PG-55 Update

TITLE: PG-55 Technology Resource Acceptable Use

ORIGINATOR(S):

Chief Information Office in the Office for Information Technology
Directory Information Security and Compliance in the Office for Information Technology

APPROVAL DATE: 02/26/1999

REVISIONS: 09/15/2005, 08/01/2006, 06/05/2008, 12/06/2018; 08/08/2019

LAST REVIEW DATE: 08/08/2019

AUDIENCE: (SELECT ALL THAT APPLY)

☒ FACULTY ☒ STAFF ☒ STUDENTS ☒ VENDORS ☒ OTHER: (SPECIFY): All Users

PURPOSE:

The purpose of this policy is to outline the acceptable use of devices, services, and technology accounts associated with delivery of technical services or processes at Morehead State University (MSU). These rules are in place to protect the faculty, staff, students and MSU. Inappropriate use exposes MSU and its users to risks including virus attacks, compromise of network systems and services. As a consumer of these devices, services, and technology accounts you have access to valuable University resources, sensitive data, and internal networks. Consequently, it is imperative to maintain security with respect to MSU devices, services, and technology accounts for the protection of the university and its users.

SCOPE:

This policy applies to the use of information, devices, services, and technology accounts to conduct Morehead State University (MSU) business or interact with associated networks and business systems, whether owned or leased by MSU, the employee, or a third party. All faculty, staff, students, contractors, consultants, temporary, and other workers at MSU and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, devices, services, and technology accounts in accordance with MSU policies and standards, and local laws and regulations.

This policy applies to faculty, staff, students, contractors, consultants, temporary, and other workers at MSU, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by MSU.

DESCRIPTION (INCLUDE DEFINITIONS):

The Office for Information Technology's (OIT) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Morehead State University's (MSU) culture of inclusion, integrity, trust. OIT is committed to protecting MSU's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

All systems, networked or standalone, including but not limited to computer equipment, software, operating systems, storage media, technology accounts providing electronic mail, WWW browsing, and FTP, are the property of MSU. These systems are to be used for business purposes in serving the interests of the university, and of our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every MSU employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

POLICY

Acceptable Use

- Personnel are responsible for complying with Morehead State University policies when using Morehead State University information resources and/or on Morehead State University time. If requirements or responsibilities are unclear, please seek assistance from the Office of Information Security and Compliance.
- Personnel must promptly report the theft, loss, or unauthorized disclosure of Morehead State University confidential or internal information to the Office of Information Security and Compliance.
- Personnel should not purposely engage in activity that may:
    - harass, threaten, or abuse others.
    - degrade the performance of Morehead State University Information Resources.
    - deprive authorized Morehead State University personnel access to a Morehead State University Information Resource.
    - obtain additional resources beyond those allocated.
    - or circumvent Morehead State University computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, Morehead State University personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Morehead State University Information Resource.
- Use of encryption should be managed in a manner that allows designated Morehead State University personnel to promptly access all data.
- Morehead State University Information Resources are provided to facilitate institutional business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Morehead State University Information Resources.
- Personnel should not intentionally access, create, store, or transmit material which Morehead State University may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a zero trust ("need to know") policy.

- Personnel are permitted to use only those network and host addresses issued to them by Morehead State University OIT and should not attempt to access any data or programs contained on Morehead State University systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal Morehead State University networks and/or environments must be made through approved, and Morehead State University-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information.
- Personnel must not share their Morehead State University authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (Eagle ID),
    - Security Tokens (i.e., MFA Tokens),
    - Access cards and/or keys or Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Lost or stolen access cards, security tokens, and/or keys must be reported to the person responsible for Information Resource physical facility management as soon as practical.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, implemented, and utilized according to the following Morehead State University Regulations (UAR 405).
- Security tokens (i.e., MFA Tokens, ID Cards, etc.) must be returned on demand or upon termination of the relationship with Morehead State University, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with applications that save embedded scripts or hard coded passwords in client software.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing confidential information should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access confidential information should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing confidential information should be immediately removed from printers and fax machines.

Data Security

- Personnel should use approved encrypted communication methods whenever sending confidential information over public computer networks (Internet).
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information. Please contact OIT for guidance or assistance.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- Confidential information must be transported either by a Morehead State University employee or a channel approved by OIT Leadership.
- All electronic media containing confidential information must be securely disposed. Please contact OIT for guidance or assistance.

