GEORGE MASON UNIVERSITY

Information Technology Systems

INFORMATION TECHNOLOGY SECURITY STANDARD

Version Control

Version	Date	Purpose of Revision
1.0	September 26, 2019	Initial Release

TABLE OF CONTENTS

1. Introduction

1.1 About this Standard

This standard details specific requirements that must be employed to support the university's Information Security Policy. The requirements are categorized in 18 "Control Family Standards" drawn from NIST SP 800-53. Some controls are required only for particular classes of systems and/or data, as noted in the corresponding description.

1.2 Applicability to IT Systems and Data

The Data Stewardship Policy (UP 1114) references three categories of data:

- Public Use Data – data intended for general public use.
- Highly Sensitive Data – data that, if exposed, could lead to identity theft or exposure of personal health information, financial theft, or otherwise have significant adverse impact on the university.
- Restricted Data – data that must not be disclosed other than to authorized individuals, in accordance with regulatory requirements.

Additionally, certain research data and systems are subject to Federal Government regulations concerning Controlled Unclassified Information (CUI) as described in UP 1316.

For the purposes of this standard, information systems that process, transmit, or store any of the following categories of data are considered "Sensitive":

- Highly Sensitive Data
- Restricted Data
- Controlled Unclassified Information

Some of the controls listed in this document are intended to apply only to the university's sensitive information systems. Controls that apply only to specific categories are marked accordingly.

2. Interpretation

The applicable controls for any university information system are defined by the category of data that is processed, stored, or transmitted by that system as described above. The university's Information Technology Security Office and the Chief Information Security Officer will work with departments to interpret requirements, and to ensure that suitable controls are in place for departmental information systems.

3. Requirements

System administrators are responsible for complying with the control requirements that are specified for the sensitivity level of systems they maintain. Questions regarding applicability, implementation, or exemption requests should be referred to the Information Technology Security Office. The corresponding control descriptions from NIST SP 800-53 are referenced in brackets at the end of each control requirement.

3.1 Access Control

The university must limit system access to authorized users, processes acting on behalf of authorized users, or authorized devices. Systems and applications that receive, create, transmit, or maintain sensitive data must be classified according to risk.

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). [AC-2, AC-3, AC-17]

3.1.1.a <CUI-systems Only> CUI environment and system access is authorized via the CUI Account Request process. This control is applied to system and service accounts, to automated processes acting on behalf of users and devices, and to services.

- User request for access to the CUI Environment will be fulfilled only if they are assigned to an existing Project
- User CUI credential will exist in disabled status after the assigned Project ends
- User CUI credential is enabled if a new project is assigned

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute. [AC-2, AC-3, AC-17]

3.1.3 <SENSITIVE-systems only> Control the flow of data within the system and between interconnected systems in accordance with approved authorizations. [AC-4]

3.1.3.a <CUI-systems Only> Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. [AC-5]

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. [AC-6, AC-6(1), AC-6(5)]

3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions. [AC-6(2)]

3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. [AC-6(9), AC-6(10)]

3.1.8 Limit unsuccessful logon attempts. [AC-7]

3.1.8.a System administrators should balance security and usability concerning this control. Unsuccessful logon lockouts should not allow a successful Denial of Service attack.

3.1.8.b <SENSITIVE-systems only> Unsuccessful logon attempts to elevated / root privilege accounts should be limited to five unsuccessful logon attempts prior to lockout for a period of five minutes.

3.1.8.c <CUI-systems Only> CUI users are limited to five unsuccessful logon attempts prior to account lockout for a period of five minutes.

3.1.9 <SENSITIVE-systems only> Provide privacy and security notices. [AC-8]

3.1.9.a <CUI-systems Only> Security and Privacy notices are displayed at user and administrator login, including root access for security and network appliances and servers.

3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after 15 minutes of inactivity, on all centrally-managed workstations. [AC-11, AC-11(1)]

3.1.10.a <CUI-systems Only> Sessions must be locked after 15 minutes of inactivity.

3.1.11 <SENSITIVE-systems only> Terminate (automatically) a user session after a defined condition, as prescribed in standard operating procedures. [AC-12]

3.1.11.a <CUI-systems Only> User sessions shall be automatically terminated when period of inactivity exceeds 12 hours.

