Data Handling Standards

Version: 1.0
Published: Dec. 20, 2022
Published by: Information Security Office

Each control is mapped to the data classification and protection standard using the applicable words: Essential, Required, Recommended, Optional

Essential: Must be addressed for all current and future systems
Required: Must be addressed for future systems and prioritized for current systems
Recommended: Not compulsory but highly encouraged
Optional: Apply if appropriate

Minimum Standards/Controls: Controls that applies to university processes, procedures and systems					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
Min-1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Essential	Recommended	Optional	
Min-2	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and the applicable policies, standards, and procedures related to the security of those systems.	Essential	Recommended	Optional	
Min-3	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Essential	Recommended	Optional	
Min-4	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Essential	Recommended	Optional	
Min-5	Protect (i.e., physically control and securely store) system media containing the University's data, both paper and digital.	Essential	Recommended	Optional	
Min-6	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation,) organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of the University's data.	Essential	Recommended	Optional	
Min-7	Remediate vulnerabilities in accordance with risk assessments	Essential	Essential	Essential	
Min-8	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Essential	Recommended	Recommended	
Min-9	Identify, report, and correct system flaws in a timely manner.	Essential	Recommended	Recommended	
Min-10	Monitor system security alerts and advisories and take action in response.	Essential	Essential	Essential	
Access Controls: Controls that ensures only authorized personnel, accounts and system processes have access to the university's data.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
AC-1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Essential	Recommended	Optional	
AC-2	Limit system access to the types of transactions and functions.	Essential	Recommended	Optional	
AC-3	Control the flow of the University's data in accordance with approved authorizations.	Essential	Recommended	Optional	
AC-4	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Essential	Essential	Essential	
AC-5	Use non-privileged accounts or roles when accessing nonsecurity functions.	Essential	Essential	Essential	
AC-6	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Essential	Essential	Essential	
AC-7	Limit unsuccessful login attempts.	Essential	Essential	Essential	
AC-8	Provide privacy and security notices consistent with applicable University data rules.	Essential	Essential	Essential	
AC-9	Terminate (automatically) a user session after a defined condition.	Essential	Recommended	Optional	
AC-10	Monitor and control remote access sessions.	Essential	Recommended	Optional	
AC-11	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Essential	Recommended	Optional	
AC-12	Route remote access via managed access control points.	Essential	Recommended	Optional	
AC-13	Authorize wireless access prior to allowing such connections.	Essential	Essential	Essential	
AC-14	Protect wireless access using authentication and encryption.	Essential	Essential	Essential	
Awareness and Training: These controls ensure that university staff are provided with appropriate training and skills.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
AT-1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Essential	Recommended	Recommended	
AT-2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Essential	Recommended	Recommended	
AT-3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Essential	Recommended	Optional	
Audit and Accountability: These controls ensure that the university's data is properly maintained, including storage, processing and handling.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
AA-1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Essential	Recommended	Optional	
AA-2	Review logged events.	Essential	Recommended	Optional	
AA-3	Alert in the event of an audit logging process failure.	Essential	Recommended	Optional	