Email and Electronic Communication

- Auto-forwarding electronic messages outside the Morehead State University internal systems are prohibited.
- Electronic communications should not misrepresent the originator or Morehead State University.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from Morehead State University OIT, except for calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive Morehead State University confidential information.
- Any personal use of Morehead State University provided email should not:
    - Involve solicitation.
    - Be associated with any political entity, excluding the Morehead State University sponsored PAC.
    - Have the potential to harm the reputation of Morehead State University.
    - Forward chain, spam, or phishing emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of Morehead State University confidential information.
- Personnel should only send confidential information using secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

Hardware and Software

- All University owned hardware must be formally approved by OIT Management before being connected to Morehead State University networks.
- Software installed on Morehead State University equipment must be approved by OIT Management and installed by Morehead State University OIT personnel, designee, or process.
- All Morehead State University assets taken off-site should be physically secured at all times.
- Employees should not allow family members or other non-employees to access Morehead State University Information Resources.

Internet

- The Internet must not be used to communicate Morehead State University confidential or internal information, unless the confidentiality and integrity of the information is ensured, and the identity of the recipient(s) is established.
- Use of the Internet with Morehead State University networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
    - Accessing or distributing pornographic or sexually oriented materials,
    - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
- Access to the Internet from outside the Morehead State University network using a Morehead State University owned computer must adhere to all the same policies that apply to use from within Morehead State University facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- All personally owned laptops and/or workstations must be onboarded to Morehead State University's mobile device management, anti-virus, and anti-malware solutions if they are to be utilized with Morehead State University information systems.
- Confidential data should only be stored on devices that are encrypted in compliance with the Morehead State University policy.
- Morehead State University confidential information should not be stored on any personally owned device.
- Theft or loss of any mobile device that has been used to create or access confidential or internal information must be reported to the Morehead State University Security Team immediately.
- All mobile devices must maintain up-to-date versions of all software and applications.
- All personnel are expected to use mobile devices in an ethical and secure manner.
- Jail-broken or rooted devices should not be used to connect to Morehead State University Information Resources.
- Morehead State University OIT Leadership may choose to execute "remote wipe" capabilities for mobile devices without warning.
- If there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Morehead State University Information Resources may be monitored, at the discretion of Morehead State University OIT Leadership.
- Morehead State University OIT Support for personally owned mobile devices is limited to assistance in complying with this policy. Morehead State University OIT Support may not assist in troubleshooting device usability issues.
- Use of personally owned devices must follow all other Morehead State University policies.
- Morehead State University reserves the right to revoke personally owned mobile device use privileges if personnel do not abide by the requirements set forth in this policy.

Physical Security

- Photographic, video, audio, or other recording equipment, such as cameras in mobile devices, is not allowed in secure areas.
- Personnel must possess and be prepared to always display photo ID access card while on campus.
- Personnel must badge in and out of access-controlled areas.
- Piggybacking, tailgating, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel.
- Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on Morehead State University Information Resources are not private and may be accessed by Morehead State University OIT employees at any time, under the direction of Morehead State University executive management, legal, and/or Human Resources, without knowledge of the user or resource owner.
- Morehead State University may log, review, and otherwise utilize any information stored on or passing through its Information Resource systems.
- Morehead State University OIT Systems Administrators, and other authorized Morehead State University personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

Removable Media

- The use of removable media for storage of Morehead State University information must be supported by a reasonable business case.
- Confidential and internal Morehead State University information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained Morehead State University information must be reported to the Morehead State University OIT.

Security Training and Awareness

- All new personnel must complete an approved security awareness training course as part of the onboarding process managed by Human Resources. If this training is not completed, access to systems may be suspended until the training is completed.
- All personnel must complete periodic security awareness training as required.

Voicemail

- Personnel should use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- Personnel should not access another user's voicemail account unless it has been explicitly authorized.

Incidental Use

- As a convenience to Morehead State University personnel, incidental use of Information Resources is permitted. The following restrictions apply:
    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to Morehead State University approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to Morehead State University.
    - Incidental use should not interfere with the normal performance of an employee's work duties.
    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Morehead State University or its customers.
- Storage of personal email messages, voice messages, files, and documents within Morehead State University Information Resources must be nominal.
- All information located on Morehead State University Information Resources are owned by Morehead State University may be subject to open records requests and may be accessed in accordance with this policy.

POLICY COMPLIANCE & ENFORCEMENT

Compliance Measurement

The Information Technology team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Information Technology team in advance.