3.1.12 Monitor and control remote access sessions. [AC-17(1)]

3.1.12a Remote access is only permitted for authorized users, conducting university business.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. [AC-17(2)]

3.1.14 Route remote access via ITS-managed or approved access control points. [AC-17(3)]

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information. [AC-17(4)]

3.1.16 Authorize wireless access prior to allowing such connections. [AC-18]

3.1.16.a Instantiation of wireless networks within Mason’s network boundary is permitted only after approval by ITS Enterprise Infrastructure Services and Information Technology Security Office. [AC-18]

3.1.16.b <CUI-systems Only> Instantiation of wireless networks within the network boundary of CUI environments or systems is prohibited by default.

3.1.17 Protect wireless access using authentication and encryption. [AC-18(1)]

3.1.18 <CUI-systems only> Mobile devices are not permitted to connect to CUI environments, systems or data-stores by default. [AC-19]

3.1.19 Do not store Highly Sensitive Data on mobile devices. [AC-19(5)]

3.1.19.a Highly Sensitive Data stored on laptops and other mobile computing platforms must be approved and encrypted in accordance with UP 1114, Data Stewardship Policy.

3.1.20 <SENSITIVE-systems only> Verify and control/limit connections to and use of external systems. [AC-20]

3.1.20.a <CUI-systems Only> Connections to external systems are permitted only by exception, wherein the exception process is reviewed and approved *or* are permitted after approval by the Architecture Standards Review Board and Information Technology Security Office. [AC20, 20(1)]

3.1.21 <CUI-systems only> Portable storage devices are not permitted to store CUI. [AC-20(2)]

3.1.22 Sensitive information must not be posted or processed on publicly accessible systems. [AC-22]

3.1.22.a <CUI-systems Only> Processing or sharing of CUI on or via publicly accessible systems is not permitted.

3.2 Awareness and Training

The university must ensure that managers, system administrators, and end users are made aware of security risks associated with their activities, and of the applicable policies, standards, and procedures related to the security of those systems.

3.2.1 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. [AT-2, AT-3]

3.2.1.a New faculty, staff, and associates must complete prescribed computer security training within 14 days after starting work at Mason. Faculty and staff must also complete annual refresher training. ITS sets the training content and methods of delivery.

3.2.1.b <CUI-systems Only> System administrators, users, and principle investigators must be trained on the CUI environment and data handling before accessing Mason CUI systems. After initial training, CUI refresher training shall occur annually.

3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. [AT-2, AT-3]

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. [AT-2(2)]

3.3 Audit and Accountability

The university must create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity on sensitive systems.

3.3.1 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. [AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12]

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. [AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12]

3.3.3 Review and update logged events. [AU-2(3)]

3.3.4 Alert in the event of an audit logging process failure. [AU-5]

3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. [AU-6(3)]

3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. [AU-7]

3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. [AU-8, AU-8 (1)]

3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. [AU-9]

3.3.9 Limit management of audit logging functionality to a subset of privileged users. [AU-9(4)]

3.4 Configuration Management

The university must establish and maintain baseline configurations of sensitive systems throughout the system life cycle. Standard security controls shall be established and enforced as a component of the baseline configuration.

3.4.1 <SENSITIVE-systems only> Establish and maintain baseline configurations and inventories of university systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. [CM-2, CM-6, CM-8, CM-8(1)]

3.4.1.a <CUI-systems Only> ITS must establish and maintain a CUI Configuration Management Library.

3.4.2 Establish and enforce security configuration settings for information technology products employed in university systems. [CM-2, CM-6, CM-8, CM-8(1)]

3.4.3 Track, review, approve or disapprove, and log changes to university systems. [CM-3]

3.4.4 Analyze the security impact of changes prior to implementation. [CM-4]

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to university systems. [CM-5]

3.4.6 Employ the principle of least functionality by configuring university systems to provide only essential capabilities. [CM-7]

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. [CM-7(1), CM-7(2)]

3.4.8 <SENSITIVE-systems only> If required in System Security Plan, 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. [CM-7(4), CM-7(5)]

3.4.9 Control and monitor user-installed software. [CM-11]

3.4.9.a Software for personal (non-Mason) use is not allowed on Mason purchased equipment.

3.4.9.b Use all software and associated documentation in accordance with contract agreements, copyright laws, and licensing requirements.

3.5 Identification and Authentication

The identity of information system users, processes acting on behalf of users, or authorized devices must be verified before being allowed access to university information systems.

