Information Technology Security Standard

Version 2.1

STANDARD INFORMATION	
This table should be completed by the responsible office(s) and IT Risk & Compliance, as it provides general information about the standard.	
RESPONSIBLE OFFICES	Information Technology Services (ITS) IT Security Office (ITSO)
ADDITIONAL INFORMATION	32 CFR 2002 Executive Order 13526 ITS.EA-PRS005 Digital Certificate Service Process ITS.ESD-POL001 ITS Change and Configuration Management Policy ITS.ESD-STD001 ITS Configuration Management Standard ITS.EIS-POL001 Firewall Management Security Policy ITS.EIS-STD003 Firewall Exception Standard ITS.EIS-STD004 Data Center Physical, Environmental, and Operational Controls Standard ITS.EIS-STD005 Firewall Ruleset Engineering Standard ITS.ITRC-PROC001 ITS Documentation Procedure ITS.ITRC-PROC004 IT Risk Assessment Procedure ITS.ITRC-PRS003 Third-Party Risk Management Process ITS.ITSO-PRS002 Vulnerability Scanning and Remediation Process ITS.ITSO-STD001 ITS Logging Standards Presidential Executive Order 13556 University Policy 1114 Data Stewardship University Policy 1118 Compliance with the Health Insurance Portability and Accountability Act (HIPAA) University Policy 1102 Records Management University Policy 1114A Removal of University Data from Electronic Media University Policy 1119 Classified Information and Personnel Security Clearances University Policy 1122 FERPA Compliance University Policy 1125 Identity Theft Prevention Program University Policy 1141 Export Controls and Sanctions Compliance University Policy 1301 Responsible Use of Computing University Policy 1305 Electronic Security Incidents University Policy 1306 Banner and Related Administrative Systems Security University Policy 1307 Procurement and/or Development of Administrative Systems/Applications University Policy Number 1311 Information Technology Security Program University Policy 1316 Controlled Unclassified Information University Policy 1413 Continuity of Operations Planning) University Policy 2106 Purchase of Goods and Services University Policy 2110 Payment Card Security University Policy 2221 Background Investigations

	University Policy 2224 Recruitment and Hiring of University Employees
DOCUMENT CONTROL NUMBER	ITS.ITS-STD003
LAST REVIEWED DATE	12/9/2024
APPLIES TO	The controls in this standard apply to all information systems in use by George Mason University, whether on-premises or externally hosted. The criteria used to determine the appropriate category are detailed in IT Risk Assessment Procedure. The High category includes three subsets: • **CUI**: Data and systems subject to Federal Government regulations concerning Controlled Unclassified Information (CUI) as described in University Policy 1316 Controlled Unclassified Information. • **PCI DSS**: Data and systems that the IT Security Office has determined to be part of the university's credit card processing functions and in-scope for the Payment Card Industry Data Security Standard requirements, per University Policy 2110 Payment Card Security. • **16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]:** Data and information systems that are subject to the requirements of the Gramm-Leach-Bliley Act (GLBA). These include systems that access or store Federal Tax Information (FTI) which requires to be labelled/tagged for **CUI** (See MP-3). Systems that have been determined to be neither a High nor Moderate category are considered to be Low. Each control statement in this standard is labeled to indicate the Federal Information Processing Standards (FIPS) 199 based (Standards for Security Categorization of Federal Information and Information Systems) category of systems to which it applies: • High (H) • Moderate (M) • Low (L) The inventory of the systems and their classifications (Sensitive IT Systems status, FIPS 199, and risk profile) are available in the Archer Integrated Risk Management (IRM) tool. Some control statements *apply only to particular subsets* of High category systems; these control statements are prepended with "**CUI Only**," or "**PCI DSS Only**" as appropriate. Control statements that are applicable for GLBA,

	are tagged as '**GLBA**' or '16 CFR 314.4 **[GLBA 'Standards for Safeguarding Customer Information' Relevant]'.** Categorization for externally hosted systems is performed during service acquisition, by the Architectural Standards Review Board (ASRB). The Information Technology Services (ITS) organization is responsible for monitoring compliance of High category external systems in accordance with the Third-Party Risk Management Process.

NOTICE TO ALL USERS

- **This Standard is in effect as of the date of publishing; however, it is recognized that system and control owners may need time to align their compliance activities to this updated Standard. Therefore, a period of one year from the date of publishing will be allowed for adoption and implementation of the controls to assist with this transition.**
- **For links to the department level documents, you must already be signed into the appropriate portal such as Microsoft365 (M365), to access the document.**

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
1.0 (Final)	7/1/2019	IT Process & Planning / Randy Anderson ITSO / Curtis McNay	Initial Release
2.0.0 (Draft)	7/31/2023	IT Risk & Compliance / Randy Anderson ITSO / Curtis McNay	Update to align with NIST SP 800-53 r5 standard
2.0.1 (Draft)	11/1/2023	IT Risk & Compliance / Noor Aarohi & Randy Anderson	Minor updates based on comments from IT Directors
2.0.2 (Draft)	12/4/2023	IT Risk & Compliance / Noor Aarohi	Removed RA-3(1) Supply Chain Risk Assessment from High baseline
2.0.3 (Draft)	1/4/2024	IT Risk & Compliance / Noor Aarohi	Additional note added to CA-8 for clarity
2.0.4 (Draft)	1/12/2024	IT Risk & Compliance / Noor Aarohi	Updated 'Notice' for clarity
2.0.5 (Draft)	1/23/2024	IT Risk & Compliance / Cindy Kim & Noor Aarohi	Reformatted using current standard template, added a Table of Contents, and corrected document control numbers for some referenced ITS documents. Added help text under 'Notice to All Users'
2.0.6 (Draft)	1/30/2024	IT Risk & Compliance / Noor Aarohi	Reconcile to the updated baselines.
2.1 (Final)	12/9/2024	IT Risk & Compliance / Noor Aarohi	Updated to map controls to GLBA Standards for Safeguarding Customer Information, introduce definition for 'Sensitive IT System' and other relevant definitions. Added PM-09 to program level controls. Updated noted CP controls to apply to only when 'Availability'

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
			requirement in FIPS 199 analysis is 'High'. George Mason branding and usage updates applied.

TABLE OF CONTENTS

ABOUT THE STANDARD

PURPOSE

This standard details specific requirements that must be employed to support the university's Information Security Policy. The requirements are categorized in 16 "Control Family Standards" and 4 Program Level control areas practices drawn from NIST SP 800-53 Rev. 5. Some controls are required only for particular categories of systems and/or data, as noted in the corresponding descriptions.

INTERPRETATION

The applicable controls for any university information system are defined by the level of potential impact and risk presented by that system as described above. The word "should" in a control statement indicates a recommendation; controls using the word "must" are requirements that are to be followed unless an exception has been approved. The Information Technology Security and the IT Risk and Compliance offices will work with departments to interpret requirements, and to ensure that suitable controls are in place for departmental information systems.

REQUIREMENTS

This standard applies to all university faculty, staff, students, visitors, and contractors to the extent they access or use George Mason systems, data, host systems or information for George Mason University. This Standard governs the privacy, security, and confidentiality of university data, especially Highly Sensitive Data (HSD), and the responsibilities of institutional units and individuals for such data. Questions regarding applicability, implementation, or exception requests should be referred to the Information Technology Security Office. All exception requests must include an explanation of the business and/or academic reasons for the exception. All exceptions must be approved by the appropriate policy, standard, process, or procedure owner.

Note: Some of the reference documents that are hyperlinked in this Standard may be located in file repositories that require special access. For documents that are behind Virtual Private Network (VPN) or Single Sign-On access, users must be logged into the VPN or the appropriate application before clicking on the link. Requests for those documents should be forwarded to Information Technology Services by contacting the IT Support Center at 703-993-8870.

DEFINITIONS

ACRONYM/TERM	DEFINITION
Controlled Unclassified Information (CUI)	As defined by Presidential Executive Order 13556, and 32 CFR 2002, Controlled Unclassified Information 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. All CUI is not Federal Tax Information (FTI). For FTI that is CUI, please refer to : https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-05-12/access-and-use-federal-tax-information-fti-federal-student-aid-programs-beginning-2024-25-fafsa-processing-cycle-updated-april-18-2024).
Critical Function	An operation or task that; (i) supports one or more of the mission essential functions (Public Safety, Education, or Research) or is required for compliance and (ii) without the operation or task continuing within 30 days there would be a cascading effect or detrimental harm to the institution.
GLBA	The Gramm Leach Bliley Act (GLBA) applies to financial institutions and includes privacy and information security provisions designed to protect consumer financial data. This law applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. Regulations include a Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314), both enforced by the Federal Trade Commission (FTC) for higher education institutions. Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). The Safeguards Rule was promulgated in 2002, with compliance required in May 2003.
Qualified Individual	The University Policy Number 1311: Information Technology Security Program establishes the Chief Information Security Officer (CISO) or equivalent staff leading the information security function at George Mason as the Qualified Individual per Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., 15 C.F.R. § 314.4 (a). Additionally, per 314.4(i), The Qualified Individual must report in writing regularly, at least annually, to the board of directors or equivalent governing body ('Board of Visitors' at George Mason) on the overall status of the information security program and compliance, including material matters related to the program.
Highly Sensitive Data (HSD)	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.
Mission Essential Function (MEF)	George Mason has identified mission essential functions (MEF) within its university-level Continuity of Operations Plan (COOP), based on the financial, economic, safety, or long-term effect of each function on the regional or state continuity and strategic plans. MEF is comprised of critical functions that are detailed in the Unit COOP Plans.

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 IT System	A "High" (as per FIPS 199 categorization criteria) category system that stores Protected data (as defined in the Data Stewardship Policy) and is an "Essential Component" of one or more Critical Functions.
Essential Component	A Component that is absolutely necessary. Without this component the Critical Function will not be operational, not even in a degraded state.

STANDARD

ACCESS CONTROL (AC)

AC-1 POLICY AND PROCEDURES (H, M, L)

Policy Statement: The university must limit system access to authorized users, processes acting on behalf of authorized users, or authorized devices. Authorization to use university computing services and applications is based on an individual's affiliation with George Mason, that individual's role and responsibilities, and the designated category of the system. Requests for privileged access beyond basic user levels are generally initiated by the individual's department or unit; approval must be based on the requester's job duties and role and limited to the minimum level of access required to perform those duties.

Managers/heads of departments and units are responsible for ensuring that access control procedures for systems and applications under their scope of control are created, maintained, and disseminated to relevant personnel. These procedures should be reviewed at least annually, or when required to address changes to the environment.

All authorized users of George Mason's computing resources are required to comply with University Policy 1301 Responsible Use of Computing and the following policies where applicable:

- University Policy 1114 Data Stewardship
- University Policy 1118 Compliance with the Health Insurance Portability and Accountability Act (HIPAA)
- University Policy 1122 FERPA Compliance
- University Policy 1119 Classified Information and Personnel Security Clearances
- University Policy 1306 Banner and Related Administrative Systems Security
- University Policy Number 1311 Information Technology Security Program
- University Policy 1316 Controlled Unclassified Information

AC-2 ACCOUNT MANAGEMENT

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- The university assigns students and employees a Patriot Pass account which serves as a digital identity for George Mason's single-sign-on authentication environment. By default, this account provides a basic level of access to email, student/employee information, timesheets, learning systems, and other university services. The following affiliation classes are defined:
    - **Employee:** an individual having a current, active job record in the Human Resources (HR) system, including faculty, classified staff, and wage staff.

  - **Student**: an individual who is enrolled and pursuing an academic program or class.
  - **Student Worker**: a student who is also employed by the university. As a subset of the Employee class, access to applications varies depending on the individual's assigned role.
  - **Alumni:** an individual having Graduated status in a valid academic program.
  - **Contractor/Affiliate:** an individual granted time-based access to systems as appropriate to perform specific activities required by their role or function at George Mason. Access is terminated once the affiliation ends.
  - **Retiree:** an individual who has retired from employment at George Mason.
  - **Emeritus:** a special designation for faculty that is assigned by the Provost; an individual having this status retains additional access beyond that of a standard Retiree, as determined by the Provost and/or their affiliation with an academic unit.
- Campus units are responsible for ensuring that George Mason personnel records reflect new hires, terminated personnel, and changes in personnel status or position.
- Privileged access beyond basic user levels requires prior approval by the relevant authority, in accordance with documented approval processes.
- System or application administrators, and others requiring enhanced access beyond that afforded by their Patriot Pass account, must have a unique logon identifier for accountability. Role and group accounts are to be used only where necessary and must provide individual accountability.
- All privileged access must be disabled when an employee transfers to a new position within the university. Services and access required for the new position must be requested by the new supervisor and appropriate Data Steward. [AC-2(13)]
- Each George Mason department is responsible for disabling access to departmentally controlled resources upon a transfer or termination. It is the supervisor's responsibility to ensure that a former employee's electronic files have been retained as necessary and protected from unauthorized access.
- Each George Mason department is responsible for reviewing accounts used by their personnel (staff, contractors/affiliates, student wage, wage or any other workers or volunteers) for compliance with account management requirements, periodically. Annual reviews are strongly recommended.
- Student Access:
  - Once the Office of the University Registrar determines a person to be a student, the student's Patriot Pass UserID is activated.
  - Students are provided access to a George Mason email account, library services, and current academic computing resources including the Learning Management System and other applications.
  - A student's access to academic resources stays active based on the student's status. The owner of each application is responsible for determining whether the application should remain available to students that are no longer active.
- Alumni Access: Former students who graduated from a George Mason academic program after December 2010 retain their Patriot Pass account and access to George Mason email indefinitely*. Email accounts are not available for alumni who graduated before 2010.
  *Future enhancement will require these users to review and renew their account entitlement at least annually.
- Retiree Access: Retirees retain access to their George Mason email account, and to their employment and tax records.

<u>Additional Control Requirements for High and Moderate Systems (H, M)</u>

The following set of controls apply to all systems which have been classified as either High or Moderate:

- Access control processes are described. This information may be specified in the System Security Plan, or the operational procedures, or other supporting documents. Such processes must include procedures for adding and removing members to any group accounts, description of types of permitted accounts and privileged access levels, and authorization procedures for privileged access.
- Privileged accounts are approved by the System Owner or designee and reviewed at least annually.

- Temporary and emergency accounts are accounts intended for short-term use and may be established as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Emergency accounts are established in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes.
- System administrators shall have both administrative and regular user accounts and must use their administrative accounts only when performing tasks that require administrative privileges.
- System Owners must ensure that each information system under their control has at least two individuals with administrative access, to provide continuity of operations.
- Accounts of individuals who have been determined to pose a significant security risk must be disabled immediately, within no more than 24 hours of discovery or determination of the risk. [AC-2(13)]

Additional Control Requirements for High Systems (H)

The following additional controls apply only to systems that have been classified as High:

- Managers and/or System Owner are responsible for disabling accounts having privileged access. These must be disabled within 72 hours when no longer needed, e.g., when triggered by employment status, role changes, or application changes. In cases of "termination for cause," the account must be disabled immediately. [AC-2(3)]
- Accounts having privileged access which have not been used in the past **six months** must be disabled, unless a documented and approved business reason exists. [AC-2(3)]
- Shared accounts are prohibited. The use of group and role accounts should be limited and must provide individual accountability. [AC-2(9)]
- **CUI Only:** Access to CUI environment(s) and system(s) is authorized via specific CUI account request processes. 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 Project-based 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.
    - User CUI credential must be disabled after 60 days of inactivity.

AC-3 ACCESS ENFORCEMENT

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Access enforcement mechanisms may be employed at the application and/or service level.

Additional Control Requirements for High Systems (H)

- **CUI Only:** Each user is assigned a unique account that may not be shared with anyone else. This account is required for access to the CUI environment. Role-based access control limits the user's access to the specific systems, data, and system actions for which they have documented authorization.

AC-4 INFORMATION FLOW ENFORCEMENT

General Controls (H, M, L)

- ITS must define and implement information flow control policies at network boundaries. Examples include blocking outside traffic that claims to originate from within George Mason's network and limiting information transfers between systems in different security domains.
- System owners and administrators must not circumvent flow control measures and network restrictions implemented by ITS. New business communications requirements that would require firewall policy adjustments must be evaluated via a new risk assessment.

- System and network architecture designs must provide technical mechanisms to enforce information flow policies.

Additional Control Requirements for High Systems (H)

- Firewalls and other technical enforcement mechanisms must be configured to control the flow of Protected Data between systems and security domains. Flow control policies must be established when information systems are brought online, and when applications and/or use cases change.
- **CUI Only:** Firewalls and other technical enforcement mechanisms must be configured to control the flow of CUI in accordance with approved authorizations.

AC-5 SEPARATION OF DUTIES

General Controls (H, M, L)

- System owners and designees are responsible for identifying relevant information technology roles for users of information systems under their control. Where feasible, roles and account privileges must be configured such that operational and support functions are separated into distinct jobs to prevent a single person from intentionally or unintentionally causing loss of data or services.
- Individuals responsible for setting control policies should also not be responsible for implementing the technical configurations that support those policies.

Additional Control Requirements for High Systems

- The owner of each High system, or designee, must indicate which roles and duties pertaining to that system are required to be assigned to separate individuals. This information may be specified in the System Security Plan or the operational procedures, or other supporting documents.

