



Information Security

policy

Standards, Guidelines, Baselines Procedures

Version 1.0

Morgan State University

The University Board of Regents has approved the following Policy.

“Morgan State University (hereinafter the "University") has computer and information technology resources, which are dedicated to the support of the University's mission of teaching, research, and service. The University provides access to computing and information resources for students, faculty, and staff (collectively "users") consistent with institutional priorities and financial capabilities. Access to University computing resources imposes certain responsibilities and obligations on the user and is granted subject to University policies, federal, state and local laws. It is the University's policy that appropriate use should always be legal and ethical, reflect academic honesty, and show restraint in the consumption of shared resources.

The President shall establish rules and general guidance to University faculty, students and staff regarding use of the University's computing resources. Those rules shall define the general principles regarding the appropriate use of University equipment, software, and networks. Such rules shall also require that all members of the University community act in accordance with relevant laws, contractual obligations, and high ethical standards.”

The following information systems security policy, standard, guidelines, procedures and baselines are approved consistent with this authority.

Approved by

Morgan State University President (Dr. Earl Richardson) / Date

Reviewed by

Vice President for Planning & Information Technology (Dr. Joseph Popovich) / Date

Additional Reviewers:

Dr. Wole Akpose
Mr. Gilbert Goetz
Mr. Adrian Wiggins
Dr. Linda Mehlinger
Mr. Gilbert Morgan
Mr. Gary Press

PURPOSE

University Business requires and depends on data and information systems. Student, employee, research, and institutional data is governed by a number of regulations, laws and standards.

This document provides clear sets of policies, standards, guidelines, baselines and procedures for the protection of data, information and information systems to guarantee compliance with appropriate laws, regulations, and standards.

This document defines the minimum requirements which must be adhered to by each division, department, school, employee, student, contractor/consultant, partner, vendor, and guest using any of the University's information systems or infrastructure.

The objectives of this document include but are not limited to:

- Establish a secure environment for data and information processing, and utilization.
- Mitigate and avoid information security risks.
- Minimize and ultimately eliminate risks to user identity and likelihood of identity theft.
- Provide information and guidance about responsibilities for data and information protection and assurance.
- Protect privacy of user data in compliance with pertinent laws, regulations and standards.

SCOPE

This document covers all data and information in storage, transit or operational on all media types across and/or within the University information infrastructure.

This document covers all hardware, software and other systems owned by the University and/or used on the University information system for data and/or information processing

This document applies to all students, employees, contractors, vendors, guests and other entities whose operations and activities result in data and/or information processing that meets the description in the preceding paragraphs.

GOVERNANCE

Review

The university Security and Architecture Committee (SAC) shall be responsible for maintaining this document.

The SAC shall meet regularly, no less than twice annually to review the policy for effectiveness, relevance, and compliance with current laws and industry best practices.

Members of the SAC shall be as defined in the University IT Governance Document and listed later in this document.

Each change to this document shall trigger a version change consistent with the University technology documentation standard.

Approval

The President of the University shall approve this policy and may delegate such responsibility to the Vice President of Planning and Information Technology.

Compliance

The University Chief Information Security Officer (CISO) is responsible for compliance and enforcement of the policies, standards, guidelines, procedures and baseline in this document, and may rely on other divisional heads and/or departmental heads as needed.

This document and its implementation complies with relevant guidelines, policies, and laws of the State of Maryland, the federal government and industry best practices.

ROLES & RESPONSIBILITIES

Chief Information Security Officer

The University CISO shall develop policies, standards, procedures, guidelines, and baselines for the protection of data, privacy, and information, and related systems, including but not limited to hardware, software and operations of the various systems.

The University CISO shall develop an information security awareness program for the University community

The University CISO shall develop an information security risk management program to mitigate risks to data and information systems across the University.

The University CISO shall develop an information security incidence management program to provide clear guidance for incidence reporting, response and analysis.

The University CISO shall conduct regularly scheduled audits of data and information systems across the University to ensure compliance with this policy and all other related policies.

Users

All Users of University data, information and information systems are expected to understand and required comply with the policy, standard, guidelines, procedures and baselines.

Users shall be informed of and agree to the policy, standard, guidelines, procedures and baselines before being granted access to University data, information and information systems.