3.5.1 Identify system users, processes acting on behalf of users, and devices. [IA-2, IA-3, IA-5]

3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to university systems. [IA-2, IA-3, IA-5]

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. [IA-2(1), IA-2(2), IA-2(3)]

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. [IA-2(8), IA-2(9)]

3.5.5 Prevent reuse of identifiers for at least 24 months. [IA-4]

3.5.6 Disable identifiers after a defined period of inactivity. [IA-4]

3.5.6.a <CUI-systems Only> Disable identifiers after sixty days of inactivity.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created. [IA-5(1)]

3.5.7.a <CUI-systems Only> CUI Users are required to change their passwords every year.

3.5.8 Prohibit password reuse for at least 24 generations. [IA-5(1)]

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password. [IA-5(1)]

3.5.10 Store and transmit only cryptographically-protected passwords. [IA-5(1)]

3.5.11 Obscure feedback of authentication information. [IA-6]

3.5.11.a <CUI-systems Only> All systems and processes identified in creating, transporting, manipulating, or transmitting CUI develop, adopt, or adhere to formal, documented identification and authentication standards that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for CUI environments, systems, and processes.

3.6 Incident Response

The university must maintain an operational incident-handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. Incidents shall be tracked, documented, and reported to appropriate authorities.

3.6.1 Establish an operational incident-handling capability for university systems that includes preparation, detection, analysis, containment, recovery, and user response activities. [IR-2, IR-4, IR-5, IR-6, IR-7]

3.6.1.a <CUI-systems Only> Incident response and handling capabilities are established and maintained for CUI environments and systems.

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. [IR-2, IR-4, IR-5, IR-6, IR-7]

3.6.3 Test the university’s incident response capability. [IR-3]

3.7 Maintenance

The university must perform periodic and timely maintenance on university information systems, and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

3.7.1 Perform maintenance on university systems. [MA-2, MA-3, MA-3(1), MA-3(2]

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. [MA-2, MA-3, MA-3(1), MA-3(2)]

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of data. [MA-2]

3.7.3.a <CUI-systems Only> Offsite maintenance is not permitted.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in university systems. [MA-3(2)]

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. [MA-4]

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. [MA-5]

3.8 Media Protection

The university must protect information system media, both paper and digital; limit access to information system media to those authorized to view it; and sanitize or destroy information system media before disposal or release for reuse.

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI or sensitive data, both paper and digital. [MP-2, MP-4, MP-6]

3.8.2 Limit access to CUI or sensitive data on system media to authorized users. [MP-2, MP-4, MP-6]

3.8.3 System media (paper or digital), is sanitized or destroyed prior to disposal or reuse. [MP-2, MP-4, MP-6]

3.8.4 <CUI-systems only> Mark media with necessary CUI markings and distribution limitations. [MP-3]

3.8.5 <SENSITIVE-systems only> Control access to media containing highly sensitive or restricted data, and maintain accountability for media during transport outside of controlled areas. [MP-5]

3.8.5.a <CUI-systems Only> Based on Data Classification, System Owners and System Administrators are responsible for:

- handling and labeling of media
- physical and technical access restrictions, security monitoring, and incident response for CUI
- administrative, technical and physical controls

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI or sensitive data stored on digital media during transport unless otherwise protected by alternative physical safeguards. [MP-5(4)]

3.8.7 Control the use of removable media on system components. [MP-7]

3.8.7.a <CUI-systems Only> The use of portable storage devices for backup retention or restoration is not permitted.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. [MP-7(1)]

3.8.9 Protect the confidentiality of backup CUI and sensitive data at storage locations. [CP-9]

3.9 Personnel Security

The university must (i) ensure that individuals occupying positions of responsibility are trustworthy and meet established security criteria for those positions; (ii) ensure that Mason information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with Mason security policies and procedures.

3.9.1 Screen individuals prior to authorizing access to university systems. [PS-3, PS-4, PS-5]

3.9.2 Disable information system access when personnel are separated from the university. [PS-3, PS-4, PS-5]

3.9.2.a <CUI-systems Only> Ensure that university systems containing CUI are protected during and after personnel actions such as terminations and transfers.

3.10 Physical and Environmental Protection

Physical access to sensitive information systems, equipment, and operating environments must be limited to authorized individuals. The physical plant, utilities, and infrastructure supporting sensitive systems must be protected and controlled.