AC-6 LEAST PRIVILEGE

General Controls (H, M, L)

- Users and processes acting on behalf of users are to be allowed only to the minimum privilege level required to accomplish assigned tasks, in accordance with the university's mission and business functions.
- System owners and designees must explicitly authorize access to the following security functions, either by role or by individual accounts:
    - Assigning server/system administrator accounts
    - Configuring rules for routers, firewalls, load balancers, and other network devices
    - Configuring vulnerability scanners, intrusion detection systems, central log servers, and other security equipment managed by the Information Security Office
    - Assigning privileged accounts for database access
    - Storing Highly Sensitive Data
    - Configuring audit logging functions
- Users having privileged system administrator or database administrator accounts must use non-privileged accounts for tasks that do not require elevated privileges. [AC-6(2)]
- Authorized access by role must be documented in the pertinent System Security Plan, or the operating procedures, or other supporting documents. [AC-6(1), AC-6(5)]

Additional Control Requirements for High and Moderate Systems (H, M)

- Privileged access accounts on High systems must only be granted to George Mason employees, or to external users under contractual control of the university. [AC-6(6)]
- System owners and designees must review privileged access accounts for information systems under their control, on at least an annual basis. Privileges must be reassigned or removed in a timely manner when employee assignments change. [AC-6(7)]
- Use of privileged access and functions must be logged and monitored to detect potential misuse. [AC-6(9)]
- Information systems must be configured to prevent non-privileged users from executing privileged functions. [AC-6(10)]

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

General Controls (H, M, L)

- Where technically feasible, information systems must enforce a limit of 10 consecutive invalid login attempts by a user during a 15-minute period, and automatically lock out further access attempts by the same account for a period of at least five minutes when the maximum number of unsuccessful attempts is exceeded.

Additional Control Requirements for High and Moderate Systems (H, M)

- Unsuccessful login attempts to elevated/root privilege accounts must be limited to five unsuccessful attempts during a 15-minute period, prior to lockout for a period of five minutes.
- **CUI Only**: Unsuccessful login attempts must be limited to five unsuccessful attempts during a 15-minute period, prior to lockout for a period of five minutes.

AC-8 SYSTEM USE NOTIFICATION

General Controls (H, M, L)

- Information systems should display a system use notification prior to login, if technically feasible. The notification statement must include the following points:
  - User is accessing an information system owned or managed by George Mason.
  - User agrees to abide by University Policy 1301 Responsible Use of Computing.
  - System usage may be monitored, recorded, and subject to audit.
  - Unauthorized use is strictly forbidden and may constitute a violation of state and/or federal law.
  - Use of the system indicates consent to monitoring and recording.
- If the system to be accessed contains student records, the system use notification must also indicate acceptance of the Student Information Security Statement.
- System use notifications are used only for access via login interfaces with human users and are not required when such human interfaces do not exist.

Additional Control Requirements for High and Moderate Systems (H, M)

- System use notifications are required for all High and Moderate systems, including root access for security and network appliances and servers.

AC-11 DEVICE LOCK

General Controls (H, M, L)

- Information system user interfaces should be configured to automatically initiate a device lock after no more than 30 minutes of inactivity or upon user request.
- Device locks must implement pattern-hiding displays to conceal previously displayed information with a publicly viewable image. [AC-11(1)]
- Centrally managed workstations must be configured to initiate device locks with pattern-hiding displays after 30 minutes of inactivity.
- Centrally managed workstations should remain locked until the user re-establishes access or reaches out to IT support to regain access.

Additional Control Requirements for High and Moderate Systems (H, M)

- User interfaces to High and Moderate systems must be configured to automatically initiate a device lock with pattern-hiding display after no more than 30 minutes of inactivity or upon user request.

AC-12 SESSION TERMINATION

General Controls (H, M, L)

- Information systems should be configured to automatically terminate a user session after a defined period of inactivity. Session termination terminates all processes associated with a user's logical session except

those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Additional Control Requirements for High and Moderate Systems (H, M)

- High and Moderate systems must be configured to automatically terminate a user session, as described above, after a period of inactivity not to exceed 12 hours. Inactivity period duration, and any other conditions triggering session termination, must be described in the System Security Plan or the operational procedures, or other supporting documents.
- High and Moderate systems must provide the capability for user-initiated session logout whenever authentication is used to access the system and must display an explicit logout message to the user indicating that the communication session has been terminated.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHORIZATION

General Controls (H, M, L)

- Websites and information services intended to be publicly accessible may allow non-privileged access by users inside and outside the university without requiring unique identification and authorization.

Additional Control Requirements for High and Moderate Systems (H, M)

- High and Moderate systems may allow certain user actions to be performed without identification or authentication, if such actions are specifically defined in the System Security Plan, or the operational procedures, or other supporting documents.

AC-17 REMOTE ACCESS

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- Remote access to the university's network and information systems is only permitted for authorized users.

Additional Control Requirements for High and Moderate Systems (H, M)

- Remote access to High and Moderate systems is monitored and logged. [AC-17(1)]
- All remote access to High and Moderate systems must conform to conditions and restrictions described in George Mason's Remote Access User Standard and Remote Access Device Standard. [AC-17(2), AC-17(3)]
- Execution of privileged commands, and access to security-relevant information, via remote access is permitted only as documented. This information may be specified in the System Security Plan, operational procedures, or other supporting documents. [AC-17(4)]

AC-18 WIRELESS ACCESS

General Controls (H, M, L)

- The university provides access to several wireless (aka Wi-Fi) networks in facilities owned and/or occupied by George Mason. Access to each wireless network type is authorized based on the user's affiliation with George Mason. In accordance with University Policy 1301 Responsible Use of Computing, all new wireless networks must be pre-approved by Information Technology Services via a Network Consultation Request.
    - Eduroam network: This network provides secure Wi-Fi access to anyone having valid account credentials at George Mason or any other educational or research institution that participates in the Eduroam global initiative. The network uses 802.1x authentication and WPA2 Enterprise/AES encryption. Authorization is based on the user's Patriot Pass single-sign-on account.
    - University's MASON-SECURE network: Provides Wi-Fi services for faculty, staff, contractors, and vendors having George Mason Patriot Pass credentials. All instantiations of this network use 802.1x authentication and WPA2 Enterprise/AES encryption. Authorization is based on the user's Patriot Pass single-sign-on account. ***NOTE:*** *The MASON-SECURE network is being phased out; the preferred wireless network is now* **eduroam**.
    - University's MASON Guest network: Unencrypted public Wi-Fi network that enables campus guests to access the Internet and publicly available information resources at George Mason. Guest

accounts are self-provisioned via a captive portal and are valid for a period of seven days; guests may re-register after their account expires. The network supports up to three concurrently connected devices per account.

- Residential Halls network (aka ResNet): Provides Wi-Fi services for resident students, Residence Hall guests, gaming systems, and Wi-Fi enabled equipment located in the Residence Halls. Access is provisioned via the supporting vendor's portal. Authorization for students is based on the client's Patriot Pass account; vendor equipment must be pre-authorized by Information Technology Services.
- Special-purpose networks: A number of private networks have been created to serve unique needs of vendors, researchers, and campus services for which none of the above network types are suitable. Each special-purpose network may have unique access, authorization, and security provisions based on their needs and risk level. All such special-purpose networks must be approved in advance and configured with guidance from the Information Technology Security Office. Network documentation must describe purpose, location, authorized users, and responsible authorities.

Additional Control Requirements for High and Moderate Systems (H, M)

- Instantiation of new wireless networks within the network boundary/security domain of High and Moderate systems is prohibited by default and permitted only by exception after approval by the Information Technology Security Office.
- Wireless networks used to access High and Moderate systems must require authentication and encryption. [AC-18(1)]
- **CUI Only**: Instantiation of wireless networks within the network boundary of CUI environments or systems is prohibited. Exceptions require approval by the Information Technology Security Office.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

General Controls (H, M, L)

- The university permits personally owned mobile devices to access campus information resources based on the user's affiliation and Wi-Fi network access as described in AC-18.

Additional Control Requirements for High and Moderate Systems (H, M)

- All George Mason-owned mobile devices must be configured to use full-device encryption when supported by the device.
- **CUI Only**: Mobile devices are prohibited by default from connecting to CUI systems. Any exception requires full device encryption with key escrow and must be approved by the Information Technology Security Office. [AC-19(5)]

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

General Controls (H, M, L)

- The university permits external connections to sites accessible on the public Internet, with the exception of certain sites that are known or suspected of hosting malware. All Internet access using George Mason facilities is permitted only in accordance with university policies, and state and federal regulations.
- Transfer of Highly Sensitive Data between George Mason networks and unauthorized external sites is prohibited by default. Such transfers are permitted only in the context of trust relationships, contractual conditions, and technical controls approved by the Architectural Standards Review Board and the appropriate Data Steward. Information systems operated by other Commonwealth agencies or entities under the Commonwealth's contractual control may be allowed when there are pre-existing sharing/trust agreements or when specified by applicable Commonwealth laws, Executive Orders, or directives. [AC-20(1)]
- Processing and/or storage of Highly Sensitive Data on external systems, including personally owned devices, is prohibited unless approval has been granted by the ITSO. [AC-20(1), AC-20(3)]

Additional Control Requirements for High Systems (H)

- **CUI Only**: Any connection between the CUI environment and external systems is prohibited by default, except via approved remote access protocols as documented in the System Security Plan, or the operational procedures, or other supporting documents.
- **CUI Only**: CUI data must not be stored on portable storage devices, with the exception of approved backup mechanisms as documented in the System Security Plan, or the operational procedures, or other supporting documents. [AC-20(2)]

AC-21 INFORMATION SHARING

General Controls (H, M, L)

- As described in AC-20, transfer of Highly Sensitive Data between George Mason networks and unauthorized external sites is prohibited. Such transfers are permitted only in the context of trust relationships, contractual conditions, and technical controls approved by the Architectural Standards Review Board and the appropriate Data Steward, or under pre-existing trust relationships with other Commonwealth agencies or entities under their contractual control.

AC-22 PUBLICLY ACCESSIBLE CONTENT

General Controls (H, M, L)

- Information to be made publicly accessible must be released only in accordance with all applicable university policies as listed under AC-1 and federal and state regulations such as Code of Virginia § 2.2-3700 and exemptions therein.

Additional Control Requirements for High Systems (H)

- **CUI Only**: Processing or sharing of CUI on or via publicly accessible systems is prohibited.

AWARENESS AND TRAINING (AT)

AT-1 POLICY AND PROCEDURES

Policy Statement: All George Mason personnel who interact with the university's non-public information resources are required to complete the IT Security Awareness training commensurate with their roles at the university. The Vice President for Information Technology establishes training requirements for the IT Security Awareness training for all members of the university community based on guidance from the Information Technology Security Office. Personnel who fail to comply with training requirements must have their access disabled until compliance is achieved.

Related Documentation:
ITS.ITRC-PRS002 IT Security Awareness Training

Scope
Security Awareness Training requirements apply to all persons who are issued credentials to access non-public information resources under the control of George Mason, including but not limited to current employees and authorized contractors.

AT-2 SECURITY AWARENESS

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- Information Technology Services reviews Security Awareness training content and requirements annually, updates as necessary, issues annual notices of refresher training, ensures the appropriate training modules are made available in the university's Mason Learning, Evaluation, and Performance System (MasonLEAPS), and tracks compliance.

- The general Security Awareness Training program must include modules on social engineering and insider threats. [AT-2(2), AT-2(3)]
- New faculty, staff, contractors, and vendors must complete prescribed security training within 14 days from their actual start date after receiving George Mason authentication credentials (NetID, Patriot Pass password, and Two-Factor Authentication). Faculty and staff must also complete annual refresher training.

AT-3 ROLE-BASED SECURITY TRAINING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- Security Awareness Training is mandated for all George Mason faculty, staff, authorized contractors, and any other persons that are issued credentials to access non-public information resources under the control of George Mason.
- Employees in the following roles have additional role-specific information security training requirements:
    - Data custodians of Highly Sensitive Data (HSD)
    - Employees in a software application development role
    - Active Directory administrators
    - Application administrators
    - Database administrators
    - Windows Server administrators
    - Linux server administrators
    - Network administrators
    - Organizational files owners
    - IT Security professionals
    - Health records privacy and security training for George Mason offices and centers that are designated as Health Care Components, per University Policy 1118 Compliance with the Health Insurance Portability and Accountability Act (HIPAA), is managed and tracked by each Health Care Component.
    - Training requirements for employees who handle or have access to education records as defined by the Family Educational Rights and Privacy Act (FERPA) are overseen by the Office of the University Registrar.
    - Principle Investigators, system administrators, and other users of systems that contain CUI must be trained in data handling and use of the CUI environment before accessing CUI systems, and annually thereafter. Information Technology Services provides technical training on the CUI environment; the Office of Research Integrity and Assurance provides training on data handling and export controls compliance based on the needs of each research project.
    - Role-based training materials must be reviewed annually, and when warranted by regulatory or technology changes.

AT-4 SECURITY TRAINING RECORDS

General Controls (H, M, L)

- Security Awareness Training records for employees are maintained in the university's learning management system of record.
- Training records for role-specific training that is not facilitated using the university's learning management system are managed by the university office that is responsible for that training.
- Historical training records are retained for the appropriate period of time in accordance with records retention schedules issued by the Library of Virginia, as required by University Policy 1102 Records Management

AUDIT AND ACCOUNTABILITY (AU)

AU-1 POLICY AND PROCEDURES

Policy Statement: 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. System owners and system administrators are responsible for ensuring that information systems under their control are configured and managed in accordance with the requirements in this section, and that logging configurations are clearly documented in operational procedures.

Related Documentation:
University Policy 1102 Records Management

Scope
The controls in this section are required for High and Moderate systems and are recommended as best practices for Low category systems.

AU-2 EVENT LOGGING
16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]
Control Requirements for High and Moderate Systems (H, M)

- High and Moderate systems must be capable of logging, at a minimum, the event types specified in the ITS Logging Standard (ITS.ITSO-STD001). The IT Security Office may require additional logging based on the risk level and functions of the information system.
- High systems must have the ability to forward logged events to the ITS centralized log repository.
- The IT Security Office may require certain Moderate systems to forward logged events to the ITS centralized log repository; if established as a result of a risk assessment.

AU-3 CONTENT OF AUDIT RECORDS
16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]
Control Requirements for High and Moderate Systems (H, M)

- Audit records must contain, to the extent supported by the information system, the following information:
    - The type of event that occurred
    - When the event occurred
    - Where the event occurred
    - Source of the event
    - Outcome of the event
    - Identity of any individuals, subjects, or objects/entities associated with the event
- Additional information to be incorporated into audit records may be identified during system risk assessments and must be added to the configuration when required by the IT Security Office. [AU-3(1)]

AU-4 AUDIT STORAGE CAPACITY
Control Requirements for High and Moderate Systems (H)

- System administrators must allocate sufficient storage capacity to meet log data retention requirements.
    - If log data is being forwarded to the ITS centralized log repository, local logs may be purged after transmission.
    - If logs are not being forwarded to the ITS centralized log repository, then log records must be available for immediate review and analysis as per the applicable Library of Virginia requirements. [AU-4(1)]

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES
Control Requirements for High Systems (H)

- System administrators must configure systems for which they are responsible to alert when log processing stops unexpectedly.
- When a log processing failure is detected, the system's administrator must investigate and implement corrective actions no later than the next available maintenance window.

- When the IT Security Office detects that log records from a system have unexpectedly stopped forwarding to the centralized log repository, the engineer or analyst responsible for monitoring must notify the relevant system administrator as soon as possible and assist them with troubleshooting, as necessary.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High and Moderate Systems (H, M)

- System administrators must monitor and review audit logs for systems under their control. Frequency of reviews may be defined on a per-system basis. Logs or other evidence must be kept to validate that the reviews have taken place. When systems are configured to forward log records to the ITS centralized log repository, monitoring responsibilities are shared between the system's administrator and IT Security Office analysts.
- Log records that exhibit indications of unusual or inappropriate activity must be brought to the attention of the IT Security Office for review and investigation. Examples include, but are not limited to, the following:
  - Unusual login events
  - Unauthorized data or content manipulation
  - Anomalous high web application or database activity
  - Unauthorized or unusual transactions
  - Unauthorized changes in user privilege level
- The Chief Information Security Officer (CISO) or equivalent leading the information security function is responsible for authorizing targeted and/or organization-wide communications regarding current threats and issues revealed during audit record analysis and escalating to university leadership when appropriate.
- Audit log records that are processed by the ITS centralized log repository are monitored in real time, and high-profile events trigger alerts to IT Security Office analysts. [AU-6(1)]
- When threat levels change based on evidence from credible sources, audit log review, analysis, and reporting must be reevaluated and modified to reflect the current risk level and threat environment.
- The ITS centralized log repository applies correlation rules and automatically alerts security analysts when suspicious events are indicated. [AU-6(3)]

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

Control Requirements for High and Moderate Systems (H, M)

- Tools and technology used to implement the ITS centralized log repository or any similar capability in the distributed IT units, must support on-demand audit record review, analysis, and reporting. The original content and time ordering of audit records must be protected from alteration or corruption, and be available for use in incident response investigations.
- Audit record reporting tools must provide customizable capabilities to process, sort, and search audit records for events of interest. [AU-7(1)]

AU-8 TIME STAMPS

Control Requirements for High and Moderate Systems (H, M)

- Systems must be configured to generate time stamps for audit records based on their internal system clocks.
- Systems must be configured to generate log record time stamps using the Eastern Time Zone (EST/EDT) if the system is technically capable of doing so. If this is not feasible, the system must be configured to use Coordinated Universal Time (UTC).

AU-9 PROTECTION OF AUDIT INFORMATION

General Controls (H, M, L)

- System administrators must take measures to protect audit records and audit logging tools in their care from unauthorized access, modification, and deletion. Audit records must be backed up at least weekly unless the data is being sent to a secondary system such as the ITS centralized log repository.