Enforcement

As the use of MSU IT resources is a privilege and not a right, a User's access to MSU IT resources may be limited, suspended, or terminated if that User violates this Policy or University regulations. Users who violate this Policy, University regulations, and/or laws governing technology may be subject to disciplinary action and/or other penalties. Disciplinary action shall be handled through the University's established student and employee disciplinary procedures. Guests and other Users may have access to MSU IT resources suspended or revoked.

The Chief Information Officer may temporarily suspend or deny a User's access to MSU IT resources when he/she determines that such action is necessary to protect such resources, the University, or other Users from harm. In such cases, the Chief Information Officer will promptly inform other University administrative offices, as appropriate, of that action. Employee violations will be reported to appropriate supervisors and Vice Presidents, while student violations will be reported to the Dean of Students. In addition to an administrative review of violations, the University may report potential violations of MSU IT resources to law enforcement agencies.

APPROVED BY:

VICE PRESIDENT: _____ DATE: _____

APPROPRIATE INSTITUTIONAL REVIEW: _____ DATE: _____

PRESIDENT: _____ DATE: _____

UAR NUMBER: 400.032

TITLE: Network Access Policy, Information Technology ~~Wireless Network Policy and Procedure~~

ORIGINATOR(S): Chief Information Officer in the Office for Information Technology

INITIAL ADOPTION: 11/06/2003

REVISION DATE(S): 07/09/2018, 01/17/2024

AUDIENCE: (SELECT ALL THAT APPLY)

~~)~~
~~✓ FACULTY ✓ STAFF ✓ STUDENTS ✓ VENDORS ✓ OTHER (SPECIFY):~~

☒ FACULTY ☒ STAFF ☒ STUDENTS ☒ VENDORS ☒ OTHER: (Visitors): ~~Visitors~~

PURPOSE:

Morehead State University invests significant resources in maintaining a secure, robust enterprise network that meets the academic, research, residential, and administrative requirements of the institution. The University must comply with applicable Federal, State, and local laws and regulations, as well as protect the campus network resources thus certain utilization, security, performance, and reliability requirements must govern the operation of these networks.~~Set forth the policy for using wireless data technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless data radio spectrum at Morehead State University (MSU). The document describes how wireless technologies are to be deployed, administered and supported at MSU.~~

SCOPE:

This ~~policy~~ regulation applies to all Morehead State University (MSU) faculty, staff, students, visitors, and contractors. The ~~policy~~ regulation applies to these persons participating in or supporting any activity in any academic and operational buildings, residence halls, and offices at all University locations, owned and leased that have access to the enterprise network.

DESCRIPTION (INCLUDE DEFINITIONS):

This ~~policy~~ regulation governs the installation, operation, and maintenance of the enterprise network~~all wireless network devices utilizing MSU Internet Protocol (IP) network space, including private IP space within University networks, and all users of such devices, and governs all wireless connections to the campus network, frequency allocation, network assignment, and registration~~. This regulation also applies to all Morehead State University (MSU) faculty, staff, students, visitors, and contractors and their devices that are attached to the enterprise network or are utilizing Morehead State University owned and operated network space, including private RFC 1918 IP (Internet Protocol) space using virtual private networking. ~~services provided over wireless connections to the campus network for colleges, departments, or divisions of the University.~~

~~The University~~MSU provides and maintains computing and telecommunications resources to support the teaching, research, and administration activities of its faculty, staff, and students. A secure and reliable data network is a critical component of the University's infrastructure. While wireless networking devices can be useful tools for enhancing productivity and convenience, they can also negatively impact the availability and security of the University network if improperly connected or administered.

DEFINITIONS:

Enterprise (or University) Network: The enterprise (or university) network is comprised of the network hardware, cable plant infrastructure and the services to support them, from the data jack or wireless access point to the University's Internet Service Provider's (ISP) connection. The university network begins at the connection to the network (wired or wireless) and ends at the service provider internet demarcation point.

Wired Network: The wired network consists of the physical cabling, infrastructure, and management systems that provide physical network access via an ethernet or fiber optic cable.

Wireless Network: The wireless network consists of the access points (connected to the wired network), wireless radio frequency spectrum, wireless controllers and management systems that provide services via the MSU provided wireless networks~~local area network technology other than wired technology, including, but not limited to, technology that uses radio frequency spectrum, to connect computing devices to college, department, and division wired networks~~.