3.10.1 Limit physical access to university systems, equipment, and the respective operating environments to authorized individuals. [PE-2, PE-4, PE-5, PE-6]

3.10.1.a Secure all telecommunications rooms and use them only for the purposes for which they were designed. Access to university telecommunications rooms shall be restricted to persons authorized by ITS Network and Security Engineering.

3.10.2 Protect and monitor the physical facility and support infrastructure for university systems. [PE-2, PE-4, PE-5, PE-6]

3.10.3 Escort visitors and monitor visitor activity. [PE-3]

3.10.4 Maintain audit logs of physical access. [PE-3]

3.10.4.a Require that facilities that house IT systems and highly sensitive data must maintain audit logs of physical access (e.g. Data Center Access (key-card) and visitor logs) which must be reviewed at least twice each year.

3.10.5 Control and manage physical access devices. [PE-3]

3.10.6 Enforce safeguarding measures for data at alternate work sites. [PE-17]

3.10.6.a *<CUI-systems Only>* User awareness to this requirement is enforced via:

- CUI security banners when user desktops are presented, and prior to user logon
- Administrative consoles prior to command prompt and administrator logon

- Technology Control Plan for individuals working with or exposed to CUI

3.10.7 Require that individuals protect highly sensitive data where such information is exposed (office, alternate worksite etc.)

The following standards apply to Mason's Data Center, alternate data center, and any facility or room that houses critical IT systems.

3.10.8 Protect power cabling for the information system from damage and destruction. [PE-9]

3.10.9 Provide the capability of shutting off power in emergencies. [PE-10]

3.10.9.a Provide safe and easy access for ITS Facilities & Infrastructure Operations personnel.

3.10.9.b Provide switches that are protected against unauthorized activation.

3.10.10 Provide short-term uninterruptable power supply (emergency power) to facilitate orderly shutdown of systems within the data center in the event of electrical power loss. [PE-11]

3.10.11 Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. [PE-12]

3.10.12 Employ and maintain automatic fire suppression and detection devices/systems for the information system that are supported by an independent energy source. [PE-13, PE-13(3)]

3.10.13 Maintain and frequently monitor temperature (between 60-73 ◦F) and relative humidity levels (between 45-75%) within the facility where the information system resides. [PE-14]

3.10.14 Protect the information system from damage resulting from water leakage by providing master shutoff valves on HVAC units that are accessible, working properly, and known to key personnel (from ITS Facility &Infrastructure Operations and University Facilities Management). [PE-15]

3.10.15 Authorize, monitor, and control new and decommissioned IT equipment entering and exiting the facility, and maintains records of those items. [PE-16]

3.11 Risk Assessment

The university must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), assets, and individuals resulting from the operation of university information systems and the associated processing, storage, or transmission of university information.

3.11.1 Periodically assess the risk to university operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of university systems and the associated processing, storage, or transmission of CUI and sensitive data. [RA-3]

3.11.2 Scan for vulnerabilities in university systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. [RA-5, RA-5(5)]

3.11.3 Remediate vulnerabilities in accordance with risk assessments. [RA-5]

3.12 Security Assessment

The university must periodically assess information security controls to determine whether the controls are effective; develop and implement plans to correct deficiencies; and monitor security controls on sensitive systems on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.1 Periodically assess the security controls in university systems to determine if the controls are effective in their application. [CA-2, CA-5, CA-7]

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in university systems. [CA-2, CA-5, CA-7]

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. [CA-2, CA-5, CA-7]

3.12.4 <SENSITIVE-systems only> Develop, document, and periodically update System Security Plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. [PL-2]

3.13 System and Communications Protection

The university must (i) monitor, control, and protect information transmitted or received by university information systems at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within university information systems.

3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by university systems) at the external boundaries and key internal boundaries of university systems. [SC-7, SA-8]

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within university systems. [SC-7, SA-8]

3.13.3 Separate user functionality from system management functionality. [SC-2]

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. [SC-4]

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. [SC-7, SA-8]

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). [SC-7(5)]

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with university systems and communicating via some other connection to resources in external networks (i.e., split tunneling). [SC-7(7)]

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI and sensitive data during transmission unless otherwise protected by alternative physical safeguards. [SC-8, SC-8(1)]

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. [SC-10]

3.13.10 Establish and manage cryptographic keys for cryptography employed in university systems. [SC-12]

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI and sensitive data. [SC-13]

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. [SC-15]

3.13.12.a Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

3.13.13 Control and monitor the use of mobile code. [SC-18]

3.13.13.a *<CUI-systems Only>* Use of Mobile Code for CUI environments and systems is not permitted.