Effective Date

This document shall be effective from the date of its approval by the University President or his designated officer. Some part of the document may be effective at a later date.

DATA SECURITY

Data is essential to University business. The University and its agents (employees, contractors) collect data for various purposes. The University also stores these data in various systems including the University ERP database (Banner). Data collected on behalf of the University for any purpose is University data.

Security of data is a collective responsibility. All data must be safeguarded in accordance with appropriate laws, regulations and standards.

Electronic data shall be protected using available technology controls, including access, classification, audit, encryption, digital signature and others.

Each data type will have a pre-designated data custodian. A data custodian is responsible for the integrity, availability, confidentiality and privacy of the data under their jurisdiction. A data custodian is usually a departmental director, a dean, a program director, a principal investigator, a departmental chair or a vice president.

A data custodian shall implement a reasonable access control mechanism, with support from appropriate quarters, and using suitable technologies, for all data under their jurisdiction.

A data custodian shall implement a suitable mechanism to govern authorization to access under their jurisdiction.

The University CISO has overall responsibility for data security. The University CISO shall develop and implement awareness programs to educate users on how to protect University data.

The University CISO shall implement reasonable security measures to minimize potential risk to data. Such measures shall include data encryption standards and guidelines, access control standards and guidelines, and data privacy standards and guidelines.

The University CISO shall oversee data custodian access control and authorization programs and assure compliance with University policies, standards, guidelines, baselines and procedures.

The University Internal Auditor shall conduct a bi-annual review of data security practices across the University. All data custodians shall provide the required support for this bi-annual review.

Also to provide basic assurance that University data is protected, various steps must be taken as stated below:

Implement¹ credible and reputable anti-virus software on the systems. Perform continuous and/or scheduled scanning, and keep anti-virus software up-to-date. An anti-virus program will protect a computer from malicious programs. (User and SA)

Implement anti-spyware software to protect private information on the system. Spyware is a class of software designed to steal personal information.(User and SA)

Enable the built-in firewall that is included in all major operating systems, and/or install a third-party firewall application. A firewall application helps restrict others from connecting to a computer. (User and SA)

Check regularly for vendor security updates and apply them. When possible turn on automatic updates. Periodically, security vulnerabilities in the operating system and/or application are discovered and software vendors typically will then provide security updates to remediate such security exposures. (Users and SA)

Use strong passwords for all devices in compliance with University password policies. A password is used to provide authentication to an application and/or system. (User and SA)

Log-out from a website session once the online transaction is completed. Also log out from desktops, laptops and other applicable devices when not at a desk or using the device. Where applicable, utilize a password protected screen saver on all devices when they are temporarily not in use. (User and SA)

Keep machines, especially laptops and portable devices, physically secured. (User and SA)

Safeguard all confidential and sensitive data and or information. Take appropriate measures; including disk encryption for electronic data or information, physically secure physical media to prevent unauthorized disclosure. (User and SA)

Know what data is on a computer at all time and remove unwanted data from computing devices, including smart phones, as soon as it is no longer needed on that device. Use data identifying tool to scan computing devices, periodically, for unnecessary data on computers.

Scan all email attachments, using anti-virus software, before opening them. Email is a method that spreads malicious programs via email attachments. (User)

¹ The following are actions that specific category of persons will have responsibilities for. User is any user of technology regardless of status. SA is System Administrator e.g. database administrator or network engineer who has technical responsibility for a common use system. The identified persons (User, SA or User and SA) will have responsibility for taking the stated action.

Refrain from using the “save password” feature in applications, to avoid inadvertent data disclosure to others who may have physical access to the computer or device.(User)

Disable accounts, which are no longer in use and always change default passwords. Some Operating Systems and applications come with predefined user accounts. These accounts could be active by default. (SA)

Disable services that are not needed. Operating systems are packaged with services that are used by specific applications, such as ftp (for file transfer) or SMTP (for email). (SA)

Backup data and files regularly. Computers are like any machinery and can fail. This may result in data and files loss or corruption. (User and SA)

Be aware of and alert to information stealing methods such as: social engineering, phishing scams, and shoulder surfing to obtain personal and sensitive information. (User).