Access Point: electronic hardware that serves as a common connection point for devices in a wireless network.

~~**Wireless Infrastructure:** wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.~~

Interference: The presence of another radio frequency signal that is operating on a frequency currently being used by the wireless network infrastructure. This additional signal, depending on the strength of the interfering signal, can cause degradation of performance to the wireless network infrastructure.~~the degradation of a wireless communication signal from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.~~

~~**Point of Contact (POC):** the person designated as having primary responsibility for a given wireless access point or network.~~

Virtual Private Network (VPN): A technology utilized to provide end-to-end encryption to connect to the enterprise network in a secure way when direct connectivity is not

availablethe use of encryption to provide a secure means of connection over an otherwise unsecure network.

POLICY

The enterprise (or university) network (wired & wireless) is an essential resource for Morehead State University (MSU) students, faculty, staff, vendors, and guests. The enterprise network provides mission critical services required to meet the academic, administrative, research and residential needs of MSU. Due to the complex nature and scale of the enterprise network, the Office of Information Technology (OIT) must be solely responsible for the overall design, installation, coordination, and operation of the University's network environment.

Network Acceptable Use

- All devices attached to the enterprise network and their associated users must follow PG-55 "Technology Resource Acceptable Use".
- Abuse or interference with other activities is a violation of acceptable use. Interference or disruption of other authorized communications or unauthorized interception of other traffic is a violation of policy.

Information Security and Compliance

General access to network infrastructure, wired or wireless, is limited to individuals authorized to use campus and network resources. Guests and vendors, unless specific use cases are approved by OIT Information Security and Compliance, will be limited to internet access only and will have no access to campus resources beyond the required systems for core connectivity (aka, DNS, DHCP, Time Services, etc.)

- Physical security of the network is maintained to protect the network from theft or unauthorized access to the data port or network devices.
- User authentication and authorization are required for access to secured campus networks or Internet services. The local, wide-area and Wireless networks shall support modern enterprise-grade authentication and authorization protocols so users can securely access the appropriate campus network.
- Networks will be segmented where possible to promote good cyber security practices, prevent unauthorized access, and to promote a zero-trust user access model where applicable.
- Firewalls are an important part of network security. Firewalls also serve as enforcement points to reduce or eliminate network policy violations and malicious activities. If your application requires specialized firewall rules, they must be officially requested and approved by Information Security and Compliance prior to being installed in the appropriate firewall or network segment.

RESPONSIBILITY:
Wireless equipment and users must follow all acceptable use provisions stated in PG-55 "Technology Resource Acceptable Use" in addition to the more specific requirements described in this document. Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks. Responsibility for electronic communication resources at Morehead State University resides with the Office of Information Technology.

Deployment by Students
Students are not permitted to connect wireless access points to the campus network unless they are working under the direction of the Office of Information Technology. Wireless access points may not be connected to the student residential network.

Public Access Points
Responsibility for deploying wireless access points that are intended for use by the general University community resides with the Office of Information Technology.

~~**APPROVED BY:**~~

~~VICE PRESIDENT: _____ DATE: _____~~

~~APPROPRIATE INSTITUTIONAL REVIEW: _____ DATE: _____~~

~~PRESIDENT: _____ DATE: _____~~

Wired Networks

- The wiring and electronic components of the network are deemed part of the basic infrastructure and utility services of MSU. Installation and maintenance of that network are to be considered part of the "up front" basic required building and renovation costs and are not considered discretionary options in construction and renovation design.
- Standards for the network wiring, electrical components, and their enclosures are defined by the Office for Information Technology (OIT) and are subject to local, regional, state, and federal regulations. These standards will be considered part of the University's "building code" to which installations must conform.
- Units that would like to use their own funding to install wired technology or change the programmatic function or use of a room to include wired network access must work directly with OIT Network Engineering for design services, adherence to current network standards and implementation.
- Units are restricted from establishing their own security using local firewalls and/or VPNs (virtual private networks). OIT Network Engineering and Information Security should be consulted if the current access to/through unit required devices is currently not possible or there is a change in Unit business practices. OIT Network Engineering must maintain the ability to see beyond the secure points of the network for diagnosing cyber threat and other problems potentially affecting the overall network.
- Units are restricted from adding devices or servers to the network that duplicate or provide network services like DHCP, DNS or Time. Any network service that is not already provided by OIT that needs to be delivered shall be established with the assistance of OIT and will have to obtain an exemption from the Chief Information Officer.

