Information Data Security

George Mason University (Mason) has a developed set of standards for information security for data acquired, generated, maintained, and disposed of by the university. These policies and practices are applicable depending on the category of data involved. Mason currently manages categories of data ranging from non-sensitive/publicly available up to top secret. The overall guiding principles for data protection at the university are specified in University Policy Number 1114, *Data Stewardship*. This policy specifies security and confidentiality provisions for protected data (including restricted and highly sensitive data) as well as breach response procedures by the Computer Security Incident Response Team. Principles for protecting export controlled information and data are specified in University Policy Number 1141, *Export Controls and Sanctions Compliance* and associated procedures (https://universitypolicy.gmu.edu/policies/export-controls-and-sanctions-compliance/). Principles for protecting classified information and information are specified in University Policy 1119, *Classified Information and Personnel Security Clearances,* and associated procedures (https://universitypolicy.gmu.edu/policies/classified-information-and-personnel-security-clearances/).

These policies and procedures set the framework for Mason's protection of data and information acquired or generated by researchers. The data owner for any research project is the Principal Investigator.

For any project or other acquisition or generation of restricted data, the Principal Investigator will work with the Chief Information Security Officer (CISO) as well as the Director, Export Compliance and Secure Research (for highly sensitive data including Export Controlled Data). For classified data, the Director will work with the Facility Security Officer. Additionally, the following controls are in place for Mason enterprise systems:

Controls on Access to University Systems and Data

Authentication

- 2 Factor Authentication for Remote Access
- Centralized audit and lockout for "at risk" or compromised accounts

Physical and Logical Access Security Policy

- Requires authentication and authorization control
- Requires strong provisioning and de-provisioning procedures
- Requires that "least privileges" access rules are applied
- Requires protection of authentication credentials

Remote Access Control

Remote Access Policy and Standard

- Defines requirements for secure remote access to IT resources
- 2 Factor Authentication
- Defines user responsibilities

Virtual Private Network (VPN)

- Provides for secure remote, authenticated access to the network
- Provides auditable logging of remote access

Network Security

Firewall Protection

- Firewalls hosted at Fairfax and Prince William for disaster recovery and redundancy
- Provides for granular network protection for University servers and critical IT systems

Wireless Security

- Centrally managed wireless networks with Access Control
- Able to identify and shut down rogue wireless networks
- Enforces secure wireless protocols

Multi-Protocol Label Switching (MPLS) Architecture - allowing for flexible, logical network security boundaries as required by security needs. Providing separate logical networks for:

- Credit card handling systems
- VoIP telephones
- Sensitive units (such as Student Health Services and others)
- Research networks
- Classrooms and labs (Higher Risk Containment)
- Physical security systems (door locks and cameras)

Cryptography

Enterprise Encryption for data "at rest" to protect laptops and desktops which have been approved to store highly sensitive data

- Bitlocker for Windows systems managed through MESA
- Apple FileVault for Apple computers managed through Casper

Incommon Certificate Services (through Comodo –Encryption certificates)

- Provides encrypted SSL (https) authentication and sessions for web applications
- Provides identity certificates
- Able to provide for federated authentication

Security Architecture and Design

Mason Enterprise Services Architecture (MESA) Desktop Management and Centralized File Storage Services

- Provides standardized desktop deployment and configuration management of Microsoft workstations, laptops and servers
- Provides secure, flexible file storage
- Manages security settings, updates, controls access, provides monitoring of Microsoft workstations, laptops and servers
- Provides for rapid rebuild of infected or repurposed Microsoft workstations, laptops

Casper Suite – JAMF Software

- Provides standardized desktop deployment and configuration management of Apple workstations, laptops and servers
- Manages security settings, updates, controls access, provides monitoring of Apple workstations, laptops and servers
- Provides for rapid rebuild of infected or repurposed Apple workstations, laptops

