UMES IT Security Program

University of Maryland Eastern Shore

Information Technology

Policies and Procedures

Subject: **UMES IT Security Program**	**Effective Date:** **08/16/2018**
Approved by:	**Review Date:**
	Approval Date:

I. Purpose

The purpose of this program is to establish a framework necessary to protect University of Maryland Eastern Shore (UMES) data and information systems by implementing a comprehensive IT Security Program. The IT Security Program, as implemented by the Information Technology Department (ITD), will enhance and protect the integrity, confidentiality, and availability of information resources by providing access controls to computing environments and information to authorized users.

Responsibility to protect and maintain UMES systems, data, and information is shared between administrators and end users. Campus personnel, including IT administrators, must follow approved procedures and prevent corruption or misuse UMES's software or hardware. In addition, end users must follow established proper usage policies for the appropriate use of systems and data as well as the protection of usernames and passwords. It is important for all UMES system users to review the following information to ensure awareness of current security practices employed at UMES.

II. Policy

It is the policy of UMES to maintain an IT security program that protects the integrity, confidentiality, and availability of information resources, as well as addresses compliance with all applicable laws and regulations. The UMES IT Security Program encompasses many key elements, including the following:

1. Planning for Security
    - Vulnerability Assessment
    - Consultation Services
2. Designing for Security
    - System Hardware and Application Architecture
    - Firewall Hardware/Software Provisioning
3. Access Control
    - Physical Security
    - Virtual Desktop Services
    - Authentication/ Authorization
    - Identity Management
4. Monitoring & Response
    - Intrusion Prevention and Detection
    - Incident Reporting and Response
    - Patch Diligence

- Disaster Recovery Planning

5. End User Diligence
    - IT Security Awareness and Training
    - E-mail Filtering (Spam & Virus), White Lists/Black Lists
    - Risk Alerts- Viruses, Phishing Scams
6. Governance
    - IT Security Officer
    - IT Related Policies/Standards
    - Intellectual Property (IP)/Illegal File Sharing Policy

III. Procedure

PLANNING FOR SECURITY

Vulnerability Assessment

The Information Technology Department provides consultation services for UMES

departments wishing to evaluate vulnerabilities in systems and procedures. Consultation can include documenting and mapping current processes, performing system audits, identifying areas for risk, reviewing Family Educational Rights and Privacy Act (FERPA) compliance, and developing mechanisms to remediate risk. In addition, the Information Technology Department Team will assist with queries for data in response to requests by auditors.

Consultation Services

The Information Technology Department provides consultation services to departments and academic entities planning new systems in order ensure acceptable availability, reliability, and maintainability. In addition, the ITD assists in planning for backup and restoration of data.

DESIGNING FOR SECURITY

System Hardware and Application Architecture

During the system development process, security architecture of the desired system is designed after completion of a security assessment in order to refine logical and physical security components to include:

- Logical architecture: Includes processes, technology and people and consists of system perimeter security, risk and threat analysis, incident response, antivirus policy, security administration, Disaster Recovery Plans (DRP), data security, application security, and infrastructure security.
- Physical architecture: Includes networking components such as firewalls, mail gateways, proxies, VLANs, Demilitarized Zone (DMZ), internal and external connections and devices.

Firewall Hardware/Software Provisioning

In order to promote and maintain the security of University of Maryland Eastern Shore (UMES) data and its network infrastructure, firewalls have been strategically installed as part of the overall network architecture. Requests for the opening or closing specific firewall ports to support applications are reviewed, researched, and acted upon by the Information Technology Department, who manages this service. Modifications to security protocols are made only upon review of requirements to ensure all changes meet UMES Security standards.

ACCESS CONTROL

Physical Security

As part of a comprehensive security program, physical security of information technology assets includes placement of equipment in locations with controlled access, as well as locations less likely to be impacted by floods, fires, and other calamities. Physical security also includes access to back-up power supplies where applicable.

Commensurate with the assessment of risks, physical access controls are in place for the following:

- Data Centers
- Areas containing servers and associated media

- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be based on need and approved by the manager responsible for the secured area.

Assets within the data center secured under this policy are listed in the UMES Disaster Recovery Plan (DRP). Risks associated with these assets are addressed in the University of Maryland Eastern Shore Disaster Recovery Plan.

As part of maintaining access control, UMES is responsible for:

- Ensuring that all portable storage media containing sensitive information such as hard drives, diskettes, magnetic tapes, laptops, and CDs are physically secured
- Ensuring that proper environmental and physical controls are established to prevent accidental or unintentional loss of sensitive information residing on IT systems
- Ensuring that any physical access controls are auditable

Storage Media Disposal - When no longer usable, diskettes, compact disks, tape cartridges, ribbons, and other similar items that contain sensitive data shall be destroyed by a NIST approved method such as shredding, incineration, overwriting, or degaussing. All IT equipment shall not be released from the university's control until the equipment is sanitized and all stored information has been cleared and documented. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient, including equipment transferred to schools. It also applies to equipment sent for maintenance or repair. Details concerning media disposal are available in the Electronic Media Disposal policy.

Authentication/ Authorization

University of Maryland Eastern Shore (UMES) employs a layered approach to accessing systems and data. This includes a robust approach to ensure that system access is granted only to users that are properly identified using login and password as a valid user (authentication) and that appropriate level of access (least privileged) is provided to the users to perform their tasks (authorization).