- If unauthorized access, modification, or deletion of audit information is detected or suspected, system administrators must immediately inform the IT Security Office. The IT Security Office is responsible for follow-up and investigation.
- Management of system audit log functionality must be restricted to authorized system administrators. Privileged access to the ITS centralized log repository is restricted to authorized IT Security Office personnel. [AU-9(4)]

AU-11 AUDIT RECORD RETENTION

General Controls (H, M, L)

- System audit logs must be managed and retained in accordance with University Policy 1102 Records Management.

Additional Control Requirements for High and Moderate Systems (H, M)

- The ITSO maintains a retention schedule for system audit records that are forwarded to the ITS centralized log repository. Retention periods vary based on source, purpose, volume, and risk level.
    - **PCI DSS Only**: Logs for the PCI environment must be retained for a minimum of 365 days.

AU-12 AUDIT RECORD GENERATION

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High and Moderate Systems (H, M)

- System administrators must configure systems under their control to provide audit record generation capability meeting the requirements of AU-2 and AU-3.

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

CA-1 POLICY AND PROCEDURES

Policy Statement: The university must develop, disseminate, and periodically review/update documented procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and associated assessment, authorization, and monitoring controls. On authority from the Vice President for Information Technology, the Information Technology Security Office (ITSO) establishes requirements and procedures for risk assessment and authorization (see IT Risk Assessment Procedure.) Ongoing monitoring is a joint responsibility of the ITSO and the IT Risk and Compliance Office. System administrators are responsible for ensuring that risk assessments have been performed on each system under their control.

Related Documentation:

IT Risk Assessment Procedure

Scope

The controls in this section apply to all systems that have been categorized as High.

CA-2 CONTROL ASSESSMENTS

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- The IT Risk and Compliance Office within ITS is responsible for developing control assessment plans and procedures that address both on-premise and external information systems that provide or support university services and data. Control assessment plans must be reviewed and approved by the Vice President and Chief Information Officer for centralized IT systems and processes, and by the Director IT or equivalent for the distributed IT areas. For colleges and departments that do not have a Director IT or equivalent, the control assessment plan may be reviewed and approved by the Vice President and Chief Information Officer.

- The Office of University Audit establishes schedules for periodic control assessments, performs assessments, and reports the results to the Vice President for Information Technology and the Chief Information Security Officer (CISO) or equivalent leading the information security function. Additionally, the university may also engage external assessors for control assessments. Departments may also conduct self-assessments or facilitated risk assessments that include assessment of controls, to [CA-2(1)]

CA-3 INFORMATION EXCHANGE

Control Requirements for High Systems (H)

- All dedicated connections between George Mason's network and external networks must be reviewed and authorized by the university. Examples of dedicated connections in-scope for this control include connections via leased lines or virtual private networks, dedicated connections to Internet service providers, and ongoing exchanges of Highly Sensitive Data with external databases or cloud services. Transitory, user-controlled connections such as email and web browsing are not in scope for this control.
- Data exchanges with external databases and/or cloud services must be authorized by the Architectural Standards Review Board (ASRB). The approved data elements and protocols are documented during the risk assessment within the ASRB process. Contractual agreements must include a Data Security Addendum describing responsibilities of the external party if the associated information exchanges involve Highly Sensitive Data.
- Dedicated connections to Internet service providers and other external networks must be documented with Interconnection Security Agreements. Such agreements must be periodically reviewed and updated when necessary.

CA-5 PLAN OF ACTION AND MILESTONES

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for Sensitive IT Systems

Control Requirements for High Systems (H) that are NOT designated Sensitive IT Systems – **encouraged but not required***

- Weaknesses and deficiencies identified during initial and subsequent control assessments and risk assessments must be documented in a Plan of Action and Milestones (POA&M).
- Each POA&M must be updated at least annually to show progress toward mitigating the identified deficiencies.

*Issues management may be used to track risk treatment decisions and actions.

CA-7 CONTINUOUS MONITORING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- The ITSO is responsible for performing periodic vulnerability scans against all internal networks that host systems deemed to be servers and notifying the appropriate system administrators when deficiencies are identified. The list of potential vulnerabilities must be updated before each scan based on the current threat environment.
- System owners are responsible for ensuring that the administrators for systems in their span of control follow established procedures for responding to vulnerability notifications and correcting deficiencies in a timely manner.
- System administrators must mitigate all vulnerabilities in compliance with the parameters and timeframes defined in the pertinent vulnerability and patch management procedures documents.
- Logs showing physical access to the Aquia Data Center and the Disaster Recovery Site must be reviewed at least monthly; unusual activity and unauthorized access attempts must be investigated by the ITS Facilities and Infrastructure Operations Manager and the ITSO.

- Chief Information Security Officer (CISO) or equivalent leading the information security, is responsible for reporting results of continuous monitoring activities to the Vice President for Information Technology periodically and when High events are identified.
- The System Owner is responsible for scheduling control assessments at least annually.
- IT Risk and Compliance is responsible for reporting results of the control assessments to ITS leadership. [CA-7(1)]

CA-8 PENETRATION TESTING

Control Requirements for High Systems (H)

- **PCI DSS Only:** Systems and networks that directly support capture and transmission of payment card data (i.e., in-scope for PCI DSS) must undergo penetration testing at least annually, and after any significant upgrades or modifications.

NOTE: Penetration tests may be commissioned for other (CUI or non-CUI) high systems following a risk-based approach, when required by regulation or if warranted as an outcome of a risk assessment.

CA-9 INTERNAL SYSTEM CONNECTIONS

Control Requirements for High Systems (H)

- Internal system interconnections enforced by firewall security zones must be established and periodically reviewed in accordance with defined procedures.
- Documentation should reflect characteristics, requirements, and justification for the interconnections.
- New systems and/or services must undergo a risk assessment and be assigned to an appropriate firewall security zone with documented firewall rules permitting the approved data flows.
- Common services having well-defined access requirements may be authorized by category, e.g., print services.

CONFIGURATION MANAGEMENT (CM)

CM-1 POLICY AND PROCEDURES

Policy Statement: The university must establish and maintain baseline configurations of in-scope systems throughout the system life cycle. Standard security controls must be established and enforced as a component of the baseline configuration. Configuration management procedures applicable to all in-scope systems must be made available to all system administrators, reviewed at least annually, and updated to be kept current.

Related Documentation:
ITS.ESD-POL001 ITS Change and Configuration Management Policy

Scope
The controls in this section apply to all High and Moderate systems that have been designated as subject to Configuration Management control as detailed in ITS.ESD-STD001, ITS Configuration Management Standard.

CM-2 BASELINE CONFIGURATION

Control Requirements for High and Moderate Systems (H, M)

- System administrators must develop, document, and maintain a current baseline configuration for each system. Baseline configurations include information about system components, network topology, standard software packages, software version and patch numbers, and configuration settings and parameters.
- Baseline configurations must include security configuration settings that factor in best practices and guidance from established benchmarks for the relevant platform.

- Baseline configurations must be updated when system components are installed, upgraded, or modified. Configuration change records must be retained for at least one year from the date the change was implemented.
- Devices that will be taken to high-risk locations may be required to employ additional controls, based on the results of a risk assessment. [CM-2(7)]

CM-3 CONFIGURATION CHANGE CONTROL

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- System administrators who are responsible for managing systems that are in-scope for Change and Configuration Management per ITS.ESD-STD001 ITS Configuration Management Standard must comply with current ITS configuration management processes and procedures, in alignment with ITS.ESD-POL001 ITS Change and Configuration Management Policy.
- Non-routine changes to High systems must be tested and validated before implementation, and a back-out/rollback plan developed for the event the change needs to be reversed. Security patches validated to come from the relevant vendors are considered "routine" and may not require advance testing, but must follow established change control procedures including back-out/rollback plans. [CM-3(2)]
- A representative from the ITSO must participate in the change control review and approval process. [CM-3(4)]

CM-4 IMPACT ANALYSES

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- System administrators and ITSO representatives must analyze and assess potential security impacts of proposed changes and bring any concerns forward before the changes are approved.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control Requirements for High Systems (H)

- Changes to hardware, firmware, and software components of the system must be implemented only by those persons designated by management to maintain the system. System access to initiate changes must be restricted to the authorized individuals.

CM-6 CONFIGURATION SETTINGS

Control Requirements for High Systems (H)

- Configuration settings that affect the security posture of the system must conform with one of these standards:
  - Relevant baseline recommendations for that platform as published by the Center for Internet Security
  - Relevant Security Technical Implementation Guides (STIG) as published by the Defense Information Systems Agency
- Deviations must be approved by ITSO. Manufacturer or vendor specifications and/or organizational requirements should be considered when approving deviations.

CM-7 LEAST FUNCTIONALITY

Control Requirements for High Systems (H)

- Systems must be configured to provide only essential capabilities, restricting the use of unnecessary ports, protocols, and services.
- Required capabilities and restricted ports, protocols, and services must be reviewed and revalidated at least annually, and when the base operating system version is upgraded. These reviews must be documented for audit purposes. [CM-7(1)]
- Licensed software must be used only in accordance with the pertinent license agreements and manufacturer's terms and conditions. [CM-7(2)]

- System administrators must comply with any restrictions and/or prohibitions issued by the ITSO concerning specific software programs or software sources. [CM-7(4)]
- If required in the System Security Plan, or the operational procedures, or other supporting documents, apply Allow All/Deny-by-Exception policy to prevent the use of unauthorized software or Deny All/Permit-by-Exception policy to allow the execution of authorized software. [CM-7(5)]

CM-8 SYSTEM COMPONENT INVENTORY

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- Components of systems that are in-scope for Change and Configuration Management must be accurately documented in the inventory and configuration management system established by ITS. The assigned system administrators are responsible for entering the inventory data and maintaining accurate entries in the system. The inventory listing must be updated as an integral part of component installations, removals, and system updates. [CM-8(1)]
- **CUI Only:** The CUI environment must be monitored for component changes. If unauthorized hardware, software, and firmware is detected it must immediately be isolated and network access disabled pending ITSO investigation. [CM-8(3)]

CM-9 CONFIGURATION MANAGEMENT PLAN

Control Requirements for Sensitive IT Systems

Control Requirements for High Systems (H) that are NOT designated Sensitive IT Systems – **encouraged but not required**

- The System Security Plan should include a Configuration Management Plan that addresses roles and responsibilities and describes the change and configuration management processes to be followed throughout the system's life cycle. Any additional steps to be implemented beyond the approved ITS Change and Configuration Management processes must be documented in the Configuration Management Plan.

CM-10 SOFTWARE USAGE RESTRICTIONS

Control Requirements for High and Moderate Systems (H, M)

- The system owner must ensure that software and associated documentation is used only in accordance with contract agreements, copyright laws, and licensing requirements.

CM-11 USER-INSTALLED SOFTWARE

Control Requirements for High and Moderate Systems (H, M)

- Software for personal (non-university) use is not allowed on George Mason purchased equipment.
- All software and associated documentation must be used only in accordance with contract agreements, copyright laws, and licensing requirements.

CONTINGENCY PLANNING (CP)

CP-1 POLICY AND PROCEDURES

Policy Statement: Units that are deemed critical to academic, research, and public safety operations of the university are required to maintain a Continuity of Operations Plan (COOP) documenting a means of achieving full or partial business operations for critical functions during a continuity event (ref: University Policy 1413 Continuity of Operations Planning). Information technology and applications that support critical business functions identified in each unit's COOP must have a corresponding Disaster Recovery Plan (DRP) which supports the restoration of those functions within the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameters detailed in the COOP.

Related Documentation:

University Policy 1413 Continuity of Operations Planning

Scope

The controls in this section apply to all information systems that directly support critical functions detailed in unit COOPs. By definition, information systems that are 'Essential' component of the university's critical functions are categorized as High.

CP-2 CONTINGENCY PLAN

Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

- The university COOP details George Mason's Mission Essential Functions, Recovery Time Objectives (RTO), roles and responsibilities, activation and reconstitution procedures, and the critical functions performed or provided by business units in support of the Mission Essential Functions.
- Business units that are responsible for one or more critical functions must ensure that the following plans are created, maintained, and made available to all key personnel that would be involved with a COOP activation:
    - Unit COOP detailing critical functions supported by the unit, as directed by the Office of Safety, Emergency, and Enterprise Risk Management. [CP-2(1)]
    - A Disaster Recovery Plan (DRP) for all information technology and/or applications required to support each critical function.
- Business units supporting critical functions must identify each critical function in the unit COOP, along with the corresponding RTO target as listed in the university COOP. [CP-2(3)]
- If a unit's critical function relies on technology assets and/or applications that are provided by another business unit, the business unit responsible for providing the required technology resources must create and maintain a DRP that supports recovery of the critical function. Both business units must negotiate and agree upon acceptable RTO and RPO parameters.
- Technology assets that are required to support critical functions may be described at a high level within the supporting unit's COOP; the DRP must include a detailed listing of critical system assets. [CP-2(8)]
- Associated operational procedures, key personnel listings, and vendor support contacts must be described in the DRP. This information must either be incorporated directly into the DRP, or referenced through pointers to readily available external sources. Potential disruption of normal information resources should be taken into account when determining how key personnel will be expected to access this information.
- Lessons learned from contingency plan testing, training, or actual contingency activities must be incorporated into subsequent contingency testing and training.

CP-3 CONTINGENCY TRAINING

Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

- System owners that are responsible for information systems supporting critical functions must ensure that system administrators are aware of their responsibilities as outlined in the unit COOP and DRP. All system administrators must be informed of their responsibilities upon assuming a COOP/DRP role, and those responsibilities must be reflected in their Employee Work Profile.
- If the information system supporting a critical function changes significantly due to upgrades, changing business needs, or other reasons the COOP and DRP must be updated. The roles and responsibilities of system administrators must be reviewed and updated at the time of the change, and appropriate technology training provided to ensure that the system administrators can effectively carry out their COOP and DRP assignments.

CP-4 CONTINGENCY PLAN TESTING

Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

- System owners are responsible for ensuring that disaster recovery plans are tested at least annually, or when major technology changes are implemented. The Office of Safety, Emergency, and Enterprise Risk Management should be informed of upcoming tests. [CP-4(1)]

- Physical failover and recovery testing must be performed at least once every two years; tabletop or simulation exercises may be substituted in the intervening years.
- Tests must involve use of the Disaster Recovery Site and any external sites or cloud services that would be involved during an actual emergency situation. [CP-4(2)]
- After each test is completed, an After-Action Report must be created documenting how and when the test was performed, personnel that were involved, and a description of the test results. The After-Action Report must be reviewed with owners of the affected systems, and shared with the university's Office of Safety, Emergency, and Enterprise Risk Management.

CP-6 ALTERNATE STORAGE SITE

Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

- System owners of High category systems are responsible for ensuring that a suitable alternate storage site is maintained and used as a backup facility for critical data.
- The alternate storage site must be sufficiently separated from the primary site to reduce its susceptibility to natural disasters and common infrastructure failure mechanisms. A different George Mason campus located in a different city, country, or state, is considered to be "sufficiently separated" for the purposes of this control. [CP-6(1)]
- The university unit(s) responsible for maintaining the alternate site must ensure that the site provides appropriate security controls to protect High category systems and data.

CP-7 ALTERNATE PROCESSING SITE

Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

- System owners of High category systems are responsible for ensuring that agreements and facilities are in place to provide an alternate processing site that supports the transfer and resumption of critical business functions within established recovery time and recovery point objectives.
- The alternate processing site must be sufficiently separated from the primary site to reduce its susceptibility to natural disasters and common infrastructure failures. A geographically separate (city, county, or state) George Mason campus is considered to be "sufficiently separated" for the purposes of this control. [CP-7(1)]
- The university unit(s) responsible for maintaining the alternate processing site must ensure that the facility provides appropriate security controls to protect High category systems and data, and essential supplies and configurations are in place to support resumption of critical business functions within established recovery time and recovery point objectives. [CP-7(4)]

CP-8 TELECOMMUNICATIONS SERVICES

Control Requirements for High Systems (H)

- ITS must establish the necessary agreements and infrastructure to provide alternate telecommunications services to maintain critical business functions in the event of a loss of primary telecommunications services.
- The alternate telecommunications capabilities must support recovery time objectives as defined in the university COOP.
- Alternate telecommunications services must be designed to reduce susceptibility to common infrastructure risks including natural disasters, structural failures, attacks, and errors of omission or commission. [CP-8(2)]

CP-9 SYSTEM BACKUP

Control Requirements for High Systems (H)

- System owners of High category systems are responsible for ensuring that the systems are backed up on a regular basis, and are capable of being restored within established recovery time and recovery point objectives. Appropriate system backups include user-level information, system-level information, and associated documentation.
- The university unit(s) responsible for maintaining the backup capabilities must employ mechanisms to protect the integrity of system backups.

- The backup system must be tested at least annually, and when significant changes are made to the technical environment. [CP-9(1)]
- **CUI and Sensitive IT Systems Only**: Backups for the environment must be protected with encryption. [CP-9(8)]

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

- System owners of High category systems where Availability requirement is 'High' and the university unit(s) responsible for maintaining the backup and recovery capabilities, must verify that the systems can be recovered and reconstituted to a known state within the parameters and targets established in the University Continuity of Operations Plan.
- Recovery is executing information systems contingency plans to restore critical business functions after a disruption. Reconstitution takes place following recovery, and includes activities for returning university systems to fully operational states. Reconstitution includes the deactivation of any interim system capabilities that may have been employed during the recovery operations.
- Transaction recovery mechanisms such as transaction rollback and journaling must be implemented for systems that are transaction-based, e.g., database management systems and transaction processing applications. [CP-10(2)]
- The university unit(s) responsible for maintaining the backup and recovery capabilities must provide an assessment of fully restored system functionality to the system owner(s), re-establish continuous monitoring activities, and prepare the system(s) for future disruptions.