3.13.14 <CUI-systems Only> Use of Voice over Internet Protocol (VoIP) for CUI environments and systems is not permitted. [SC-19]

3.13.15 Protect the authenticity of communications sessions. [SC-23]

3.13.16 Protect the confidentiality of CUI and sensitive data at rest. [SC-28]

3.14 System and Information Integrity

The university must (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within university information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

3.14.1 Identify, report, and correct system flaws in a timely manner. [SI-2, SI-3, SI-5]

3.14.2 Provide protection from malicious code at designated locations within university systems. [SI-2, SI-3, SI-5]

3.14.2.a System administrators are responsible for using malware protection (e.g. antivirus software or file integrity monitoring) on the servers or endpoints they administer

3.14.2.b ITS is responsible for malware filtering on Mason email systems and at Mason boundaries

3.14.3 Monitor system security alerts and advisories and take action in response. [SI-2, SI-3, SI-5]

3.14.4 Update malicious code protection mechanisms when new releases are available. [SI-3]

3.14.5 Perform periodic scans of university systems and real-time scans of files from external sources as files are downloaded, opened, or executed. [SI-3]

3.14.6 Monitor university systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. [SI-4, SI-4(4)]

3.14.7 Identify unauthorized use of university systems. [SI-4]

3.15 Contingency Planning

The university must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the university's information systems to ensure the availability of critical information resources and continuity of operations in an emergency situation.

3.15.1 Document, maintain and implement a contingency planning policy and associated procedures. [CP-1]

3.15.2 Establish and maintain contingency plans for critical functions and systems to sustain continuity of operations during unplanned disruptions of information systems. [CP-2]

3.15.3 Coordinate contingency plan development with the Enterprise Risk Management function. [CP-2]

3.15.4 Identify critical information systems and assets supporting critical business functions. [CP-2]

3.15.5 Define and document Recovery Time Objectives for resumption of critical business functions. [CP-2]

3.15.6 Provide contingency training to information system users and support personnel. [CP-3]

3.15.7 Test information systems contingency plans at least annually, or when major changes are made to the technical environment. [CP-4]

3.15.8 Coordinate contingency plan testing with the Enterprise Risk Management function. [CP-4]

3.15.9 Maintain an alternate storage site, geographically separated from the primary site, as a backup facility for critical information systems and data. [CP-6, CP-6(1)]

3.15.10 Maintain an alternate processing site, geographically separated from the primary site, to enable resumption of critical business functions when the primary site is unavailable. [CP-7, CP-7(1)]

3.15.11 Establish alternate telecommunications services to support critical business functions when the primary telecommunications capabilities are unavailable. [CP-8]

3.15.12 Back up information systems on a regular basis, consistent with defined recovery time and recovery point objectives. [CP-9]

3.15.13 Provide for recovery and reconstitution of information systems after a disruption, compromise, or failure. [CP-10]

3.16 Security Planning

The university must:

3.16.1 Establish and make readily available an Acceptable Use Policy that describes responsibilities and expected behavior of individuals accessing the university's information systems, and require individuals to acknowledge their understanding of the policy. [PL-4]

3.17 System and Services Acquisition

The university must: (i) allocate sufficient resources to adequately protect information systems; (ii) employ system development life cycle processes that incorporate information security considerations; and (iii) ensure that third-party providers employ adequate security measures, through applicable laws, contracts, certifications, and formal agreements to protect information, applications, and/or services outsourced by the university.

3.17.1 Incorporate information security requirements into systems acquisition plans and operating budgets. [SA-2]

3.17.2 Ensure that information security considerations, based on the assessed level of risk, are built into the system development life cycle. [SA-3]

3.17.3 Manage licensed software usage to reduce the chances of violating licensing terms and conditions. [CM-10]

3.17.4 Employ security engineering principles in the specification, design, development, implementation, and modification of information systems. [SA-8]

3.17.5 Require external information system service providers to comply with the university's security requirements and to employ appropriate security controls. [SA-9]

3.17.6 Replace information system components when support for the components is no longer available, or provide justification and documented approval for the continued use of unsupported system components that are required to meet business needs. [SA-22]

3.18 Program Management

The following control family applies to Mason, with ITS as the lead office of responsibility.

