3.8.1	All desktops and laptops which are not stored in a data center and regardless of operating system, must be tracked in a central inventory database.		Required	Required	Required	Required
3.8.2	Name, serial number, MAC addresses, physical location, operational state, device ownership, and technology support group must be recorded for each tracked device.		Required	Required	Required	Required
3.8.3	All physical hardware running Windows or macOS operating systems, which are not stored in a data center, and not managed by a vendor or third-party, must be managed using centrally managed endpoint management systems.		Required	Required	Required	Required
3.8.4	All tracked hardware must be retired using ISU Surplus's excess property disposal process		Required	Required	Required	Required
3.8.5	Retired devices must be removed from ISU systems, including endpoint management, Active		Required	Required	Required	Required

	Directory, and network registration					
3.8.6	All assets tracked in the central inventory database must be accounted for every two years.		Required	Required	Required	Required

top

4. Exceptions

If any of the required minimum standards cannot be met, a Security Exception Plan [link pending], which reports the non-compliance and describes the plan for risk assessment and mitigation, must be filed with the Information Security Office for approval. Upon approval of the plan, a limited exception may be granted.

5. Compliance

Non-compliance with these standards will result in revocation of access to the data, system, and/or network, as well as notification of superiors.

All Iowa State University employees are required to comply with all applicable policies, standards, rules, regulations and laws.

6. Resources

Data Classification Policy
Data Classification Standards and Guidance
Information Security Office (email) (link pending)
Information Technology Security Policy
IT Security Incident Reporting Policy
IT Glossary of Terms
Implementation Guidelines (link pending)