IDENTIFICATION AND AUTHENTICATION (IA)

IA-1 POLICY AND PROCEDURES

Policy Statement: The university must ensure that the identity of information system users, processes acting on behalf of users, or authorized devices are verified before being allowed access to university information systems. A unique identifier must be assigned to each individual having a business, research, or educational need to access George Mason's information resources. Owners of information systems are responsible for ensuring that procedures to facilitate the implementation of this policy are developed, documented, maintained, and disseminated to system administrators.

Related Documentation:

University Policy 1125 Identity Theft Prevention Program

IA-2 IDENTIFICATION AND AUTHORIZATION (ORGANIZATIONAL USERS)

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- System owners and system administrators must ensure that George Mason's information systems are configured to uniquely identify and authenticate organizational users and processes acting on behalf of users. Organizational users include affiliation classes defined in AC-2. This control applies to all accesses other than (i) accesses that are authorized in AC-14 and (ii) accesses that occur through authorized use of group authenticators without individual authentication.
- Group and role accounts must follow the individual accountability provisions defined in AC-2.
- Network and remote access to privileged and non-privileged accounts must require multi-factor authentication and employ replay-resistant authentication mechanisms unless compensating controls are approved by the ITSO. [IA-2(1), IA-2(2), IA-2(8)]
- Acceptable multi-factor authentication options may vary based on the level of risk.

Additional Control Requirements for High Systems (H)

- Local access to High category systems by privileged accounts must require multi-factor authentication unless compensating controls are approved by the ITSO. [IA-2(1)]
- Acceptable multi-factor authentication options may vary based on the level of risk.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control Requirements for High category Systems (H)

- Certain High category systems and applications may require unique device identification and authentication before connections are permitted, based on the assessed risk level and business functions of the system. This requirement may be established during system risk assessment and documented in the System Security Plan, or the operational procedures, or other supporting documents.
- **CUI Only -** Device authentication must not rely solely on Internet Protocol addresses and/or Media Access Control addresses.

IA-4 IDENTIFIER MANAGEMENT

Control Requirements for High and Moderate Systems (H, M)

- System administrators must follow established authorization processes when assigning a user, group, role, or device identifier.
- Unique user identifiers (i.e., NetIDs) must not be reused.
- Accounts must be disabled in accordance with timeframes and triggers defined in AC-2.

IA-5 AUTHENTICATOR MANAGEMENT

Control Requirements for High and Moderate Systems (H, M)

- Administrators of High and Moderate systems must take the following steps to manage system authenticators/passwords:
    - Verify the identity of the individual, group, role, service, or device receiving the authenticator.
    - Establish initial authenticator content for any authenticators being issued (e.g., generate an initial password or certificate). When a temporary password is issued to a user, the user must change the temporary password at first logon (where applicable).
    - Ensure that authenticators have sufficient strength for their intended use. At a minimum, password strength must comply with the ITS Password Complexity Standard.
    - Establish and follow procedures for distributing initial authenticators, responding to lost, compromised, or damaged authenticators, and revoking authenticators.
    - Change default authenticators prior to first use, and when installing information systems.
    - User passwords must be changed at least once every 180 days, and immediately if a compromise is suspected. Certificates must be changed prior to their expiration date.
    - Protect authenticator content from unauthorized disclosure and modification.
    - Employ the following controls to protect authenticators:
        - Passwords must be encrypted using industry standard strong encryption, both at rest and in transit.
        - Temporary passwords that are transmitted for the purpose of establishing a new password or changing an existing password may be exempted from the requirement to encrypt if it is a one-time transmission, and the user must change the password upon first logon.
        - Smart phones used to access university data must be protected with a password/PIN having at least four characters.
        - Prohibit passwords from being reused for at least 24 generations. Information systems must enforce this restriction when technically feasible.
        - Passwords used for device-to-device interactions may be randomly generated by a method approved by the ITSO, and are not required to expire.
    - Change authenticators for group or role accounts when membership to those accounts change.

- System administrators and system users must also comply with the following controls and practices for password-based authentication [IA-5(1)]:
    - Transmit passwords only over cryptographically-protected channels.
    - When possible, passwords must be stored as salted hashes rather than plain text. Hashes should employ current industry standard encryption algorithms.
    - Compromised, forgotten, or re-activated passwords must be replaced with new passwords, rather than being re-issued.
    - Allow user selection of long passwords and phrases, including all printable characters, where technically feasible.
    - Passwords that are selected by the user must be checked, using automated tools, to verify compliance with the ITS Password Complexity Standard when technically feasible.
    - Systems must be configured to enforce compliance with the ITS Password Complexity Standard, or with a higher standard of complexity if a unique requirement is established during system risk assessment and documented in the System Security Plan, or the operational procedures, or other supporting documents.
- When public key-based authentication is used, the corresponding private key must be restricted to authorized access, and the authenticated identity mapped to the account of the individual or group to which it applies. [IA-5(2)]
- When public key infrastructure (PKI) is used, certificates must be validated by a verified certification path to an accepted trust anchor. [IA-5(2)]
- Authenticators must be protected commensurate with the highest risk category of the systems and information to which they provide access. [IA-5(6)]

IA-6 AUTHENTICATION FEEDBACK

Control Requirements for High and Moderate Systems (H, M)

- Administrators of High and Moderate systems must configure the systems to obscure feedback of authentication information by masking passwords upon key entry. Mobile devices with small screens (e.g., 2-4 inches) may be exempted from this requirement due to decreased likelihood of unauthorized individuals viewing the information.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control Requirements for High and Moderate Systems (H, M)

- Administrators of High and Moderate systems must ensure that encryption mechanisms used on the systems comply with, at a minimum, federal standard FIPS 140-2.

IA-11 RE-AUTHENTICATION

Control Requirements for High and Moderate Systems (H, M)

- Users must re-authenticate when moving between privileged and non-privileged roles, and when authenticators or credentials are changed.

IA-12 IDENTITY PROOFING

Control Requirements for High and Moderate Systems (H, M)

- Faculty, students, and staff must provide a valid government photo ID verifying proof of identity before being assigned a George Mason information system user account. [IA-12(2)]
- Contractors and affiliates may be assigned a George Mason information system account at the request of their organizations.
- Privileged access and access to protected data must be authorized by the system or data owner. [IA-12(3)]

MAINTENANCE (MA)

MA-1 POLICY AND PROCEDURES

Policy Statement: 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.

Related Documentation:
University Policy 1114A Removal of University Data from Electronic Media

General Controls (H, M, L)

- One or more qualified system administrators must be designated to manage each information system. The system administrator may be a contractor or a university employee.
- University employees tasked with managing one or more information systems must have system administration duties incorporated into their Employee Work Profiles or Position Descriptions.
- Contractors who manage university information systems must have system administration duties defined in the governing contract documents.
- All university information systems must be effectively maintained, with security patches and updates applied in a timely manner.

Additional Control Requirements for High Systems (H)

- Maintenance of High category systems must be guided by one or more documents describing roles and responsibilities for performing maintenance activities on the system, and required timelines for applying system updates. This information may be incorporated into the System Security Plan, or the operational procedures, or other supporting documents.

MA-2 CONTROLLED MAINTENANCE
16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]
Control Requirements for High Systems (H)

- System administrators must maintain assigned equipment and applications in accordance with manufacturer specifications. Recommended updates and changes should be considered in the context of operational uptime requirements, level of risk, and compensating controls.
- Controls and configuration elements that could impact security must be checked for proper functioning after maintenance, repair, or replacement actions.
- All maintenance activities must be approved and recorded in accordance with ITS Change and Configuration Management policies and procedures.
- Removal of information systems equipment for offsite repairs or maintenance must be approved by the responsible technician/administrator's supervisor.
- **CUI Only**: Offsite repair of information systems that are, or have been, used in the CUI environment is not permitted.
- Information systems that stored or may have stored sensitive or restricted data must be wiped in accordance with University Policy 1114A Removal of University Data from Electronic Media before being sent offsite for repair, replacement, or disposal.

MA-3 MAINTENANCE TOOLS
Control Requirements for High Systems (H)

- System administrators identify and recommend for purchase maintenance tools based on perceived usefulness to the operating environment. Recommended equipment and applications are approved by the system administrator's supervisor prior to purchase.
- Maintenance and diagnostic tools that have reached the end of their useful life or have been rendered obsolete by changes in the technical environment should be retired and sent for disposal.
- Any indication or suspicion that a maintenance tool may have improper or unauthorized modifications must be investigated prior to use, or as soon as the potential discrepancy is observed. Suspected malicious activity must be reported to the ITSO for further investigation. [MA-3(1)]

- **CUI Only**: Media containing diagnostic and test programs must be checked for existence of malicious code before being used in the CUI environment. Presence of suspected malicious code must be referred to the ITSO for investigation. [MA-3(2)]

MA-4 NONLOCAL MAINTENANCE

Control Requirements for High Systems (H)

- Nonlocal maintenance and diagnostic activities are conducted by individuals (either George Mason system administrators or vendors) who connect to the information system via an external network. Allowed mechanisms and required procedures for nonlocal vendor maintenance on High category systems may be documented in the System Security Plan, or the operational procedures, or other supporting documents.
- Multifactor authentication is required for establishment of nonlocal maintenance and diagnostic sessions, and the sessions must be terminated once the activity is completed.
- Nonlocal maintenance and diagnostic sessions that are performed by vendors must be monitored and documented by the George Mason system administrator or system owner.

MA-5 MAINTENANCE PERSONNEL

Control Requirements for High Systems (H)

- George Mason personnel are authorized to perform hardware and/or software maintenance on assigned information systems in accordance with duties defined in their Employee Work Profile or Position Description as approved by their supervisor.
- Contractors and vendor personnel may be authorized for physical access to maintain assigned information systems. Such access must be approved by the information system owner or designee, and must be reauthorized at least annually.
- Contractors and vendor personnel who do not have standing authorization for physical access to information systems for diagnostic and maintenance purposes may be issued temporary access credentials by the system owner or designee. Such access is subject to monitoring and oversight by George Mason personnel as defined in applicable operational procedures and standards.

MEDIA PROTECTION (MP)

MP-1 POLICY AND PROCEDURES

Policy Statement: 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. Per University Policy 1114 Data Stewardship, Data Owners are responsible for ensuring that access and protection requirements consistent with university policies and the data classification are in place and responsive to business needs. Information system owners are responsible for implementing, documenting, and maintaining security controls and procedures that meet standards established by the ITSO. The ITSO reviews and updates security control standards as necessary to reflect changes in the technical environment and current and emerging threats.

Related Documentation:
University Policy 1114 Data Stewardship
University Policy 1114A Removal of University Data from Electronic Media

MP-2 MEDIA ACCESS

Control Requirements for High Systems (H)

- Access to Highly Sensitive Data, Controlled Unclassified Information, and other protected data as defined in University Policy 1114 Data Stewardship must be restricted only to authorized personnel, and incidentally

to Data Custodians in performance of their assigned tasks. Data Custodians are not authorized to disclose, disseminate or review protected data except as required during the performance of their assigned duties.
- Access controls are to be applied to both digital and non-digital media.

MP-3 MEDIA MARKING

Control Requirements for High Systems (H)

- Removable digital media containing Highly Sensitive Data must be labeled as such, unless the media remains within the Aquia Data Center.
- **CUI Only:** All data categorized as Controlled Unclassified Information must be labeled with required CUI markings in accordance with current federal policies and guidance. **IMPORTANT**: Federal Tax Information (FTI) is a category of CUI and is required to have a banner marking the information as CUI. A federal aid applicant's Institutional Student Information Record (ISIR) will include two (2) FTI label fields:
  - FTI Label Start at the beginning: 'CUI//SP-TAX'
  - FTI Label End near the end: 'CUI//SP-TAX'

  Departments and process owners must ensure that they receive ISIR data must retain the CUI labeling of FTI wherever the data is stored and used within the student information system(s).

MP-4 MEDIA STORAGE

Control Requirements for High and Moderate Systems (H, M)

- Digital and non-digital media containing protected data must be stored securely, with access restricted to authorized persons. Security controls should be commensurate with the data's sensitivity classification. Digital media includes flash drives, magnetic media, external hard drives, compact discs (CD), and digital versatile discs (DVD). Non-digital media includes paper and microfilm. The secure storage requirements remain in force until the media are destroyed or sanitized using approved procedures.
- Controlled areas having physical and procedural access controls may be used to meet secure storage requirements.

MP-5 MEDIA TRANSPORT

Control Requirements for High Systems (H)

- George Mason personnel must take measures to secure system media containing protected data during transport outside of controlled areas, commensurate with the level of risk and sensitivity. Highly Sensitive Data and/or CUI contained on digital media must be encrypted with methods and algorithms approved by the ITSO; locked containers are required to protect non-digital media.
- Data custodians must document activities associated with the transport of system media containing protected data, and maintain accountability for transport by restricting transport activities to authorized personnel and/or courier services. If system media containing Highly Sensitive Data is to be transported by an external courier or service, tracking records must be maintained to indicate when the system media was handed off.

MP-6 MEDIA SANITIZATION

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H, M, L)

- System media and electronic storage devices that contain, or may have contained, Highly Sensitive Data or CUI must be destroyed, or securely erased in accordance with University Policy 1114A Removal of University Data from Electronic Media when the media or device is removed from service or transferred to another university unit.
- Non-digital media containing Highly Sensitive Data targeted for disposal must have the sensitive information completely obscured or redacted, or be destroyed.
- **CUI Only:** Non-digital media containing CUI that is targeted for disposal must be destroyed.

MP-7 MEDIA USE

Control Requirements for High Systems (H)

- All removable digital media (as defined in MP-4) containing Highly Sensitive Data must be encrypted using methods and algorithms approved by the ITSO.
- All removable digital media containing Highly Sensitive Data must have a clearly designated owner, accountable for ensuring that all applicable security controls are met.
- **CUI Only:** The use of removable digital media for backup retention or restoration is not permitted.

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-1 POLICY AND PROCEDURES

Policy Statement: 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 in proportion to the criticality or importance of their function at the university. Responsibilities for ensuring physical security of information resources may be part of the job function for departmental staff including, but not limited to, information technology staff, data custodians, Facilities staff, and supervisors. The heads of George Mason units that are responsible for information assets categorized as High or Moderate must ensure that procedures to facilitate the implementation of the physical and environmental protection policy and associated controls are created, maintained, and reviewed annually and when required to address environmental changes. Departmental operations staff must be aware of, and are required to follow, these procedures.

- The Vice President for Information Technology is responsible for ensuring physical and environmental protection of the Aquia Data Center and all sites providing backup and/or Disaster Recovery services for the Aquia Data Center.
- Responsibility for ensuring physical and environmental protection of High and Moderate information assets that are located outside of the Aquia Data Center and its backup sites lies with the head of the department that owns the assets. Examples are departmental computer rooms and shared access telecommunications rooms that house information assets that have been categorized as High or Moderate.

Related Documentation:
ITS.EIS-STD004 Data Center Physical, Environmental, and Operational Controls Standard

Scope
The controls in this section apply to facilities that house information systems and resources that are categorized as either High or Moderate, as specified in each control description.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control Requirements for High Systems (H)

- The unit head or designee must develop, approve, and maintain a list of individuals that are authorized to have physical access to information resource facilities under their control, and must ensure that:
    - Individuals are issued authorization credentials for facility access.
    - The access list is reviewed at least once every six months, and when needed to address environmental changes.
    - Individuals are promptly removed from the facility access list when access is no longer required.
    - Physical access rights are disabled upon suspension of personnel for more than one day for disciplinary purposes.
    - Physical access rights are temporarily suspended when personnel do not need access for more than 30 days because they are not working due to leave, disability, or other authorized purpose.

PE-3 PHYSICAL ACCESS CONTROL

Control Requirements for High Systems (H)

- The unit head or designee must ensure that:

- Physical access authorizations are enforced by verifying individual access authorizations before granting access to the facility.
- Access to the facility is controlled in accordance with documented procedures.
- Physical access audit logs are protected and maintained for at least two years.
- Visitors (i.e., persons who have not been granted access authorization) to restricted areas of the facility are escorted and monitored.
- Keys, combinations, swipe cards and other physical access devices are inventoried and secured. Keys must be changed when compromised, and combinations must be changed when compromised and when individuals possessing the combination are terminated, or transferred and are no longer authorized to have access.
- High category information systems and assets that are housed in areas that cannot be completely secured from unauthorized access are protected with locked cabinets and monitored with cameras or other protections approved by the ITSO.
- Visitor access to the Aquia Data Center is monitored and secured via an access control vestibule. [PE-3(8)]

PE-4 ACCESS CONTROL FOR TRANSMISSION

Control Requirements for High Systems (H)

- Publicly accessible network jacks and wireless networks must not permit direct access to network segments that connect to High category servers and systems.
- Physical access to network equipment that supports network segments connecting High category servers and systems must be restricted to authorized personnel.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control Requirements for High Systems (H)

- Information system output devices that regularly output Highly Sensitive Data must be secured to prevent unauthorized individuals from obtaining the output.
  - Examples of information system output devices include printers, facsimile machines, computer monitors, and audio devices.

PE-6 MONITORING PHYSICAL ACCESS

Control Requirements for High Systems (H)

- The manager of a facility that houses information assets categorized as High category must ensure that:
  - Physical access to the facility is monitored to detect and respond to actual and suspected physical security incidents.
  - Physical access logs are reviewed in accordance with documented standards and/or operating procedures.
  - Results of reviews and investigations are managed and coordinated in accordance with the appropriate authorities per the university's incident response procedures.
  - Physical access to the Aquia Data Center and the Disaster Recover (DR) Site is monitored via real-time and recorded video surveillance. [PE-6(1), PE-6(3)]

PE-8 VISITOR ACCESS RECORDS

Control Requirements for High Systems (H)

- The manager of a facility that houses information assets categorized as High category must ensure that:
  - Visitor access logs for secured areas are maintained and secured, and retained for at least two years.
  - Visitor access logs are reviewed at least once every 60 days, and any suspicious activity is investigated.