3.18.1 Control:

3.18.1.a Develop and disseminate a Mason-wide information security program plan that:

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Includes the identification and assignment of roles, responsibilities, management commitment, coordination among university entities, and compliance;
- Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
- Is approved by a senior official with responsibility and accountability for the risk being incurred to university operations (including mission, functions, image, and reputation), university assets, individuals, and other organizations;

3.18.1.b Review the Mason-wide information security program plan annually.

3.18.1.c Update the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

3.18.1.d Protect the information security program plan from unauthorized disclosure and modification.

3.18.2 Appoint a Chief Information Security Officer (CISO) with the mission and resources to coordinate, develop, implement, and maintain the Mason-wide information security program.

3.18.3 Control:

3.18.3.a Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

3.18.3.b Employ a business case to record the resources required; and

3.18.3.c Ensure that information security resources are available for expenditure as planned.

3.18.4 Control:

3.18.4.a Implement a process for ensuring that plans of action and milestones (POA&M) for the security program and associated university information systems:

- Are developed and maintained;
- Document the remedial information security actions to adequately respond to risk to university operations, assets, and individuals

3.18.4.b Review plans of action and milestones for consistency with the university’s risk management strategy and Mason-wide priorities for risk response actions.

3.18.5 Develop and maintain an inventory of information systems.

3.18.6 Develop, monitor, and report on the results of information security measures of performance.

3.18.7 Develop an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, and individuals.

3.18.8 Address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

3.18.9 Control:

3.18.9.a Develop a comprehensive strategy to manage risk to organizational operations and assets, and individuals, associated with the operation and use of information systems;

3.18.9.b Implement the risk management strategy consistently across Mason; and

3.18.9.c Review and update the risk management strategy annually or as required, to address organizational changes.

3.18.10 Control:

3.18.10.a Manage (i.e., document, track, and report) the security state of Mason information systems and the environments in which those systems operate through security authorization processes;

3.18.10.b Designate individuals to fulfill specific roles and responsibilities within the Mason risk management process; and

3.18.10.c Fully integrate the security authorization processes into a Mason-wide risk management program.

3.18.11 Control:

3.18.11.a Define mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, and individuals; and

3.18.11.b Determine information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

3.18.12 Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

3.18.13 Establish an information security workforce development and improvement program.

3.18.14 Control:

3.18.14a Implement a process for ensuring that Mason plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

- Are developed and maintained; and
- Continue to be executed in a timely manner;

3.18.14b Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and Mason-wide priorities for risk response actions.

3.18.15 Establish and institutionalize contact with selected groups and associations within the security community:

3.18.15.a To facilitate ongoing security education and training for Mason personnel;

3.18.15.b To maintain currency with recommended security practices, techniques, and technologies; and

3.18.15.c To share current security-related information including threats, vulnerabilities, and incidents.

3.18.16 Implement a threat awareness program that includes a cross-organization information-sharing capability.

Glossary/Definitions

Controlled Unclassified Information (CUI)

As defined by Presidential Executive Order 13556, and 32 CFR 2002, is information that the Federal Government creates or possesses, or that an entity creates or possesses for or on behalf of the Federal Government, that a law, regulation, or Federal Government–wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies that is classified under Executive Order 13526 or the Atomic Energy Act, as amended. The Federal CUI regulation applies to Federal executive branch agencies that handle CUI and all organizations (including universities) that handle, possess, use, share, create, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of such an agency.

Highly Sensitive Data

Data that (1) could lead to identity theft or exposure of personal health information if exposed, or (2) has been identified by a researcher, funding agency, or research partner as requiring a high level of security protection. Reference *University Policy 1114, Data Stewardship*.

Mobile Code

Code that is transmitted from a host to be executed on a client machine, often without the client user's initiation or knowledge. Examples include Java, JavaScript, ActiveX, PDF, Postscript, Shockwave, Flash animations, VBScript.

Mobile Computing Platform

Portable electronic devices having hardware and software capabilities to execute typical desktop and Web applications. Examples include laptop computers, tablets, and netbooks.

Mobile Devices

Handheld computing devices such as smartphones and personal digital assistants.

Sensitive Systems

Information systems that process, transmit, or store any of the following categories of data:

- Highly Sensitive Data
- Restricted Data
- Controlled Unclassified Information