Notify the University Office of Information Security as soon as you discover the loss of a computer or related system or devices, and/or as soon as a suspected potential data breach as a result of unauthorized access to a data or computer system. (User and SA)

Sanitize computers before donating or disposing. (User and SA)

PHYSICAL SECURITY

Security perimeters (barriers such as walls, card controlled entry gates/doors or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

All data centers and all computer systems shall be protected against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster as reasonably as possible.

Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Equipment shall be correctly maintained to ensure its continued availability and integrity.

Hosted system security shall be reviewed to ensure compliance with University security policy.

Items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Additional guidelines may be provided in a physical security standards and guidelines document.

USER ACCEPTABLE USE

Users shall demonstrate responsibility in the use of the Morgan State University information system and network (MSUISN) and protect the devices and resources in their care, including desktop computers, laptop/palmtop computers, personal digital assistant (PDA), servers, mainframe, network equipment and all other computing accessories including software, storage devices, printing devices etc.

Users with access to data in any part of the network shall not use such data for any purpose other than that for which they have been given expressed access. Personnel shall maintain a responsible password procedure to safeguard the resources at their disposal, as well as the privacy of others on the network.

Users with privileged access shall not misuse such access by unlawful or un-permitted disclosure, outside the discharge of their regular duties. Unlawful disclosure amounts to violation of the State of Maryland Privacy Act of 2000 and the Federal Privacy Act of 1974.

Users shall not do anything that will or could hurt the reputation of the University by wrongful disclosure of information or data on the MSUISN, dissemination of harmful software from the MSUISN, unauthorized monitoring of the traffic on MSUISN, and unauthorized access to resources on MSUISN, and/or illegal transfer of media files/content and software.

Individuals using the MSUISN shall adhere to the following standards of conduct:

Users shall only access information and/or data on a need-to-know basis for the discharge of their duty.

Users shall not do anything by omission or commission to compromise the integrity of information and/or data they are charged with.

Users shall not use information obtained in the discharge of their duty for any profit purpose.

Users with privileged access shall not misuse such access by unauthorized disclosure or aggregation.

No user shall disclose password or access information over the phone

No User shall attach an unauthorized device to any network terminal on the MSUISN

No User shall engage in unauthorized monitoring of traffic on the MSUISN

No User shall intentionally transmit malicious software codes on, to, or from the MSUISN

Users shall change their password every 90 days or more frequently.

Users shall ensure that the devices under their control are running the current software update/patches supplied by the software vendor at any given time.

All Users shall ensure that their computers run the latest version of the University issued anti-virus software or some other industry recognized and/or certified antivirus software.

No User shall have an un-protected guest account on any computer under their jurisdiction.

No User shall use the MSUISN as a gateway for the transmission of unsolicited emails for commercial or non-commercial purpose(s)

No User shall obtain (by any means) or transfer illegal copies of copyright materials from, to, or within the MSUISN at any time.

An access log shall be maintained for all administrative systems to monitor access and the logs shall be reviewed periodically to verify access and access permissions.

All Information Technology personnel charged with management and protection of information and information flow at Morgan State University shall abide by the highest professional standards and ethics:

- Restrict possible conflict of interest where it exists
- Access to information and resources on a need to know basis
- No use of information gathered/obtained for any purpose other than that for which authority has been obtained.
- Protection of the privacy of MSUISN users
- Adherence to the principle of freedom of speech, expression, and access except where it conflicts with MSUISN security objectives or a state or federal regulation.

An Administrator's user account shall be disabled as soon as possible (typically within 2 working days), after the administrator loses his/her administrative rights or privileges, by virtue of transfer, termination or resignation.

Personnel shall not connect unauthorized device(s) to the MSUISN at any time.

Personal Computers, Servers and Other Network Attached Systems

Network attached computer system are required to have current host antivirus running.

Network attached computer systems are required to have current critical updates within 72 hours of release by vendors, unless where it is not operationally feasible.

Network attached computers are required to be connected by duly authenticated and authorized user.

Responsibilities

End Users are responsible for keeping their computers/devices up to date.

Administrators are responsible for keeping public computers and servers up to date.

The University may implement technologies to enforce compliance, and non-compliant devices may be denied access.

Wireless Access

The University provides wireless access at various locations within the University network to improve connectivity and productivity across the network.

Requirements for Wireless Access are similar to requirements for wired access.