PE-9 POWER EQUIPMENT AND CABLING

Control Requirements for High Systems (H)

- The manager of a facility that houses information assets categorized as High category must ensure that power equipment including uninterruptible power supplies, generators, and power distribution units, and associated cabling are protected from damage and destruction.
- The Aquia Data Center and the DR Site must employ automatic controls to regulate and condition power supplied to High category assets. [PE-9(2)]

PE-10 EMERGENCY SHUTOFF

Control Requirements for High Systems (H)

- Data centers and computer rooms housing information assets categorized as High category must have emergency power shutoff switches located near the main entrance to the room, protected from unauthorized or accidental activation but readily accessible to authorized personnel. The shutoff devices must be capable of removing all electrical power from the information assets located in the room.

PE-11 EMERGENCY POWER

Control Requirements for High Systems (H)

- Data centers and computer rooms housing High category information assets must have an uninterruptible power supply to facilitate transition of the information systems to generator power, or to facilitate orderly shutdown in the event of a primary power source loss.
- The Aquia Data Center and its Disaster Recovery backup sites, and their supporting network equipment, must have alternate power supplies that are activated automatically and can maintain minimally required operational capability in the event of an extended loss of the primary power source. [PE-11(2)]

PE-12 EMERGENCY LIGHTING

Control Requirements for High and Moderate Systems (H, M)

- Data centers and computer rooms housing High and/or Moderate systems must have emergency lighting that activates automatically in the event of a primary power outage or disruption, and covers emergency exits and evacuation routes within the facility.

PE-13 FIRE PROTECTION

Control Requirements for High Systems (H)

- Data centers and computer rooms housing High category information assets must have fire detection and suppression systems that are supported by an independent energy source.
- Fire detection and suppression systems for data centers and computer rooms housing High category information assets must activate automatically and must automatically alert first responders and university Facilities personnel. [PE-13(1), PE-13(2)]

PE-14 ENVIRONMENTAL CONTROLS

Control Requirements for High Systems (H)

- Data centers and computer rooms housing High category information assets must employ environmental controls that can maintain temperature and humidity at recommended levels defined by American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) guidelines. If automated monitoring and alerting is not in place, environmental parameters must be checked at least daily to ensure they remain within the specified parameters.
- Temperature and humidity levels in the Aquia Data Center and the DR Site must be monitored and automatically adjusted to maintain the specified conditions and must alert operations personnel that are responsible for responding when environmental conditions go outside of the specification limits. [PE-14(1), PE-14(2)]

PE-15 WATER DAMAGE PROTECTION

Control Requirements for High Systems (H)

- Data centers and computer rooms housing High information assets must be protected from water leakage or accidental discharge by master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
- The Aquia Data Center and the DR Site must incorporate sensors, alarms, and automated notification systems to alert operations personnel that are responsible for responding to water leaks. [PE-15(1)]

PE-16 DELIVERY AND REMOVAL

Control Requirements for High Systems (H)

- All equipment deliveries to the Aquia Data Center must be coordinated with the Data Center Operations staff to ensure proper receipt, storage, and documentation. Each group/unit that arranges for equipment to be delivered is responsible for notifying Operations staff and confirming acceptance of the equipment.
- Equipment owners are responsible for the decommissioning of their equipment in the Aquia Data Center. All removal of decommissioned equipment must be coordinated with Data Center Operations staff for proper documentation of data center assets, and for security purposes. Equipment removal activity is tracked via the ITS Service Management ticketing system.
- **CUI Only**: Owners of High category systems that store or process CUI, and are located outside of the Aquia Data Center, must maintain protections and operating procedures that support this control.

PE-17 ALTERNATE WORK SITE

Control Requirements for High and Moderate Systems (H, M)

- University employees and contractors are permitted to access High and Moderate systems from home and other remote locations, in accordance with guidelines and approval from the university's Human Resources division. All George Mason policies and security standards must be followed when working remotely.
    - Highly Sensitive Data must not be stored on portable storage or computing devices without explicit approval from the ITSO.
    - **CUI Only**: CUI security banners must be presented prior to user and administrator logons to CUI systems, and CUI data must be handled only in accordance with the Technology Control Plan for each project.

PLANNING (PL)

PL-1 POLICY AND PROCEDURES

16 CFR 314.3 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Policy Statement: The ITSO must develop and document a security program policy for the university that overarches the information technology security standards, roles, responsibilities, and projects that affect the university's security posture. Supporting plans should be developed in coordination with the university's Office of Audit, Risk, and Compliance and must be approved by the Vice President for Information Technology. The policy must be published and updated as per documented frequency or more frequently if required to address an environmental change. Implementation of the security policy may require changes or additions to existing operating procedures; those changes, and the units or groups responsible for creating or updating the procedures, must be notified.

Related Documentation:

University Policy 1301 Responsible Use of Computing

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

Control Requirements for Sensitive IT Systems

Control Requirements for High Systems (H) that are NOT designated Sensitive IT Systems – **encouraged but not required**

- System owners are responsible for ensuring that a System Security Plan is developed for each Sensitive IT System. These may be created using the Integrated Risk Management (IRM) tool workflow or separately on a word document. The System Security Plan must:

- Be consistent with the university's enterprise architecture;
- Explicitly define the system's constituent components and authorization boundary;
- Describe the operational context of the system in terms of mission and business processes;
- Identify roles and responsibilities associated with maintaining and operating the system;
- Identify the information types processed, stored, and transmitted by the system;
- Provide supporting rational for the security categorization of the information system;
- Describe any specific threats to the system that are a concern to the university;
- Describe the operational environment for the information system, and relationships with or connections to other information systems;
- Provide an overview of the security requirements for the system;
- Identify any relevant control baselines or overlays, if applicable;
- Describe the security controls in place or planned for meeting those requirements, including rationale for tailoring and supplementation decisions;
- Include any security-related activities affecting the system that require planning and coordination with other units or groups; and
- Be reviewed and approved by the authorizing official or designee prior to plan implementation. The authorizing official must be a senior executive having authority to assume formal responsibility for operating the information system at an acceptable level of risk to the university. Examples are the Vice President for Information Technology (for ITS-owned systems), and Deans/Directors of university units for departmental-owned systems.

- Copies of the System Security Plan, and subsequent changes, must be distributed to or authorized individuals be granted access to the record, as appropriate.
- The System Security Plan must be reviewed on an annual basis, or more frequently if required to address environmental changes.
- The System Security Plan must be updated when required to address changes to the information system or environment, or to address problems identified during implementation or security control assessments.
- The System Security Plan must be protected from unauthorized disclosure and modification.

PL-4 RULES OF BEHAVIOR

General Controls (H, M, L)

- All persons who use information systems that are under the control of George Mason are required to comply with University Policy 1301 Responsible Use of Computing.
- George Mason employees and students are required to acknowledge that they agree to abide by University Policy 1301 each time they log into the Banner system.
- All employee position descriptions and performance plans must include a statement acknowledging the employee's responsibility to comply with all applicable university policies.
- UserID and password combinations that are used to access George Mason information systems (e.g., PatriotPass) must not be used to create accounts on external (non-university) sites and applications. [PL-4(1)]

PL-8 SECURITY AND PRIVACY ARCHITECTURES

Control Requirements for Sensitive IT Systems

Control Requirements for High Systems (H) that are NOT designated Sensitive IT Systems – **encouraged but not required**

- The System Security Plan for each Sensitive IT System category system must include a description of the security architecture explaining the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of sensitive information, and any dependencies on external systems or services.
- The security architecture description must be reviewed, and updated as necessary, each time the System Security Plan is reviewed.

PL-10 BASELINE SELECTION

General Controls (H, M, L)

- System owners and designees that are developing a new system for deployment must employ all controls in the "George Mason University Information Technology Security Standard" that are applicable to the security categorization of the system. Requests for exceptions must be submitted to the ITSO for consideration.

PL-11 BASELINE TAILORING

Control Requirements for High Systems (H)

- Any and all tailoring or exceptions to the baseline controls included in the "George Mason University Information Technology Security Standard" must be approved by the ITSO.

PERSONNEL SECURITY (PS)

PS-1 POLICY AND PROCEDURES

Policy Statement: The university must develop documented procedures to facilitate the implementation of the controls in this family, and disseminate them to individuals and roles that are responsible for implementing them. The Vice President for Information Technology, jointly with the Vice President and Chief Human Resource Officer, establishes control requirements for personnel security that are consistent with applicable state and federal laws, regulations, standards, and guidelines. Personnel policies and procedures must be reviewed annually and updated when required.

Related Documentation:

University Policy 1141 Export Controls and Sanctions Compliance
University Policy 1305 Electronic Security Incidents
University Policy 1316 Controlled Unclassified Information
University Policy 2221 Background Investigations
University Policy 2224 Recruitment and Hiring of University Employees

PS-2 POSITION RISK DESIGNATION

General Controls (H, M, L)

- The university must identify and classify personnel positions based on risk category in order to determine the level of risk associated with the position and the appropriate controls that are required to be implemented. Currently all employee positions are considered to be security-sensitive and subject to background investigations. Position risk designations must be reviewed annually and updated when required to address changes in the environment.
- All new and rehired university employees, and employees that are transferred or promoted into new positions, are required to undergo and pass a criminal background check in accordance with University Policy 2221 Background Investigations.
- Certain positions may require additional screening based on state and/or federal laws and regulations. The information system owner or manager, in conjunction with George Mason's Human Resources office, determines whether additional personnel screening criteria are required based on the position's duties and applicable law.

PS-3 PERSONNEL SCREENING

Control Requirements for High Systems (H)

- University employees in positions that require privileged access to High category systems must have passed all background check requirements prior to being granted privileged access.
- CUI and university research and information systems involving military or dual-use items, software, or technology controlled under the International Traffic in Arms Regulations ("ITAR") or the Export Administration Regulations ("EAR") have additional citizenship, screening, and licensing requirements per

University Policy 1141 Export Controls and Sanctions Compliance. These additional personnel screening requirements are determined by the Office of Research Integrity and Assurance. [PS-3(4)]

PS-4 PERSONNEL TERMINATION

General Controls (H, M, L)

- Information system owners and unit managers, in coordination with Human Resources, must disable a terminated employee's privileged access to George Mason-controlled information resources in accordance with the parameters prescribed in AC-2.
    - Terminated employees may retain non-privileged access to Banner, as needed to access payroll and tax statements and other records concerning their employment history.
- The terminated employee's manager is responsible for ensuring that:
    - Privileged access, and all credentials on systems for which the employee is no longer authorized, are promptly revoked;
    - All George Mason property has been returned;
    - All security-related items such as keys, access cards, and hardware authentication devices have been returned or disabled; and
    - Any privileged access to George Mason-controlled information systems and resources formerly controlled by the terminated employee has been transitioned as required.

PS-5 PERSONNEL TRANSFER

General Controls (H, M, L)

- Information system owners and unit managers have the responsibility to review and confirm ongoing needs for current logical and physical access authorizations to information resources when individuals are reassigned or transferred to other positions within the university. Access authorizations must be modified as appropriate to facilitate ongoing operations while complying with the principle of Least Privilege (control AC-6).
    - Access authorizations that are not required for the transferred employee's new role, but are being temporarily maintained to facilitate operations during a transition period, must be reviewed monthly by the transferred employee's former manager and revoked when they are no longer deemed to be necessary.

PS-6 ACCESS AGREEMENTS

General Controls (H, M, L)

- Position descriptions for classified and administrative faculty employees include Confidentiality and Compliance statements acknowledging the employee's responsibility to comply with all university policies and procedures, and state and federal laws when accessing George Mason systems and data. The employees sign these documents when entering a new position, and when substantive changes are made to their existing position.

PS-7 EXTERNAL PERSONNEL SECURITY

Control Requirements for High Systems (H)

- Contract employees working for George Mason who will be responsible for handling Highly Sensitive Data and/or managing High category systems must be bound by contractual agreements which include requirements to comply with university policies and procedures.

PS-8 PERSONNEL SANCTIONS

General Controls (H, M, L)

- George Mason employees who fail to comply with established information security policies and procedures are subject to disciplinary action in accordance with the university's Human Resources policies and procedures.

- Minor offenses may be addressed by the employee's supervisor, with feedback and coaching. This may include documentation such as a counseling memo and/or formal notice of substandard performance, with follow-up to verify that the issue is not continuing to occur.
- Repeated minor offenses, or more serious breaches including unauthorized access of sensitive systems, warrant formal disciplinary action including a Due Process Notification. The employee's supervisor must contact Human Resources within one week of discovery of the offense, to discuss the appropriate actions.
- Serious offenses such as unauthorized release of Highly Sensitive Data or intentional compromise of university information systems must be reported and managed in accordance with University Policy 1305 Electronic Security Incidents. This may result in formal disciplinary actions, up to and including termination and legal action.

PS-9 POSITION DESCRIPTIONS

General Controls (H, M, L)

- Position descriptions for employees who will be responsible for managing information resources must include specific details of the security responsibilities associated with the role and must outline training requirements and expectations.

RISK ASSESSMENT (RA)

RA-1 POLICY AND PROCEDURES

Policy Statement: The ITSO, under authority of the Vice President for Information Technology, is responsible for developing, documenting, and disseminating to information resource owners a set of required Risk Assessment controls and procedures. These controls and procedures outline the steps that must be taken in order to properly categorize the level of risk associated with George Mason-controlled information systems. Each Risk Assessment shall be reviewed and updated as necessary to address environmental changes. The IT Risk and Compliance is responsible for reviewing and updating the Risk Assessment Procedures annually, and when necessary to address environmental changes.

Related Documentation:
ITS.ITRC-PROC004 IT Risk Assessment Procedure

RA-2 SECURITY CATEGORIZATION

General Controls (H, M, L)

- The IT Risk and Compliance is responsible for categorizing George Mason-controlled systems as determined during initial review and periodic risk assessments, to aid the system owner's awareness of the assigned categorization or risk level, and maintaining a list of all High and Moderate systems and components.
- The CISO or equivalent staff leading the information security function is the authorizing official responsible for reviewing and approving the security categorization decision.

RA-3 RISK ASESSMENT

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

General Controls (H)

- The IT Risk and Compliance office is responsible for ensuring that a risk assessment is performed on George Mason-controlled systems. Newly instantiated systems shall undergo a categorization and assessment before they are permitted to attach to a production network. Thereafter, the risk assessment for each system must be performed in accordance with IT Risk Assessment Procedure, and shall be reviewed annually and when necessary to address environmental changes. The information security program shall be based on risk assessment that identifies and evaluates internal and external risks to customer information and assesses the sufficiency of safeguards in place [PM-9].

- The IT Risk and Compliance office shall disseminate the results of the risk assessment to the system owner and system administrator(s) for awareness.

Additional Control Requirements for High Systems (H)

- Each George Mason-owned system that has been categorized as a Sensitive IT System must have a System Security Plan which includes a summary of the system's assessment results, documenting the major threats to the system and risks to the university and/or individuals if compromised. The system owner or is responsible for ensuring that a System Security Plan has been created and that and/or the risk assessment contains this threat and risk detail. Other High category systems that are not Sensitive IT Systems, may also maintain System Security Plans which includes this information, however at this time it is not mandatory for them.

RA-5 VULNERABILITY MONITORING AND SCANNING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High and Moderate Systems (H, M)

- The ITSO is responsible for performing vulnerability scans of all High and Moderate systems on a weekly basis, and when necessary to address new high impact threats. The vulnerability scanning tools must be capable of enumerating platforms, software flaws, and improper configurations and must include the capability to readily update the vulnerabilities to be scanned.
- The vulnerability scanning tools must be kept up to date with current threat and vulnerability signatures. [RA-5(2)]
- The vulnerability scanning tools must automatically update the ITS Governance, Risk, and Compliance (GRC)/ Integrated Risk Management (IRM) system with scan results for each system.
- System owners and system administrators must permit ITSO to perform vulnerability scans using privileged access credentials when ITSO determines such scans are warranted based on risk and impact. Privileged access scans are typically required for High category systems. [RA-5(5)].
- **CUI Only**: Vulnerability scans on systems that store or process CUI must use privileged access credentials.
- When a system fails a vulnerability scan, the responsible system administrator is automatically notified. The system administrator must confirm the existence of the vulnerability and implement remediations within the timeframes prescribed in ITS.ITSO-PRS002 Vulnerability Scanning and Remediation Process.
- The ITSO is responsible for assessing the impact of discovered vulnerabilities, taking into account impact on Confidentiality, Integrity, and Availability and the associated Common Vulnerability Scoring System (CVSS) score.
- The ITSO is responsible for verifying that vulnerabilities identified in the scans have been effectively treated by the system administrator, and sharing vulnerability information obtained from the scans with the George Mason system administration community.
- The ITSO must maintain a public channel to receive reports of vulnerabilities in university information systems, and advertise its availability to the George Mason community. [RA-5(11)].

RA-7 RISK RESPONSE

General Controls (H, M, L)

- The Director, IT Risk and Compliance in consultation with domain experts determines and/or approves remedial actions required to address findings from security assessments, monitoring, and audits. System owners are responsible for creating plans of action and milestones to implement the prescribed remedial actions.
- In cases where the Director, IT Risk and Compliance and the system owner fail to agree on remedial actions and timeframes, or the specified actions would entail significant cost and/or impact on university operations, the Vice President for Information Technology determines the course of action based on the university's risk tolerance. Risk response actions may include avoiding the risk, accepting the risk, transferring the risk, or remediating the risk by employing compensating controls, proceeding with the prescribed mitigation, or developing a plan of action and milestones to implement the mitigation at a future date.