Security Architecture for Physical and Virtual Server Hosting

- Security zone containment for different classes of risk

- Allows for disaster recovery, as virtual systems are replicated to disaster recovery hot site

Data Destruction Program

- Data removal and/or destruction for all surplus computers, servers network appliances and printer equipment through a recycling company

Operations Security

Security Operations Center within the IT Security Offices

- Staff actively monitor for malicious activity or compromised systems
- Active work flow for identifying and remediating at-risk and infected systems

Security Information and Event Management System (SIEM) –

- Allows for remote collection and analysis of system logs from firewalls, intrusion detection systems (IDS), vulnerability scanners, antivirus software, network devices, servers, authentication systems, databases and other critical and sensitive systems
- Correlated event analysis and alerting. Examples are:
    - Privileged account fails or succeeds in authenticating to a system after multiple failures
    - Repeated attacks from a specific address

Intrusion Detection System

- Provides for the monitoring of suspicious network traffic

Malware Protection from web based threats and infected workstations

- Provides for passive and active protection from malicious web sites, botnets and malicious "command and control" systems
- Quick Identification of infected workstation providing for quick remediation

Vulnerability Scanning

- A central solution with delegated access for scanning any system on the University LAN
- Provides system administrators the ability to perform their own scans

Monitor System Service Continuity

- Can determine if a system or service is down
- Alerts if a condition is not met or a system is down

Email Filtering and Alerting

- Filters out more than 94 percent of spam and malicious email
- Is used in creating alerts if a phishing email attack has occurred

Anti-Virus Program (End Point Protection)

- Anti-virus Protection for all users
- Features host based firewall and intrusion protection services
- Checks for file reputation
- Provides centralized logging and alerting

Application Security

Architectural Standards Review

- IT Security Office vets any new service or system that integrates with central systems or has substantial business impact

Compliance and Investigations

Data Stewardship Policy outlines data classification and control requirements

Designated Data Owners and Chief Data Stewards with responsibilities for compliance to Federal and State Regulations

Risk Assessment for Highly Sensitive Systems

- Performed on systems that have been classified as Highly Sensitive

Computer Security Incident Response Team (CSIRT) –

- The CSIRT Team controls and assures that appropriate chain of custody is maintained and documented
- Performs forensic investigation and reporting on compromised systems to determine the nature of the compromise, and potential exposure of data, and when needed, partners with the University Police Department

Physical Security

Data Center Physical Security Controls

- Staffed 24 X 7
- Environmental controls for temperature, dust, humidity and fire prevention
- Controlled, limited physical access
- Redundant power with generator backup

Cyber Security Awareness

Security Liaisons, departmental representatives, meet once a semester, email communications, web site and "tool kit" packet for information sharing, special information sessions scheduled as needed

Systems Administrators Leadership Team (SALT) meets monthly, communications through BlackBoard group and a mailing list

Security Awareness Training, for all users, once a year, as an integrated part of the user's password change process

Communications campaigns that included:

- Phishing poster
- Security cards for students and another for faculty/staff
- Cyber Security Month (October) promotions
- Table during Welcome Week for students
- Security alerts to staff on phishing emails, critical vulnerabilities and security threats
-

Mason also has university policies on the following related topics:
1124 - University Owned Cellular Equipment
1301 - Responsible Use of Computing
1302 - Wireless Networking
1303 - Telecommunications Spaces and Cabling
1304 - Public Internet Address Policy
1305 - Reporting Electronic Security Incidents
1306 - Banner and Related Administrative Systems Security
1307 - Procurement and/or Development of Administrative Systems/Applications
1308 - Electronic and Information Technology Accessibility
1309 - Information Technology Infrastructure, Architecture and Ongoing Operations
1310 - Information Technology Project Management
1311 - Information Technology Security Program
1312 - Physical and Logical Access Security
1313 - Remote Access
1314 - Physical Access to Sensitive IT Facilities
1315 - Employees' Electronic Communications