Wireless Networks

- Wireless Network (Wi-Fi or 802.11x protocols) utilize public unlicensed radio frequencies. These services can be severely impacted by unwanted interference. For this reason, Wi-Fi networks are subject to additional rules concerning interference and shared use.
    - OIT will ensure that wireless infrastructure meets all applicable rules of regulatory agencies, such as, the Federal Communications Commission and Public Utilities Commission.
    - Wireless infrastructure must be designed and installed to minimize RF (Radio Frequency) interference without impacting performance.
- Units that would like to use their own funding to install wireless technology or change the programmatic function or use of a room to include wireless network access point must work directly with OIT Network Engineering for design services, adherence to current network standards and implementation. Wireless performance is impacted by the architectural features, building materials, and furnishings of a contemporary workspace. Construction and renovation projects must be coordinated with OIT and include funding for additions or adjustments required to optimize performance and serviceability of impacted wireless access points and systems.
- Any devices, either not part of or that cause significant RF interference with the University wireless network will be considered a "rogue" access point or device. OIT will pursue all reasonable efforts to contact the owner of the rogue device, and if necessary, may disable or disconnect them from the University network. This includes devices and equipment that operate in the frequency ranges

occupied by the University Wi-Fi network.
- Guest networks will utilize portal-based access and require guests and vendors to provide a reliable method for identification before obtaining credentials to utilize the guest network.

Network Reliability and Interference

In an enterprise network environment, network reliability is a function of proper design which accommodates the level of user congestion (traffic loads) and service availability (interference and coverage). To provide an acceptable level of reliability, this policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum. ~~In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). In an effort to provide an acceptable level of reliability, this policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum.~~

Wireless networking technology uses unlicensed frequency bands to create small local area network cells. Since unrelated devices such as cordless telephones, wireless audio speakers, and even microwave ovens may also use these same frequency bands, the potential for disruption of service exists when multiple devices are placed in close proximity to one another.

While OIT does not actively monitor use of the frequency spectrum for potential interfering devices, it responds to reports of specific devices that are suspected of causing interference and disruption of the campus network. Where interference between the campus network and other devices cannot be resolved, OIT reserves the right to restrict the use of all wireless devices in university-owned buildings and all outdoor spaces.

Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited. ~~In the event that a wireless device interferes with other equipment, OIT will work with the affected departments to resolve the interference.~~

- If a wireless device interferes with other equipment, the OIT or designee shall resolve the interference as determined by use priority.
- If other equipment interferes with a wireless device, the OIT or designee shall resolve the interference as determined by use priority.
- The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list: instruction, administration, research, and public access.
- Any unapproved or rogue access points found connected to the network will be disabled.
- New plans for buildings and gathering areas must consider the need for and use of wireless networking.

Monitoring of Network

OIT is responsible for monitoring all network devices associated with the enterprise network. This includes servers and applications that are required for proper operation of the network. This monitoring will be done with multiple protocols and all equipment must support the current protocols in use:

- ICMP
- SNMP Version 3 (Fall back to Version 2 if not available)

- CLI Access
- Windows WMI Access
- Secure Shell (SSH)
- Agent Based Monitoring
- API or REST

Responsibility

The Office of Information Technology (OIT) will be ~~is~~ responsible for the following:

- Maintain all backups and archives associated with the network devices and maintain the previous 10 revisions where available.
- Creating, maintaining and updating wireless plans, wireless policy and wireless security standards
- Maintaining a registration of all wireless access points on campus
- Resolving wireless communication interference problems
- Monitoring performance and security of all networks and maintaining network statistics as required for preventing unauthorized access to the campus network

The campus community, including Colleges, divisions and/or departments are responsible for:

- Adherence to PG-55 "Technology Resource Acceptable Use".
- Adhering to Network Access Policy (This Policy)
- Informing wireless users of security and privacy policies and procedures related to the use of wireless communications.

Enforcement

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, and the Student Code.

Any unusual network event that may reflect unauthorized use of the enterprise network should be immediately reported to OIT for review and, if appropriate, investigation. Such reportable events include the discovery of unauthorized wired switches or hubs, rogue wireless access points or other equipment transmitting or receiving on established wireless frequencies.