RA-9 CRITICALITY ANALYSIS

Control Requirements for High Systems (H)

- When High category systems are being developed, modified, or acquired, any components that are determined to be particularly critical shall be identified by the engineering team and specified as a critical component. This information may be specified in the System Security Plan, or the operational procedures, or other supporting documents.
- Additional protective measures such as redundancy and increased monitoring should be considered for critical components

SYSTEM AND SERVICES ACQUISITION (SA)

SA-1 POLICY AND PROCEDURES

Policy Statement: The university's Purchasing Office, under authority of the Vice President for Finance, has primary responsibility for establishing policy and procedures concerning the procurement of goods and services. The Vice President for Information Technology is responsible for establishing policy and procedures concerning the acquisition of systems, software, and services that could impact the security of the university's information resources. All related policies and procedures must be reviewed at least once every three years, updated as necessary, and disseminated to all university units

Related Documentation:
University Policy 1307 Procurement and/or Development of Administrative Systems/Applications
University Policy 2106 Purchase of Goods and Services

SA-2 ALLOCATION OF RESOURCES

Control Requirements for High Systems (H)

- Per University Policy 1307 Procurement and/or Development of Administrative Systems/Applications, all software applications and information services that will use George Mason data or integrate with George Mason's administrative systems must undergo review by the Architectural Standards Review Board (ASRB) prior to purchase. One purpose of this review is to establish information security requirements that must be included in the contract documentation before the acquisition is approved. Approval may be withheld, or made contingent upon additional investment if necessary to meet information security requirements.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- All George Mason-controlled information systems must be designed, developed, configured, and operated within a security framework that ensures confidentiality, integrity, and availability throughout the system's life cycle.
- Information security roles and responsibilities must be defined and documented throughout the system life cycle.
- Individuals having information security roles and responsibilities must be identified.
- Applied security controls shall be based on the highest risk category of the data that will be stored, transmitted, or processed by the system.
- The system to be acquired must effectively integrate with George Mason's information security architecture. This is determined during the initial ASRB review, and must be revalidated with security reviews when the system is modified or updated.
- Systems owned by the George Mason that are categorized as Sensitive IT Systems must have a System Security Plan that details information security controls that are implemented and enforced.

SA-4 ACQUISITION PROCESS

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- External information systems and services to be acquired must effectively integrate with George Mason's information security architecture. This is determined during the initial ASRB review, and must be revalidated with security reviews when the system is modified or updated.
- Suppliers of external information systems and services must provide documentation describing the functional properties of security controls and mechanisms visible at the interfaces to George Mason systems, implementation and configuration information for security-relevant system interfaces, and the ports, protocols, and functions that are required to interface with George Mason systems and users. [SA-4(1), SA-4(2), SA-4(9)]
- Contracts for external information systems and services that are categorized as High must include a Data Security Addendum detailing information security requirements and responsibilities.
- Suppliers of external information systems and services that are categorized as High must provide security assessment reports in accordance with ITS.ITRC-PRS003 Third-Party Risk Management Process. The IT Risk and Compliance office shall track and review the assessment reports, and escalate exceptions and issues to the ITSO for determination of next steps.
- Information technology products to be used for personal identity verification and multi-factor authentication must be on the FIPS-201 approved products list. [SA-4(10)]

SA-5 SYSTEM DOCUMENTATION

Control Requirements for High Systems (H)

- For all High category systems, the information resource owner or designee is responsible for:
    - Obtaining administrator documentation for the system, component, or service that describes:
        - Secure configuration, installation, and operation;
        - Effective use and maintenance of security functions and mechanisms; and
        - Known vulnerabilities regarding configuration and use of administrative or privileged functions.
    - Obtaining user documentation for the system, component, or service that describes:
        - User-accessible security functions and mechanisms and how to effectively use them;
        - Methods for user interaction, which enables individuals to use the system, component, or service in a secure manner; and
        - User responsibilities in maintaining the security of the system, component, or service.
    - Documenting attempts to obtain system, component, or service documentation when such documentation is unavailable or nonexistent; and
    - Distributing documentation to appropriate information resource custodians and users.

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- When High category systems are being developed, modified, or acquired, the system owner is responsible for ensuring that basic information security principles are followed. Examples include but are not limited to:
    - Developing layered protections;
    - Establishing sound security architecture and controls in the design;
    - Incorporating security requirements and guidance from ITSO into the system development life cycle;
    - Ensuring that developers have appropriate training in how to build secure software; and
    - Reducing risk to acceptable levels.
- For legacy systems, security engineering principles shall be applied to upgrades and modifications where feasible. Complementary controls may be added to reduce risk in cases where the existing hardware and software limits the implementation of good security practices.

SA-9 EXTERNAL SYSTEM SERVICES

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- Suppliers of external information systems and services that are categorized as High must comply with the provisions in SA-4 Acquisition Process.
- The head of the university unit that initiated the purchase of the system or service is considered to be the system owner. The system owner or designee is responsible for defining and documenting oversight and user roles and responsibilities, and for abiding by any requirements or restrictions mandated by the ASRB.
- The ITS Risk and Compliance office is responsible for monitoring security control compliance on an ongoing basis in accordance with ITS.ITRC-PRS003 Third-Party Risk Management Process.
- Suppliers of external information systems and services that are categorized as High and will interface with George Mason systems must identify the functions, ports, and protocols that are required for the use of the system or service. [SA-9(2)]

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control Requirements for High Systems (H)

- Developers of applications that directly interface with the university's Enterprise Resource Planning Banner Core system must follow a documented design process that:
  - Explicitly addresses security requirements;
  - Identifies the standards and tools used in the development process;
  - Documents tool options and configurations to be used in the development process; and
  - Documents, manages, and ensures the integrity of changes to the process and tools used in development.
- The head of the unit that is responsible for the application development is responsible for ensuring that the design process, standards, and tools are reviewed at least every three years, and when required to address changes to the environment. The process, standards, and tools must be updated when required in order to comply with the university's information security standards and requirements.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control Requirements for High Systems (H)

- The system owner of a High category system must ensure that components that are no longer being supported by the developer, vendor, or manufacturer are replaced in a timely manner; if replacement must be delayed, an alternative source for support must be provided.
- If in-house support is the only viable alternative, the system owner must review the effectiveness of the support processes at least annually. If deficiencies in security and/or system availability are noted, the component's replacement must be expedited.

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

SC-1 POLICY AND PROCEDURES

Policy Statement: The Vice President for Information Technology is responsible for establishing control requirements that address Systems and Communications Protection of George Mason's information resources. Security standards and controls are published by the IT Security Office; information system owners must ensure that appropriate procedures to implement those controls are developed, disseminated to system administrators and system users, and maintained through regular updates. All related policies and procedures must be reviewed per designated cadence, and when necessary to address environmental changes.

Installation of new communications cabling in university-occupied spaces must be performed to current George Mason and industry standards, and must meet all federal, state, and local regulations including fire codes. ITS Facilities and Infrastructure Engineering must be consulted in advance of any installation of new communications

cabling, in new or existing telecommunications pathways. Communications cabling installed on behalf of, and strictly for use by, outside organizations or business partners occupying George Mason facilities may not be required to meet all George Mason standards for materials or installation techniques. However, ITS Facilities and Infrastructure Engineering must review and approve all installations. If a proposed installation would have a negative impact on the availability, maintainability, safety, or security of George Mason facilities it may be disallowed until the deficiencies in the plan are corrected.

Related Documentation:
ITS.EIS-POL001 Firewall Management Security Policy

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Control Requirements for High Systems (H)

- For High category systems, regular user functions must be separated from system management functions that require privileged user access. This may be accomplished by using different computers, operating system instances, network addresses, virtualization, or some combination of these methods.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

Control Requirements for High Systems (H)

- For High category systems, information produced by the actions of prior users or roles (including the actions of processes acting on their behalf) and contained in shared system resources must not be available to current users or roles, or processes acting on their behalf.

SC-5 DENIAL-OF-SERVICE PROTECTION

Control Requirements for High Systems (H)

- ITS must employ technologies and controls designed to limit the impact of denial-of-service attacks against the university's High category systems. Controls may include a combination of: packet filters at network boundaries, increased network and server capacity and redundancy, traffic blackholing arrangements with service providers, and anti-malware protection on endpoints. Automated monitors and alerts must be configured to ensure that denial-of-service attacks are detected, and system administrators are notified.

SC-7 BOUNDARY PROTECTION

General Controls (H, M, L)

- System owners must monitor and control communications at the external boundaries, and key internal boundaries, of information resources. Information system architectures must employ network segmentation to separate publicly accessible system components from internal networks.
- Connections to external networks and systems are permitted only through managed interfaces consisting of boundary protection devices arranged in accordance with George Mason's security architecture and standards. Such connections may be instantiated only after review and approval of ITS, under authority of the Vice President for Information Technology. [SC-7(3)]
- ITS is responsible for establishing traffic flow policies for interfaces to external networks, and protecting the confidentiality and integrity of the information being exchanged at each interface in accordance with ITS.EIS-STD005 Firewall Ruleset Engineering Standard, and ITS.EIS-STD003 Firewall Exception Standard.[SC-7(4)]
- Remote connections to George Mason's network must be instantiated only in accordance with the Remote Access Device Standard. Split tunneling is not permitted and must be restricted by configuration, with the exception of private local networks which may be allowed to facilitate a remote worker's access to local system resources. [SC-7(7)]

Additional Control Requirements for High Systems (H)

- Connections to High category systems must be instantiated and managed by ITS; network communications traffic policy must deny all by default, and allow only authorized traffic by exception. [SC-7(5)]

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- Information transmitted to and from High category systems and components must be protected from unauthorized access and disruption. Physical access to High category systems and components must be controlled.
- All Highly Sensitive Data that is transmitted over a public network must be encrypted with industry-standard strong encryption using at least 128-bit keys. [SC-8(1)]

SC-10 NETWORK DISCONNECT

Control Requirements for High Systems (H)

- Network connections associated with a communications session to a High category system must be terminated at the end of the session, or after a defined period of inactivity as defined in related standard, procedure, or process document.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control Requirements for High Systems (H)

- Digital certificates for all High category systems and components must be acquired, installed, and maintained in accordance with ITS.EA-PRS005 Digital Certificate Service Process.
- System owners are responsible for ensuring that system administrators follow established procedures for obtaining, renewing, and revoking digital certificates and for securely storing and managing cryptographic keys.

SC-13 CRYPTOGRAPHIC PROTECTION

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Control Requirements for High Systems (H)

- Highly Sensitive Data must be protected with encryption, while at rest and in transit. The encryption method must be approved by the IT Security Office, and must use an algorithm with a minimum cipher key size of 128 bits.
- High category systems and components may require encryption, based on documented risk management decisions. The encryption method must be approved by the IT Security Office, and must use an algorithm with a minimum cipher key size of 128 bits.
- Encryption keys must be securely generated, stored, and archived in accordance with documented procedures. A copy of each key, when instantiated or changed, must be securely delivered to the IT Security Office for escrow.
- **CUI Only**: CUI including Federal Tax Information (FTI) data must be protected, while at rest and in transit, using FIPS validated cryptography.
- **GLBA In-Scope:** If encryption of customer information, either in transit over external networks or at rest, is infeasible, then to secure such customer information alternative effective compensating controls may be applied and be acceptable with review and approval by George Mason's Qualified Individual.

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

General Controls (H, M, L)

- Collaborative computing devices such as cameras, microphones, videoconferencing equipment and networked white boards installed in sensitive work areas must have remote activation methods disabled, and administrative access limited to authorized IT personnel.
- Collaborative computing devices installed in common areas including university classrooms and conference rooms may permit remote activation, but must provide an explicit indication of use to physically present users.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control Requirements for High and Moderate Systems (H, M)

- All public key certificates used by or with George Mason-controlled systems categorized as Moderate or High must be issued by an authorized certificate authority (CA). Self-signed or automated self-generated certificates are not authorized for use. Exception: Test and development systems may use self-signed or vendor self-generated certificates during initial configuration, but must be transitioned to a certificate issued by an authorized CA prior to operational use.
- ITS, under direction of the Vice President for Information Technology, is responsible for defining authorized certificate authorities and issuing certificates for use with George Mason-controlled information systems. Authorized CA's may include a private root CA to be used only for internal authentication and communications between internal systems. The private root CA is not authorized for use with public-facing systems.

SC-18 MOBILE CODE

Control Requirements for High Systems (H)

- Acceptable mobile code technologies for High category systems, components, and applications may be defined in the in the System Security Plan, or the operational procedures, or other supporting documents.
- Mobile code includes any program, application, or content that can be transmitted across a network and executed on a remote system. Examples of mobile code technologies include Java applets, JavaScript, HTML5, WebGL, ActiveX, PDF, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers, and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones.
- The use of mobile code must be authorized by the ASRB, in cooperation with the relevant developer team and/or system owner.
- **CUI Only**: The use of mobile code in a CUI environment is prohibited.
- Firewalls and endpoint management software associated with the system must monitor the use of mobile code through the use of current malware and vulnerability signatures, and protect against malicious code by blocking its execution and alerting administrators.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

General Controls (H, M, L)

- ITS must ensure that the systems that collectively provide name and address resolution service for George Mason are fault-tolerant, and implement internal and external role separation. The primary and secondary authoritative domain name servers must be geographically separated.

SC-23 SESSION AUTHENTICITY

Control Requirements for High and Moderate Systems (H, M)

- System owners or designees must ensure that the authenticity of communication sessions is protected. Controls may include requiring that users and/or endpoints are properly authenticated prior to establishing a communications session, and employing Transport Layer Security (TLS) 1.2 or above, to protect against "man-in-the-middle" attacks and verify authenticity of endpoints.

SC-28 PROTECTION OF INFORMATION AT REST

Control Requirements for High Systems (H)

- For High category systems and components, the system owner must ensure that all sensitive data is protected via approved encryption methods or other security mechanisms and should document the information in the System Security Plan, or the operational procedures, or other supporting documents.
- Highly Sensitive Data must be encrypted at rest, in accordance with University Policy 1114, Data Stewardship. [SC-28(1)]

- **CUI Only:** CUI data must be protected at rest, in accordance with the relevant Technology Control Plan. [SC-28(1)]

SC-39 PROCESS ISOLATION

Control Requirements for High and Moderate Systems (H, M)

- High and Moderate systems must use operating system software that maintains a separate execution domain for each executing system process. This may be accomplished by implementing separate address spaces and/or using sandboxing and virtualization to logically separate software and firmware from other software, firmware, and data.

SC-45 SYSTEM TIME SYNCHRONIZATION

Control Requirements for High and Moderate Systems (H, M)

- Systems must be configured to synchronize their internal clocks with one or more ITS-approved Network Time Protocol (NTP) servers.

SYSTEM AND INFORMATION INTEGRITY (SI)

SI-1 POLICY AND PROCEDURES

Policy Statement: The Vice President for Information Technology is responsible for establishing control requirements that address System and Information Integrity of the university's information resources. The IT Security Office, in coordination with system owners, is responsible for developing and disseminating to all George Mason units a set of standards and controls to implement the policy. System owners must ensure that operating procedures supporting the standards and controls are developed and followed. All related policies and procedures must be reviewed annually, and when necessary to address environmental changes.

Related Documentation:
ITS.ESD-POL001 ITS Change and Configuration Management Policy

SI-2 FLAW REMEDIATION

Control Requirements for High and Moderate Systems (H, M)

- System owners, with the assistance and oversight of the IT Security Office, are responsible for identifying, reporting, and correcting security flaws in systems and components under their control as described in **RA-5 Vulnerability Monitoring and Scanning**.
- System administrators must test and install software and firmware updates related to security flaw remediation within appropriate risk-based timelines as prescribed in **CM-3 Configuration Change Control** and ITS.ITSO-PRS002 Vulnerability Scanning and Remediation Process.
    - Security patches categorized by the vendor as "critical" or "high" must be applied within 10 business days, unless an alternate strategy is approved by the IT Security Office.
    - Security patches categorized by the vendor as "moderate" or "low" must be applied within 25 business days, unless an alternate strategy is approved by the IT Security Office.
- All High and Moderate systems must employ automated methods and software to check the current state of operating system patch levels at least weekly. [SI-2(2)]

SI-3 MALICIOUS CODE PROTECTION

Control Requirements for High and Moderate Systems (H, M)

- System owners are responsible for ensuring that all George Mason-owned High and Moderate systems and components employ current endpoint protection software approved by the IT Security Office and are configured for automatic updates. The software must allow users to manually perform scans on their workstation and removable media, and must be configured to automatically scan for malicious code as follows:
    - Servers must be scanned for malicious code on a continuous basis.

- Workstations must be automatically scanned for malicious code on a daily basis.
- Systems and components relying on software for which the manufacturer is no longer providing security updates are not permitted on George Mason's network unless an exception is granted by the IT Security Office.
- High and Moderate system components that do not allow for user-installed software (e.g., network devices, virtual appliances, vendor-restricted systems) are only required to run protection software that the vendor supports.
- ITS is responsible for employing malicious code protection mechanisms for George Mason email systems and at George Mason's network boundaries. Such protection mechanisms must be kept current with automatic updates as new releases are made available.
- All malicious code protection mechanisms must be configured to automatically block and/or quarantine malicious code, and alert system administrators based on risk and when further action is required.