The University reserves the right to monitor, record, restrict and/or deny access to wireless access users.

Only University installed and wireless access points are approved for connecting to the University Network.

FIREWALL

The University shall implement firewall or related systems at different locations within its network and on different computer systems as necessary to identify, detect, block and/or mitigate, as appropriate, exploitation of known and unknown vulnerabilities in network services and/or systems.

The University shall implement best practices in the management of its firewall systems including:

Maintain a regular update of firewall configuration and software to reflect current best practices and guidance from leading organizations.

Document firewall configurations, procedures, practices and changes.

Maintain strong password policy for the firewall system access that is at least comparable to the password policy described in this text.

Maintain separation of duties to the extent possible.

To assist with housekeeping, firewall change or exception request documentation could depend on the following template.

PASSWORDS

Access to many University provided information systems and technology services campus wide, require the use of a password, pin or paraphrase. Proper management of passwords and other authentication tokens will help reduce exposure to certain cyber attacks. The University, thus require that:

Strong Passwords be used for all technology services where required. A strong password will typically have multiple characters, including different types of characters and will be difficult to guess.

Passwords shall not be the same as a user id or other personal identifiers

Passwords shall not be displayed on screen by any application. This will prevent others from seeing your password while you type them in.

Where possible, passwords must be a minimum of 8 mixed characters. Examples of mixed characters include alpha-numeric characters, mixture of small and capital letters, or mixture of alpha-numeric characters and special keyboard characters such as @.

Passwords must not contain either leading or trailing blanks and no more than two consecutive identical characters. This will increase the password strength and make it more difficult to guess by hackers.

Password reuse frequency must be at least ten and with minimum age of two days for general users, five days for administrative users. User should not change their passwords before two days, except a breach is suspected. Users should not re-use the same password after it expires.

For reset or redistribution, user validation must be at least as strong as when account was originally established. When a user requests password reset or that password be sent, the support personal must verify that the user is indeed who they claim they are.

Passwords should be changed every 90 days for all users. It is desirable that system administrators change their passwords more frequently.

Passwords shall not be disclosed over the phone to anyone regardless of the condition.

No two persons shall share any given password.

No generic password (same password for multiple users) shall be created under any condition or circumstance.

All password changes shall be properly logged and regularly audited.

Compromised Password(s) shall be reported to a supervisor or help desk as soon as compromise is noted. Password compromise include sharing it anyone, or suspicion that someone else has gained access to the password.

Compromised Password(s) shall be changed as soon as compromise is noticed or observed.

Administrative Users shall not use the same password for *root or Administrative Account*, as is used for normal user accounts.

PERSONAL COMPUTERS

This section affects all personal productivity systems including desktop , laptop, notebook, tablet pc, or related devices of all operating systems (Windows, Linux, Mac), pda, blackberry or any other device connected to the University Network either locally or remotely.

Antivirus:

All machines shall have some antivirus software installed

Installed antivirus software shall be active every time the machine is connected to the University network.

Automatic Virus Scan Schedule shall be turned on and Automated Scan must be enabled for at least every week.

Updated Version of Antivirus Software, including up-to-date patches shall be installed.

Antivirus Software shall support automatic signature updates and this feature must be enabled

Antivirus Software shall provide support for all applications on the given system.²

Patches:

All computers and or computer systems connected to any part of, through any link type, the University network are required to have installed and activated all vendor provided, required and tested software patch with security implications.

Patches are required to have been installed within 48 hours of availability for all windows based computers.

Patches are required to have been installed within one week for all other operating systems and platforms.

Exceptions may be granted for critical server computers only when an appropriate waiver request is approved by the University CISO.

All waivers must be rectified and systems brought into compliance within 30 days of patch availability.

Where possible, automated patch management solutions shall be preferred.

² The University provides free antivirus for resident students and for all University computers.

PRIVACY

The University may collect, process, and store data or information passing through the University network or stored on a University computer system in the course of regular business operations. This information may be used for system or network diagnosis or for infrastructure planning purposes and basic institutional research.

Information so gathered may also be available to law enforcement agencies with proper legal authorization.

Researchers and others collecting or in contact with personally identifying information, personal health information or other personal information covered by appropriate sections of pertinent laws, regulations and standards will follow the recommendations outlined in those laws or standards or the direction of this document, whichever provides most protection for subjects.