Identity Management

University of Maryland Eastern Shore (UMES) employs a centralized and integrated means of managing identity management for faculty, staff, and students. Identity management includes the provisioning of network accounts to new faculty, staff, and students, as well as role management, account termination, and password resets and synchronization.

MONITORING & RESPONSE

Intrusion Prevention and Detection

UMES systems are monitored routinely in order to detect any signs of intrusion attempts. Automated review of system logs is performed using specialized software. In addition, system domain policies have been put in place to lock out system access in cases of successive login failures.

Upon detection, the affected system(s) shall be isolated and suspected user accounts suspended, if applicable. UMES personnel shall investigate the scope and impact of the incident.

Incident Reporting and Response

Users are instructed to report any known breach of computer security as well as any suspicious or unusual computer incidents. In the event of an incident, the Information Technology Department will contact users and provide follow-up including forensic investigation, documentation, and systems and process remediation. Details concerning incidence response are available in the Incident Response Policy.

Patch Diligence

University of Maryland Eastern Shore systems and applications require periodic updates in response to existing or emerging security threats. Approved patches are applied to operating systems and applications as they are made available and updates may be installed outside of normal maintenance windows if deemed necessary by the Information Technology Department.

Disaster Recovery

The Information Technology Department provides Disaster Recovery (DR) planning assistance to departments including risk assessment and development of Business Impact Assessments (BIA) and Disaster Recovery plans. Services include consultation with departments to collect process details and assistance with documenting risks and remediation.

Disaster Recovery planning, Risk Assessments, and Business Impact Assessments are provided on an as-needed basis to departments and academic units requesting assistance. Details concern disaster recovery are available in the university's Disaster Recovery Plan.

END USER DILIGENCE

IT Security Awareness and Training

All University of Maryland Eastern Shore system users shall be provided an overview of fundamental security practices in use at UMES in order minimize risk when using IT systems. The training shall include a discussion including, but not limited to:

Passwords - The use of strong passwords.

Usernames - In conjunction with a valid password, the use of a unique identifier that will provide access to authorized systems.

Screen Saver Locks - Users shall be encouraged to utilize automated screen savers that employ a lock that requires them to enter a password after a period of inactivity.

Sensitive information – Protection of sensitive information.

Logoff – Protection of assets and information through timely system logoff.

Use by Proxy - Users shall be reminded never to access systems on behalf of someone else by logging into systems with another individual's username and password.

Business purpose only – Appropriate use of systems and information limited to UMES business only.

Phishing scams – attempts to falsely obtain network or application passwords.

E-mail Filtering (Spam & Virus), White Lists/Black Lists

As a part of University of Maryland Eastern Shore's (UMES) comprehensive security program, incoming email is automatically filtered for potential unwanted and potentially malicious email (spam).

Generally, the configuration of the filter adequately removes unwanted email while allowing appropriate email though. Occasionally, adjustments may be needed to ensure known and approved domains are added to the allowed (white) list and known and disapproved domains are added to the disallowed (black) list. Modifications to these lists will be made upon request.

Risk Alerts- Viruses, Phishing Scams

UMES monitors for emerging threats in the form of viruses and phishing scams. The Information Technology Department will send alerts to system users in cases where known and credible threats exist. Users are encouraged to contact the IT Helpdesk if they have any concerns about the contents of email.

GOVERNANCE

IT Security Officer

The University Of Maryland Eastern Shore Office Of Information Technology includes an IT Security Officer, reporting to the Director of Information Technology. The IT Security Officer helps minimize the risk of cyber-attacks, educates employees on computer security, monitors networks for security breaches, and responds to cyber-attacks as necessary with the appropriate countermeasures. In addition, the IT Security Officer enforces IT security policy compliance and supports security and audit inquiries.

Intellectual Property (IP)/Illegal File Sharing Policy

In support of Higher Education Opportunity Act (HEOA) and Digital Millennium Copyright Act of 1998 (DMCA) directives, UMES expects that all members of the university community (users) respect the rights of ownership of intellectual property by adhering to United States copyright laws, UMES policies, and state and federal laws. Users shall utilize copyrighted material, including materials and software, for authorized purposes only and in accordance with their specific copyrights, licenses, or agreements.

Users shall not copy, download, store, or share unauthorized copyrighted material (e.g. music and videos) on UMES computers, IT systems or networks. In addition, users shall not engage in the sharing of copyrighted material through the use of peer-to-peer networks.

Policy Compliance

All members of the campus community including faculty, staff, and students shall:

- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal and academic use.
- Be aware that file sharing in violation of copyright is prohibited.
- Not use, copy, or share copyrighted works unless possessing a legal right to do so.

Failure to comply with the above may provide the basis for sanctions or disciplinary action, and in serious violations, civil litigation and/or criminal prosecution.

Technology Support: UMES shall minimize the potential for illegal file sharing by implementing the following measures:

- Block access to Peer-to-Peer connections between UMES equipment and external networks. Special requests to access Peer-to-Peer networks shall be evaluated by OIT on a case-by-case basis and permission determined by academic need and potential risk.
- Utilize media monitoring software to determine if infractions have occurred.
- Violators risk losing access to the Internet until illegal file sharing activities/software are removed from their computing device(s).

Cabinet approval pending. 12/13/18