SI-4 SYSTEM MONITORING

Control Requirements for High and Moderate Systems (H, M)

- For all High and Moderate systems, system owners or designees must:
  - Enable system logging features, and monitor systems to detect attacks and indicators of potential attacks.
  - Review audit logs regularly in accordance with AU-6 Audit Review, Analysis, and Reporting.
  - Refer instances of attacks and suspected unauthorized use to the IT Security Office for investigation.
- ITS must monitor George Mason network boundaries and connections to High and Moderate systems to detect unauthorized network and remote connections, and analyze detected events and anomalies.
- ITS and system owners must heighten the level of system monitoring activity when there is an indication of increased risk to George Mason operations and assets.
- System monitoring must comply with Federal and Commonwealth of Virginia laws and directives. ITS is responsible for obtaining legal opinions from University Counsel regarding system monitoring activities and policies.
- The IT Security Office is responsible for notifying George Mason system owners, system administrators, and the campus community of changes to centralized system monitoring system.
- The IT Security Office is responsible for configuring the ITS centralized logging system to automatically alert on critical events where feasible; notifying system administrators when compromises are suspected; and coordinating incident response activities. [SI-4(2), SI-4(4), SI-4(5)]

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

General Controls (H, M, L)

- The IT Security Office is responsible for:
  - Receiving and evaluating information security alerts, advisories, and directives from established external security resources on an ongoing basis. Information security resources may include Federal, Commonwealth of Virginia, Higher Education, and industry entities.
  - Generating internal security alerts, advisories, and directives as deemed necessary.
  - Disseminating security alerts, advisories, and directives to system owners, system administrators, data owners, and system users as deemed necessary, including required response activities and time frames.
  - System owners must implement security directives in accordance with established time frames, and must notify the IT Security Office of any noncompliance.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control Requirements for High Systems (H)

- For High category systems, system owners and designees must employ file integrity monitoring tools to detect unauthorized changes to critical system files, configurations, and content; alert appropriate

personnel to unauthorized changes; and configure the software to perform critical file comparisons at least weekly. Examples of files to be monitored include, but are not limited to, the following:
    - System executables;
    - Application executables;
    - Configuration and parameter files; and
    - Log and audit files.
- Where technically feasible, file integrity checks must be performed:
    - At system startup;
    - Upon installation of new hardware, software, or firmware; and
    - When new security threats are identified which could impact the integrity of the monitored system. [SI-7(1)]
- System administrators are responsible for ensuring that suspected unauthorized file changes are reported to the IT Security Office, following established incident response procedures. [SI-7(7)]

SI-8 SPAM PROTECTION

Control Requirements for High and Moderate Systems (H, M)

- ITS must employ spam protection mechanisms for inbound and outbound email, on all authorized George Mason email systems.
- ITS may employ additional spam protection mechanisms at firewalls, remote access servers, and other system entry and exit points where technically feasible.
- Spam signature definitions must be automatically updated when new releases are available. Spam protection mechanisms must be updated when new releases are made available, following ITS configuration management procedures. [SI-8(2)]

SI-10 INFORMATION INPUT VALIDATION

Control Requirements for High Systems (H)

- For custom-developed applications including web forms, software developers must employ input validation rules to enforce specified syntax and semantics of user input data. System inputs include, but are not limited to:
    - Character set;
    - Length;
    - Numerical range; and
    - Acceptable values.

SI-11 ERROR HANDLING

Control Requirements for High Systems (H)

- For custom-developed applications, software developers and system administrators must ensure that system-generated error messages visible to the user do not reveal information that could be exploited; and that error messages providing information necessary for corrective actions are visible to authorized personnel. Information that could be exploited includes, for example, erroneous logon attempts with passwords mistakenly entered as the username and personally identifiable information such as account numbers, social security numbers, and credit card numbers.
- For all High category systems, system owners and designees must ensure that log messages containing system error information are visible only to authorized personnel, and that any configurable mechanisms to protect against inadvertent display of exploitable information are identified and appropriately enforced.

SI-12 INFORMATION MANAGEMENT AND RETENTION

Control Requirements for High and Moderate Systems (H, M)

- Data owners and data custodians are responsible for ensuring that information contained in, and output from, George Mason systems is managed and retained in accordance with University Policy 1102 Records Management and other relevant laws, regulations, and policies.

SI-16 MEMORY PROTECTION

Control Requirements for High and Moderate Systems (H, M)

- System administrators must employ security safeguards to protect system memory from execution of unauthorized code. Safeguards must be selected based on risk and impact, and may be documented in the associated baseline configuration and/or in the System Security Plan, or the operational procedures, or other supporting documents.
  Examples of controls that may be employed to protect memory include data execution prevention, and address space layout randomization.

EXCEPTIONS AND EXEMPTIONS

An exception is deviation from established policies, standards, procedures, or controls. Exceptions can arise when a risk control measure cannot be applied or is ineffective under certain conditions, leading to a temporary or permanent deviation from standard policies. Exceptions must be reviewed and approved in the context of the applicable Policy, Standard, Process, or Procedure.

Departments should reach out to IT Risk & Compliance at itrc@gmu.edu for assistance regarding using the Exceptions template (Sample in Appendix D).

Systems under development and/or experimental systems that do not create additional risk to production systems or data are exempt from complying with the requirements defined in this standard.

Note: Pre-production environments that utilize and/or contain production data, even if the data are older copies of data from the production environment, are not exempt from complying with the requirements defined in this standard.

TIMETABLE FOR REVIEW

This standard will be reviewed every 2 years.

APPROVALS

ROLE	NAME & ORGANIZATION	SIGNATURE	DATE
Director - IT Security Office	Curtis McNay	DocuSigned by: Curtis McNay 6179577EE174479...	12/13/2024
Vice President and Chief Information Officer	Charmaine Madison	Signed by: Charmaine Madison 213112EC65F44A7...	12/20/2024

APPENDIX A – PROGRAM-LEVEL CONTROLS

The additional controls in this section are foundational and pertain to the university's overall information security program, rather than to specific information system baselines or system users. As such, ITS and university leadership are responsible for implementing these controls.

INCIDENT RESPONSE (IR)

IR-1 POLICY AND PROCEDURES

Policy Statement: The university must maintain an operational incident-handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, reporting, and user response activities. All suspected electronic security incidents, threats, and cyber-attacks must be reported following the guidelines and procedures described in University Policy 1305 Reporting Electronic Security Incidents. The Information Technology Security Office is responsible for creating, maintaining, and updating incident handling procedures and serves as the central authority for tracking incidents, assessing impact, coordinating response and remediations with the appropriate offices and legal authorities, and reporting.

Related Documentation:
University Policy 1305 Reporting Electronic Security Incidents

IR-2 INCIDENT RESPONSE TRAINING

- The ITSO is responsible for ensuring that cybersecurity incident response training is provided for all university staff having incident response roles and responsibilities. Such training is required annually and when warranted by significant changes to the information systems environment, or to applicable laws, directives, and standards.
- The ITSO incorporates simulated events into incident response training, through the use of annual tabletop exercises to help ensure that personnel involved with incident response understand their responsibilities and required actions during an actual incident. [IR-2(1)]

IR-3 INCIDENT RESPONSE TESTING

- The ITSO monitors effectiveness of the incident response capability by assessing the results of annual tabletop exercises and simulations, summarizing lessons learned, and reviewing results with the participants. Corrective actions must be employed to address any weaknesses or deficiencies in procedures or training that are identified during the reviews.
- Factors to be considered during the design of incident response tests include reporting requirements to state and federal government agencies, university leadership, and affected individuals. George Mason's Environmental Health and Safety office shall be informed of upcoming incident response tests, and invited to participate in light of their key role in emergency management and crisis communications. [IR-3(2)]

IR-4 INCIDENT HANDLING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- ITS must maintain incident handling capabilities that effectively support the incident response process. These capabilities are comprised of people, processes, and technology and include preparation, detection and analysis, containment, eradication, and recovery.

- Incident handling plans and activities must be integrated with information system recovery and reconstitution plans (i.e., COOP), emergency management policies and procedures, and legal requirements for reporting incidents.
- ITS must incorporate lessons learned from incident handling activities into operational procedures, training, and testing.
- ITS must employ automated mechanisms such as Intrusion Detection Systems and network packet capture devices to support incident handling processes. [IR-4(1)]

IR-5 INCIDENT MONITORING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- ITS must document basic information concerning reported electronic security incidents in the service ticket management system. Such information shall contain at a minimum contact information for the reporting entity, high level description of the issue, timeline of response, and outcome of the response. The ITSO may determine that detailed information about the incident and impacts must remain confidential, depending on the nature of the incident.
- The ITSO integrates reported incidents with results from network and audit monitoring to evaluate and track trends and metrics.

IR-6 INCIDENT REPORTING

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- University personnel must report suspected electronic security incidents as soon as possible and within 24 hours of discovery, following the guidance in University Policy 1305 Reporting Electronic Security Incidents.
- The suspected incident may be reported to one or more of the following:
  - The affected unit's Security Liaison if that point of contact exists
  - The ITS Support Center
  - The IT Security Office
- Per Virginia Code § 2.2-5514 the Vice President for Information Technology is required to report cybersecurity threats and incidents to the Virginia Fusion Intelligence Center, in the following cases:
  - The incident threatens the security of the Commonwealth's data or communications, or results in exposure of data protected by federal or state laws.
  - The incident compromises the security of the university's information technology systems, with the potential to cause major disruption to the normal activities of the university or other public bodies.
- Cybersecurity threats and incidents involving Controlled Unclassified Information or export-controlled data must be reported to the university's Office of Research Integrity and Assurance, and to the appropriate government channels.
- Incidents involving exposure of Personally Identifiable Information (PII) or Protected Health Information (PHI) must be reported in accordance with state and federal regulations. ITS reports these events in collaboration with the Office of University Counsel.

IR-7 INCIDENT RESPONSE ASSISTANCE

- ITS serves as the central point of contact for incident response activity, providing advice and assistance and incident tracking via the service ticket management system.
- The ITSO manages threat and incident response activities, relying on internal capabilities with access to external forensic services and resources when required. [IR-7(2)]

IR-8 INCIDENT RESPONSE PLAN

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- ITS maintains the following documents detailing incident response process and procedures:
  - ITS.ITS-PRS004 ITS Incident Management Process
  - ITS.ITSO-PROC004 Security Incident Response Procedures
- These documents shall be reviewed and approved by ITS leadership as per the ITS.ITRC-PROC001 ITS Documentation Procedure, or when required to address changes to the operating environment.
- Incident response procedures must include any state and federal requirements for reporting breaches of Personally Identifiable Information. [IR-8(1)]

PROGRAM MANAGEMENT (PM)

PM-1 INFORMATION SECURITY PROGRAM PLAN

Policy Statement: The university must develop, document, and implement an information security program to protect the university's information and information resources, commensurate with risk. The Vice President for Information Technology is responsible for ensuring that an information security program plan, approved by the university President or designee, is created and disseminated to all authorized individuals who are responsible for implementing the plan. The program should be reviewed annually and updated as required to address environmental changes.

Key elements of the plan include:

- 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.
- Identification and assignment of roles, responsibilities, management commitment, coordination among university entities, and compliance.
- Requirements for coordination among university entities responsible for the different aspects of the plan (i.e., technical, physical, personnel, and privacy).

Related Documentation:
University Policy 1114 Data Stewardship
University Policy 1316 Controlled Unclassified Information

PM-2 INFORMATION SECURITY LEADERSHIP ROLE

- The Vice President for Information Technology is responsible for designating a role for a CISO or equivalent staff leading the information security function, who has the authority and duty to administer the information security policy, standards, and procedures included in the overall information security program.

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

- The Vice President for Information Technology, university President and designees are responsible for ensuring that capital planning and investment requests include the resources needed to implement the information security program. Exceptions must be documented, including a description of any compensating controls that will be implemented to mitigate risk.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

- The Vice President for Information Technology must ensure that a process is implemented to develop and maintain plans of action and milestones for the information security program. The plans of action and milestones must be reviewed for consistency with the university's risk management strategy and priorities, and remedial actions required to adequately respond to risk to university operations and assets must be documented.

PM-5 SYSTEM INVENTORY

- Information resource owners at the university must comply with the ITS Risk Assessment Procedure when instantiating new information systems. All information systems that will store or process regulated personally identifiable information shall be categorized as High. Under the University policy, such data are classified as Protected categories (Highly Sensitive Data and Restricted Data) Departmental leaders are responsible for putting mechanisms in place to report any new systems or significant changes to existing systems (including decommissions of systems) to the ITS within a reasonable period (not to exceed 90 business days).
- The inventory of High systems must include indicators designating systems that have been approved to store regulated PII. [PM-5(1)]

PM-6 MEASURES OF PERFORMANCE

- The Vice President for Information Technology or designee is responsible for developing, monitoring, and reporting on the results of information security measures of performance.

PM-7 ENTERPRISE ARCHITECTURE

- The Vice President for Information Technology or designee is responsible for developing and maintaining an enterprise architecture that incorporates consideration for information security and the resulting risk to university operations, assets, individuals, and other organizations. The architecture strategy may include offloading supportive but non-essential functions such as printing to external service providers.

PM-9 RISK MANAGEMENT STRATEGY

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- The information security program shall be based on risk management activity that identifies and evaluates internal and external risks to customer information and assesses the sufficiency of safeguards in place.

PM-13 SECURITY AND PRIVACY WORKFORCE

- The ITSO is responsible for establishing a security workforce development and improvement program. Goals of the program shall include defining knowledge, skills, and abilities needed to perform information security duties, developing or identifying specific role-based training programs for individuals that are assigned security roles and responsibilities, and providing standards and guidelines for incumbents and applicants for security-related positions. The security workforce development and improvement program is complementary to George Mason's security awareness and training program, and focuses on developing and institutionalizing the information security capabilities of personnel tasked with protecting the university's operations, assets, and individuals.

PM-14 TESTING, TRAINING, AND MONITORING

- ITS, under direction of the Vice President for Information Technology, is responsible for implementing a process for ensuring that George Mason's plans for conducting information security testing, training, and system monitoring activities are developed, maintained, and regularly executed. Testing, training, and monitoring plans shall be reviewed for consistency with George Mason's risk management strategy and priorities for risk response.

PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

- The ITSO is responsible for establishing and institutionalizing contact with selected groups within the security community:

- To facilitate ongoing information security education and training for George Mason personnel;
- To stay current with recommended security practices, techniques, and technologies; and
- To share current security information, including threats, vulnerabilities, and incidents.

PM-16 THREAT AWARENESS PROGRAM

- The ITSO is responsible for implementing a threat awareness program that includes a cross-organization information sharing capability for threat intelligence.
- Automated information feeds shall be employed to update threat detection and monitoring tools with timely intelligence and threat detection signatures. [PM-16(1)]

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

- The university President and designees are responsible for establishing policy and procedures to ensure that controlled unclassified information that is processed, stored, or transmitted on external systems is protected in accordance with applicable laws, executive orders, directives, policies, regulations, and standards. The policy and procedures shall be reviewed and updated as per ITS.ITRC-PROC001 ITS Documentation Procedure.

PM-23 DATA GOVERNANCE BODY

- The university President and designees are responsible for establishing a Data Governance body consisting of persons appointed by the Chief Data Stewards. The Data Governance body is tasked with establishing policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, regulations, policies, and standards.

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

- The Vice President for Finance and the Vice President for Information Technology are jointly responsible for developing the university's strategy for managing supply chain risk associated with the development, acquisition, maintenance, and disposal of information systems, system components, and services, and implementing it consistently across the organization. The supply chain risk management strategy shall be reviewed and updated as required, to address environmental changes and changes in the university's risk profile.
- Suppliers of critical or mission-essential technologies, products, and services, and all supplier/service arrangements involving the transfer, processing, or storage of protected data, must be identified, prioritized, and assessed prior to implementation. [PM-30(1)]

PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY (PT)

PT-1 POLICY AND PROCEDURES

Policy Statement: The university must protect personally identifiable information in accordance with obligations defined by applicable state and federal statutes. Personally identifiable information is categorized as protected data, and managed in accordance with University Policy 1114 Data Stewardship. Information collected by George Mason websites is handled in accordance with the university's Internet Privacy Policy Statement.

Other applicable policies include:

- University Policy 1102 Records Management

- University Policy 1117 Responding to Virginia Freedom of Information Act (FOIA) Requests for Records
- University Policy 1118 Compliance with the Health Insurance Portability and Accountability Act (HIPAA)
- University Policy 1122 FERPA Compliance
- University Policy 1315 Employees' Electronic Communications
- University Policy 4017 Research Involving Human Subjects

SUPPLY CHAIN RISK MANAGEMENT (SR)

SR-1 POLICY AND PROCEDURES

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

Policy Statement: Managing supply chain risk is a shared responsibility. The Purchasing Office, under authority from the Vice President for Finance, establishes policies, standards, procedures, and guidelines for acquiring goods and services. ITS, under authority of the Vice President for Information Technology, is responsible for establishing control requirements to protect George Mason data and information resources. The two offices, with guidance from University Counsel, develop contract language and oversight requirements for vendor relationships involving information technologies, products, and services. In the context of information technology security, the primary supply chain concerns at George Mason are associated with supplier/service arrangements involving the transfer, processing, or storage of protected data (aka Third-Party Risk Management.)