AA-4	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Essential	Recommended	Optional	
AA-5	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Essential	Recommended	Optional	
AA-6	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Essential	Recommended	Optional	
AA-7	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Essential	Recommended	Optional	
AA-8	Limit management of audit logging functionality to a subset of privileged users.	Essential	Recommended	Optional	
Configuration Management: Configurations, systems and software are standardized and managed to ensure they perform in definable and measurable ways.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
CM-1	Analyze the security impact of changes prior to implementation.	Essential	Recommended	Optional	
CM-2	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Essential	Recommended	Optional	
CM-3	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Required	Essential	Recommended	
Identification and Authentication: controls to ensure only confirmed and approved identities gain authorized access.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
IA-1	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged account	Essential	Recommended	Optional	
IA-2	Prevent reuse of identifiers for a defined period.	Essential	Recommended	Optional	
IA-3	Enforce a minimum password complexity and change of characters when new passwords are created.	Essential	Recommended	Recommended	
IA-4	Prohibit password reuse for a specified number of generations.	Essential	Recommended	Optional	
IA-5	Allow temporary password use for system logons with an immediate change to a permanent password.	Essential	Recommended	Optional	
IA-6	Obscure feedback of authentication information.	Essential	Recommended	Optional	
Incidence Response: Establishes an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
IR-1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Essential	Recommended	Optional	
IR--2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Essential	Essential	Recommended	
IR-3	Test the organizational incident response capability.	Essential	Recommended	Recommended	
Maintenance: Controls and mitigate vulnerabilities through hardware, firmware and software updates					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
M-1	Perform maintenance / apply updates or patches on organizational systems.	Essential	Recommended	Optional	
M-2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Essential	Recommended	Optional	
Media Protection: Media protection controls ensure media that hold data, including paper and electronic storage, are protected.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
MP-1	Protect (i.e., physically control and securely store) system media containing data, both paper and digital.	Essential	Recommended	Optional	
MP-2	Limit access to the University's data on system media to authorized users.	Essential	Recommended	Optional	
MP-3	Sanitize or destroy system media containing the University's data before disposal or release for reuse.	Essential	Recommended	Optional	
MP-4	Control access to media containing the University's data and maintain accountability for media during transport outside of controlled areas.	Essential	Recommended	Optional	
MP-5	Implement cryptographic mechanisms to protect the confidentiality of the University's data stored on digital media during transport unless otherwise protected by alternative physical safeguards. optional recommended essential essential	Essential	Recommended	Optional	
MP-6	Protect the confidentiality of backup University data at storage locations.	Essential	Recommended	Optional	
Personnel Security: controls that protect University data against unauthorized access through staff authorization changes.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
PS-1	Ensure that organizational systems containing the University's data are protected during and after personnel actions such as terminations and transfers.	Essential	Essential	Essential	
Physical Protection: Access to physical systems and locations controlled through appropriate security measures.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
PP-1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Essential	Essential	Recommended	
PP-2	Control and manage physical access devices.	Essential	Essential	Required	
PP-3	Enforce safeguarding measures for the University's data at alternate work sites.	Essential	Essential	Optional	
Risk Assessment: Risk assessment controls ensure appropriate measures are in place to assess and remediate identified risks.					
Control ID	**Control Description**	**Information Risk Classification**			

		High	Moderate	Low	Assessment
RA-1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of the University's data	Essential	Recommended	Optional	
RA-2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Essential	Recommended	Recommended	
RA-3	Remediate vulnerabilities in accordance with risk assessments.	Essential	Recommended	Recommended	
Security Assessment: Security assessment controls to ensure the security program is operating effectively.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	**Assessment**
PS-1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Essential	Recommended	Optional	
PS-2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Essential	Recommended	Recommended	
PS-3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Essential	Recommended	Optional	
Systems and Communication Protection:These controls ensure University data is protected from unauthorized exposure while at rest or in transit over university services and networks.					
Control ID	**Control Descritpion**	**Information Risk Classification**			
		High	**Moderate**	**Low**	
SCP-1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Essential	Recommended	Optional	
SCP-2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Essential	Recommended	Optional	
SCP-3	Implement cryptographic mechanisms to prevent unauthorized disclosure of the University's data during transmission unless otherwise protected by alternative physical safeguards.	Essential	Recommended	Optional	
SCP-4	Establish and manage cryptographic keys for cryptography employed in organizational systems	Essential	Recommended	Optional	
SCP-5	Employ University approved cryptography when used to protect the confidentiality of the University's data.	Essential	Recommended	Optional	
SCP-6	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies	Essential	Recommended	Optional	
SCP-7	Protect the authenticity of communications sessions	Essential	Recommended	Optional	
SCP-8	Protect the confidentiality of the university's data at rest	Essential	Recommended	Optional	
System and Information Intergrity:These controls ensure University systems, data, and processes are trusted and protected against malicious or accidental alteration.					
Control ID	**Control Description**	**Information Risk Classification**			
		High	**Moderate**	**Low**	
SII-1	Identify, report, and remediate system flaws in a timely manner.	Essential	Recommended	Recommended	
SII-2	Provide protection from malicious code at designated locations within organizational systems.	Essential	Recommended	Recommended	
SII-3	Monitor system security alerts and advisories and take action in response.	Essential	Recommended	Optional	
SII-4	Update malicious code protection mechanisms when new releases are available.	Essential	Recommended	Optional	
SII-5	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Essential	Recommended	Optional	