For all other use or purpose, a concise privacy statement shall be provided as part of the data/information request process, a copy of which shall be available on the University Information Security website.

All privacy concerns or requests for clarification can should be sent to the University privacy desk at privacy@morgan.edu

OVERSIGHT COMMITTEE

The Information Security and Architecture Committee (SAC) shall oversee this policy and be responsible for the following:

Regular review of document for effectiveness and currency

Committee Membership

1. University Chief Information Security Officer (CISO)
2. University Internal Auditor
3. University Chief of Police
4. University Counsel
5. Director of Human Resources
6. Director of Office of Residence Life
7. Faculty members (At least two at any one time)
8. Students (At least two at any one time)

CURRENT SECURITY & ARCHITECTURAL COMMITTEE (SAC)

Member	Role & Title
Dr. Wole Akpose	Chief Technology Officer
Mr. Gilbert Goetz	Internal Auditor
Mr. Adrian Wiggins	Director, Public Safety
Ms. Julie Goodwin (Mr. Bryan Perry)	University Counsel
Ms. Armada Grant	Director, Human Resources
Ms. Kim McCalla	Directory, Design & Construction (A.V.P)
Mr. Seymour Chambers	Judiciary Officer
Mr. Doug Gwynn	Director Residence Life
Dr. Monsoureh Jeihani	Faculty Member (Assistant Professor)
Ms. Natasha Otto	Faculty Member (Lecturer)
Ms. Nicassia Williams	Faculty Member (Lecturer)
Mr. Arceonal Moore *	Undergraduate Student
Ms. Kerubo Orwenyo *	Graduate Student
Mr. Kelechi Oparadike	Graduate Student / Student worker

JANUARY 2010

LAWS, REGULATIONS, STANDARDS

Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), United States Federal Law, Dec 2009; www.ed.gov

Communications Assistance for Law Enforcement Act (CALEA) (47 U.S.C. § 1001, § 1002); United States Federal Law, Aug 2005 ; www.fcc.gov

Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347; United States Federal Law; www.nist.gov

Fair Credit Reporting Act of 1970 as amended in June 2008; United States Federal Law; www.ftc.gov

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; 16 C.F.R. Part 681.2; United States Federal Law; www.ftc.gov

Health Insurance Portability and Accountability Act (HIPAA) ; United States Federal Law; www.hhs.gov

Purchasing Card Industry Data Security Standard (PCI-DSS) ; version 1.2, Oct 2008; Purchasing Card Industry Standard; www.pcisecuritystandards.org

information technology – security techniques; International Standard Organization (ISO) / International Electrotechnical Commission (IEC) Standard; ISO/IEC 27001:2005 ; www.iso.org

National Institute of Standards and Technology Special Publication Series (NIST SP-X); US Federal Government Standards; multiple documents; www.nist.gov

State of Maryland Department of Information Technology (MD DoIT) Information Security Policy and Standards; www.doit.maryland.gov

Health Information Technology Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5).

GLOSSARY OF TERMS & DEFINITIONS

3DES	Triple DES
AES	Advance Encryption Standard
CBC	Code Block Chaining
CCNA	Cisco Certified Network Associate
CERT	Computer Emergency Response Team
CISSP	Certified Information System Professional
DES	Data Encryption Standard
FDDI	Fiber Distributed Data Interface
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I.T	Information Technology
Lab	Laboratory
LAN	Local Area Network
MCP	Microsoft Certified Professional
MD5	Message Digest 5
MSU	Morgan State University
MSUISN	Morgan State University Information Network
MSUSAC	Morgan State University Security Awareness Center
NIST	National Institute of Science & Technology
PC	Personal Computer
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
POP	Point of Presence
RADIUS	Remote Access Dial In User Server
RC-5	Rivest Cipher 5
RFC	Request For Comment
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
TACACS	Terminal Access Control Access Control Server
SHA-1	Secure Hash Algorithm 1 (80 bit version)
SHA-256	Secure Hash Algorithm 256 (256 bit version)
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
VLAN	Virtual LAN
V.P	Vice President
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wireless Encryption Protocol
Wi-fi	Wireless Fidelity
WPA	Wifi Protected Access

intentionally left blank