Related Documentation:
University Policy 1307 Procurement and/or Development of Administrative Systems/Applications
University Policy 2106 Purchase of Goods and Services

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- For all proposed purchases that would involve the transfer, processing, or storage of protected data, ITS and the Purchasing Office must develop and implement processes and procedures to:
  - Identify and assess risks associated with the proposed purchase;
  - Define required control requirements, usage parameters, and contract language to reduce residual risk;
  - Validate the eligibility of potential suppliers;
  - Establish a contract with the selected supplier;
  - Monitor supplier performance, to include regular assessments of the supplier's information security program; and
  - Implement corrective actions and/or compensating controls in cases where the supplier fails to meet contractual requirements or demonstrates deficiencies in their security program.
- Supply chain risks must be evaluated using a team approach, to include the ASRB, Purchasing, and IT Risk & Compliance groups with input from the IT Security Office and functional areas as required. [SR-2(1)]

SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES

16 CFR 314.4 [GLBA 'Standards for Safeguarding Customer Information' Relevant]

- ITS must establish processes to identify and manage third-party risks in coordination with the university Purchasing Office. Salient elements include:
  - Developing and employing processes and methods to assess third-party vendor risk;

- Coordinating with business units to evaluate, categorize, and address risks associated with proposed usage and operating environment;
- Assessing suitability of a proposed supplier's information security program;
- Maintaining an inventory of supplier/service arrangements that are categorized as High;
- Monitoring performance of each High category supplier's security program over the contract lifecycle; and
- Identifying security deficiencies with High category suppliers, and forwarding issues of noncompliance to the Purchasing Office to institute remedial actions.

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

- University units must comply with the ASRB review process when submitting requests for proposed purchases and contract arrangements that involve the transfer, processing, or storage of George Mason data.
- Supplier arrangements categorized as High category during the ASRB review must be inventoried and managed by ITS in accordance with ITS.ITRC-PRS003 Third-Party Risk Management Process.
- ITS must assess the effectiveness of each High category supplier's security program annually, and upon learning of a major security breach. The results of each assessment must be maintained for future reference and audits.
- For each High category supplier, ITS must evaluate the applicability of any complementary user entity controls called out in the supplier's information security audit reports, determine the university business unit that is responsible for implementing each user entity control, and assess whether each required control is suitably implemented.
- University business units are responsible for effectively implementing any required complementary user entity controls, and must institute corrective actions as directed by ITS.

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

- For purchases and contracts that would involve the transfer, processing, or storage of protected data, proposed new suppliers must undergo an ASRB review which includes a risk assessment. The risk assessment process may include any or all of the following:
  - Security questionnaires;
  - Usage scenarios, parameters, constraints, and complementary controls;
  - Publicly available information regarding prior security breaches;
  - Vendor reputation scores generated by third-party risk monitoring services; and
  - Reviews of audit reports or other independent assessments of the supplier's information security program.
- ITS raises any risk-related concerns with Purchasing, the proposed supplier, the responsible business unit, and other internal entities as needed to determine whether the contract should proceed, or if compensating controls must be implemented.

APPENDIX B – CONTROL BASELINES

The table included here shows which controls are applicable to each system category. Based on FIPS 199 based categorization, if a system is not deemed as High or Moderate, it is considered Low.

Control Identifier	Control (or Control Enhancement) Name	Security Control Baseline High	Security Control Baseline Moderate	Security Control Baseline Low
AC-1	Policy and Procedures	x	x	x
AC-2	Account Management	x	x	x
AC-2(3)	Account Management | Disable Accounts	x		
AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts	x		
AC-2(13)	Account Management | Disable Accounts for High-risk Individuals	x	x	x
AC-3	Access Enforcement	x	x	x
AC-4	Information Flow Enforcement	x		
AC-5	Separation of Duties	x		
AC-6	Least Privilege	x	x	x
AC-6(1)	Least Privilege | Authorize Access to Security Functions	x	x	x
AC-6(2)	Least Privilege | Non-privileged Access for Non-security Functions	x	x	x
AC-6(5)	Least Privilege | Privileged Accounts	x	x	
AC-6(6)	Least Privilege | Privileged Access by Non-organizational Users	x		
AC-6(7)	Least Privilege | Review of User Privileges	x	x	
AC-6(9)	Least Privilege | Log Use of Privileged Functions	x	x	
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	x	x	
AC-7	Unsuccessful Logon Attempts	x	x	x
AC-8	System Use Notification	x	x	
AC-11	Device Lock	x	x	

AC-11(1)	Device Lock | Pattern-hiding Displays	x	x	
AC-12	Session Termination	x	x	
AC-14	Permitted Actions Without Identification or Authentication	x	x	
AC-17	Remote Access	x	x	x
AC-17(1)	Remote Access | Monitoring and Control	x	x	
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	x	x	
AC-17(3)	Remote Access | Managed Access Control Points	x	x	
AC-17(4)	Remote Access | Privileged Commands and Access	x		
AC-18	Wireless Access	x	x	x
AC-18(1)	Wireless Access | Authentication and Encryption	x	x	
AC-19	Access Control for Mobile Devices	x	x	
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	x		
AC-20	Use of External Systems	x	x	x
AC-20(1)	Use of External Systems | Limits on Authorized Use	x		
AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	x		
AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	x		
AC-21	Information Sharing	x		
AC-22	Publicly Accessible Content	x		
AT-1	Policy and Procedures	x	x	x
AT-2	Literacy Training and Awareness	x	x	x
AT-2(2)	Literacy Training and Awareness | Insider Threat	x	x	x
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	x	x	x

AT-3	Role-based Training	x	x	x
AT-4	Training Records	x	x	x
AU-1	Policy and Procedures	x	x	x
AU-2	Event Logging	x	x	
AU-3	Content of Audit Records	x	x	
AU-3(1)	Content of Audit Records | Additional Audit Information	x		
AU-4	Audit Log Storage Capacity	x	x	
AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	x		
AU-5	Response to Audit Logging Process Failures	x	x	
AU-6	Audit Record Review, Analysis, and Reporting	x	x	
AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	x		
AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	x		
AU-7	Audit Record Reduction and Report Generation	x	x	
AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	x		
AU-8	Time Stamps	x	x	
AU-9	Protection of Audit Information	x	x	x
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	x	x	x
AU-11	Audit Record Retention	x	x	x
AU-12	Audit Record Generation	x	x	
CA-1	Policy and Procedures	x	x	x
CA-2	Control Assessments	x		
CA-2(1)	Control Assessments | Independent Assessors	x		
CA-3	Information Exchange	x		
CA-5	Plan of Action and Milestones	x		
CA-7	Continuous Monitoring	x		
CA-7(1)	Continuous Monitoring | Independent Assessment	x		

CA-8	Penetration Testing	x		
CA-9	Internal System Connections	x		
CM-1	Policy and Procedures	x	x	x
CM-2	Baseline Configuration	x	x	
CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas	x		
CM-3	Configuration Change Control	x		
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	x		
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	x	x	
CM-4	Impact Analyses	x		
CM-5	Access Restrictions for Change	x		
CM-6	Configuration Settings	x		
CM-7	Least Functionality	x		
CM-7(1)	Least Functionality | Periodic Review	x		
CM-7(2)	Least Functionality | Prevent Program Execution	x		
CM-7(4)	Least Functionality | Unauthorized Software	x		
CM-7(5)	Least Functionality | Authorized Software	x		
CM-8	System Component Inventory	x		
CM-8(1)	System Component Inventory | Updates During Installation and Removal	x		
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	x		
CM-9	Configuration Management Plan	x		
CM-10	Software Usage Restrictions	x	x	
CM-11	User-installed Software	x		
CP-1	Policy and Procedures	x	x	x
CP-2	Contingency Plan	x**		
CP-2(1)	Contingency Plan | Coordinate with Related Plans	x**		

CP-2(3)	Contingency Plan | Resume Mission and Business Functions	x**		
CP-2(8)	Contingency Plan | Identify Critical Assets	x**		
CP-3	Contingency Training	x**		
CP-4	Contingency Plan Testing	x**		
CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans	x**		
CP-4(2)	Contingency Plan Testing | Alternate Processing Site	x**		
CP-6	Alternate Storage Site	x**		
CP-6(1)	Alternate Storage Site | Separation from Primary Site	x**		
CP-7	Alternate Processing Site	x**		
CP-7(1)	Alternate Processing Site | Separation from Primary Site	x**		
CP-7(4)	Alternate Processing Site | Preparation for Use	x**		
CP-8	Telecommunications Services	x		
CP-8(2)	Telecommunications Services | Single Points of Failure	x		
CP-9	System Backup	x		
CP-9(1)	System Backup | Testing for Reliability and Integrity	x		
CP-9(8)	System Backup | Cryptographic Protection	x		
CP-10	System Recovery and Reconstitution	x**		
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	x**		
IA-1	Policy and Procedures	x	x	x
IA-2	Identification and Authentication (organizational Users)	x	x	x
IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	x		

IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	x		
IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	x		
IA-3	Device Identification and Authentication	x		
IA-4	Identifier Management	x	x	
IA-5	Authenticator Management	x	x	
IA-5(1)	Authenticator Management | Password-based Authentication	x	x	
IA-5(2)	Authenticator Management | Public Key-based Authentication	x		
IA-5(6)	Authenticator Management | Protection of Authenticators	x	x	
IA-6	Authentication Feedback	x	x	
IA-7	Cryptographic Module Authentication	x	x	
IA-11	Re-authentication	x	x	
IA-12	Identity Proofing	x	x	
IA-12(2)	Identity Proofing | Identity Evidence	x	x	
IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification	x		
MA-1	Policy and Procedures	x	x	x
MA-2	Controlled Maintenance	x		
MA-3	Maintenance Tools	x		
MA-3(1)	Maintenance Tools | Inspect Tools	x		
MA-3(2)	Maintenance Tools | Inspect Media	x		
MA-4	Nonlocal Maintenance	x		
MA-5	Maintenance Personnel	x		
MP-1	Policy and Procedures	x	x	x
MP-2	Media Access	x		
MP-3	Media Marking	x		
MP-4	Media Storage	x	x	
MP-5	Media Transport	x		

MP-6	Media Sanitization	x	x	x
MP-7	Media Use	x		
PE-1	Policy and Procedures	x	x	x
PE-2	Physical Access Authorizations	x		
PE-3	Physical Access Control	x		
PE-3(8)	Physical Access Control | Access Control Vestibules	x		
PE-4	Access Control for Transmission	x		
PE-5	Access Control for Output Devices	x		
PE-6	Monitoring Physical Access	x		
PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	x		
PE-6(3)	Monitoring Physical Access | Video Surveillance	x		
PE-8	Visitor Access Records	x		
PE-9	Power Equipment and Cabling	x		
PE-9(2)	Power Equipment and Cabling | Automatic Voltage Controls	x		
PE-10	Emergency Shutoff	x		
PE-11	Emergency Power	x		
PE-11(2)	Emergency Power | Alternate Power Supply — Self-contained	x		
PE-12	Emergency Lighting	x	x	
PE-13	Fire Protection	x		
PE-13(1)	Fire Protection | Detection Systems – Automatic Activation and Notification	x		
PE-13(2)	Fire Protection | Suppression Systems – Automatic Activation and Notification	x		
PE-14	Environmental Controls	x		
PE-14(1)	Environmental Controls | Automatic Controls	x		
PE-14(2)	Environmental Controls | Monitoring with Alarms and Notifications	x		
PE-15	Water Damage Protection	x		
PE-15(1)	Water Damage Protection | Automation Support	x		

PE-16	Delivery and Removal	x		
PE-17	Alternate Work Site	x	x	
PL-1	Policy and Procedures	x	x	x
PL-2	System Security and Privacy Plans	x		
PL-4	Rules of Behavior	x	x	x
PL-4(1)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	x	x	x
PL-8	Security and Privacy Architectures	x		
PL-10	Baseline Selection	x	x	x
PL-11	Baseline Tailoring	x		
PS-1	Policy and Procedures	x	x	x
PS-2	Position Risk Designation	x	x	x
PS-3	Personnel Screening	x		
PS-3(4)	Personnel Screening | Citizenship Requirements	x		
PS-4	Personnel Termination	x	x	x
PS-5	Personnel Transfer	x	x	x
PS-6	Access Agreements	x	x	
PS-7	External Personnel Security	x		
PS-8	Personnel Sanctions	x	x	x
PS-9	Position Descriptions	x	x	x
RA-1	Policy and Procedures	x	x	x
RA-2	Security Categorization	x	x	x
RA-3	Risk Assessment	x		
RA-5	Vulnerability Monitoring and Scanning	x	x	
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	x	x	
RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	x		
RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	x	x	x
RA-7	Risk Response	x	x	x
RA-9	Criticality Analysis	x		
SA-1	Policy and Procedures	x	x	
SA-2	Allocation of Resources	x		

SA-3	System Development Life Cycle	x		
SA-4	Acquisition Process	x		
SA-4(1)	Acquisition Process | Functional Properties of Controls	x		
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	x		
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	x		
SA-4(10)	Acquisition Process | Use of Approved PIV Products	x		
SA-5	System Documentation	x		
SA-8	Security and Privacy Engineering Principles	x		
SA-9	External System Services	x		
SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	x		
SA-15	Development Process, Standards, and Tools	x		
SA-22	Unsupported System Components	x		
SC-1	Policy and Procedures	x	x	x
SC-2	Separation of System and User Functionality	x		
SC-4	Information in Shared System Resources	x		
SC-5	Denial-of-service Protection	x		
SC-7	Boundary Protection	x	x	x
SC-7(3)	Boundary Protection | Access Points	x	x	x
SC-7(4)	Boundary Protection | External Telecommunications Services	x	x	
SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	x		
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	x	x	
SC-8	Transmission Confidentiality and Integrity	x		

SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	x		
SC-10	Network Disconnect	x		
SC-12	Cryptographic Key Establishment and Management	x		
SC-13	Cryptographic Protection	x		
SC-15	Collaborative Computing Devices and Applications	x		
SC-17	Public Key Infrastructure Certificates	x	x	
SC-18	Mobile Code	x		
SC-22	Architecture and Provisioning for Name/address Resolution Service	x	x	x
SC-23	Session Authenticity	x	x	
SC-28	Protection of Information at Rest	x		
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	x		
SC-39	Process Isolation	x	x	
SC-45	System Time Synchronization	x	x	
SI-1	Policy and Procedures	x	x	x
SI-2	Flaw Remediation	x	x	
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	x	x	
SI-3	Malicious Code Protection	x	x	
SI-4	System Monitoring	x	x	
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	x		
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	x	x	
SI-4(5)	System Monitoring | System-generated Alerts	x	x	
SI-5	Security Alerts, Advisories, and Directives	x	x	x
SI-7	Software, Firmware, and Information Integrity	x		

SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	x		
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	x		
SI-8	Spam Protection	x	x	
SI-8(2)	Spam Protection | Automatic Updates	x	x	
SI-10	Information Input Validation	x		
SI-11	Error Handling	x		
SI-12	Information Management and Retention	x	x	
SI-16	Memory Protection	x	x	

** Control Requirements for High Systems where 'Availability' requirement in FIPS 199 is 'High'

APPENDIX C – SYSTEM USE NOTIFICATION BANNER TEMPLATES

George Mason information systems must be configured to display a system notification banner conforming to the requirements of control AC-8, prior to login if technically feasible. The following examples meet these requirements; any one of these may be employed as appropriate for the system use cases and technical capabilities.

Version 1:
This computer system is the property of George Mason University. It is for authorized use only. By using this system, all users acknowledge notice of and agree to comply with University Policy Number 1301 (universitypolicy.gmu.edu/policies/responsible-use-of-computing) and University Policy Number 1311 (universitypolicy.gmu.edu/information-technology-security-program) and the related policies and standards, as well as Code of Virginia, Section 2-28272.

LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Version 2:
This computer system is the property of George Mason University. Usage may be monitored, recorded, and subject to audit. Unauthorized use of this system is strictly forbidden and may violate state and/or federal law. By using this system, all users acknowledge notice of and agree to comply with University Policy Number 1301 (universitypolicy.gmu.edu/policies/responsible-use-of-computing) and University Policy Number 1311 (universitypolicy.gmu.edu/information-technology-security-program), and if applicable, the Student Information Security Statement (patriotweb.gmu.edu/secagree.html), related policies and standards, and the Code of Virginia, Section §2.2-2827. Use of this system constitutes express consent to these terms and conditions.

Please log off immediately if you do not agree to the conditions stated in this notice.

Version 3:
This computer system is the property of George Mason University. It is for authorized use only. Usage may be monitored, recorded, and subject to audit. All users must comply with University Policy Number 1301 Responsible Use of Computing. Click here to read the policy. Unauthorized use of this system is prohibited and may be subject to administrative disciplinary action and/or criminal and civil penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions.

LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

GEORGE MASON UNIVERSITY

APPENDIX D – EXCEPTIONS FORM TEMPLATE

Exception Type		Exception ID	EXP-001		
Issue Sub-Type	Not Applicable				
Date Identified	2/1/2023				
Date Reported	2/1/2023	Requester			
Exception Expires		Control Owner	Noor Aarohi		
Requester	Noor Aarohi	Exception Extension Valid Thru			
Short Description		Notification to	ITS Senior Leadership Listserv		
Detailed Description		Program ID			
Asset (s) - attach list if needed	Attached list	Project ID			
Vendor Name	N/A	Project Priortization			
Criteria		Project Status			
Root Cause		Authority Document			
TCF Control ID	1.2.2	Control Objective	The governance of the Technology organization to policies, standards, and procedures is established through a formally defined program.	Control Sub-Objective	The governance of the Technology organization to policies, standards, and procedures is established through a formally defined program.
NIST 800-53 Control	RA-1				
Applicable Regulations					
Risk Statement					
Inherent Risk	Medium				
Residual Risk	Medium				
Direction of Risk	Stable				
Risk Treatment Decision	Remediate				
Remediation Plan	Risk and Compliance to work with the document owners to review and refresh				
Prioritization Decision					
Plan of Action and Milestones (POA&M) Status	In Progress				
Exception Approved by		Approver Comments			
Approver Signature					