APPROVED BY:

VICE PRESIDENT: DATE:

APPROPRIATE INSTITUTIONAL REVIEW: DATE:

PRESIDENT: DATE:

- ~~Managing and deploying wireless communications systems~~
- ~~Approving wireless communication hardware, software and installation services used by University schools/departments~~
- ~~Informing wireless users of security and privacy policies and procedures related to the use of wireless communications in common areas~~
- ~~Providing assistance to the campus community for the development, management and deployment of wireless networks~~

- ~~Monitoring performance and security of all wireless networks and maintaining network statistics as required for preventing unauthorized access to the campus network~~

- Monitoring the development of wireless network technologies, evaluating wireless network technology enhancements and, as appropriate, incorporating new wireless network technologies within the University network infrastructure

The campus community, including Colleges, divisions and/or departments are responsible for:

- Adhering to Wireless Network Policy
- Informing wireless users of security and privacy policies and procedures related to the use of wireless communications

Security Awareness: Instructional materials will be made available to all wireless users via the University web site. The instructional material will include, but not be limited to the following topics:

- Authentication for wireless network access and protection of passwords
- Authorized use of wireless network technology
- Wireless interference issues
- Procedures for reporting wireless network service problems
- Procedures for responding to a suspected privacy or security violation
- Procedures for revoking user accounts due to termination of an affiliation with the University

Monitoring and Reporting: The use of wireless network technology is to be monitored by the OIT on a regular basis for security and performance.

Any unusual wireless network event that may reflect unauthorized use of wireless network services should be immediately reported through the OIT for review and, if appropriate, investigation. Such reportable events include the discovery of unauthorized Wireless Access Points on any MSU properties.

POLICY

Responsibility for Wireless Access Points: Campus responsibility for electronic communication resources reside with the Office of Information Technology, who must approve all installations of wireless access points used on all campus sites.

- Wireless equipment and users must follow PG-55 “Technology Resource Acceptable Use”. Wireless services are subject to the same rules and policies that govern other electronic communications services at the University.

- Abuse or interference with other activities is a violation of acceptable use. Interference or disruption of other authorized communications or unauthorized interception of other traffic is a violation of policy.
- Radio communication, due to its dependence on a scarce and shared resource, is subject to additional rules concerning interference and shared use.

1. Wireless access points must meet all applicable rules of regulatory agencies, such as, the Federal Communications Commission and Public Utilities Commission.
2. Wireless access points must be installed so as to minimize interference with other RF activities particularly as described below.

- Only hardware and software approved by the Office of Information Technology or designee shall be used for wireless access points.

Security: General access to the network infrastructure, including wireless infrastructure, is limited to individuals authorized to use campus and Internet resources.

- Physical security of wireless access points is maintained to protect the access point from theft or access to the data port.
- Access points shall enforce user authentication at the access point before granting access to secured campus or Internet services. Wireless network interfaces shall support authentication to access the secured campus wireless network.

Network Reliability and Interference

In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). In an effort to provide an acceptable level of reliability, this policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum.

Wireless networking technology uses unlicensed frequency bands to create small local area network cells. Since unrelated devices such as cordless telephones, wireless audio speakers, and even microwave ovens may also use these same frequency bands, the potential for disruption of service exists when multiple devices are placed in close proximity to one another.

While OIT does not actively monitor use of the frequency spectrum for potential interfering devices, it responds to reports of specific devices that are suspected of causing interference and disruption of the campus network. Where interference between the campus network and other devices cannot be resolved, OIT reserves the right to restrict the use of all wireless devices in University-owned buildings and all outdoor spaces.

~~Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited.~~

- ~~In the event that a wireless device interferes with other equipment, the OIT or designee shall resolve the interference as determined by use priority.~~
- ~~If other equipment interferes with a wireless device, the OIT or designee shall resolve the interference as determined by use priority.~~
- ~~The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list: instruction, administration, research, and public access.~~
- ~~Any unapproved or rogue access points found connected to the network will be disabled.~~
- ~~New plans for buildings and gathering areas must consider the need for and use of wireless networking.~~

UAR NUMBER: 404.03

TITLE: Technology Account Policies and Procedures

ORIGINATOR(S): Chief Information Officer in the Office for Information Technology

INITIAL ADOPTION: 07/09/2018
REVISED: 02/01/2020, 8/1/2022
AUDIENCE: (SELECT ALL THAT APPLY)

☒ FACULTY ☒ STAFF ☒ STUDENTS ☒ VENDORS ☒ OTHER: (SPECIFY): All Users

PURPOSE:
To establish acceptable guidelines for technology accounts maintained by the Office of Information Technology and Morehead State University (MSU). To establish and ensure adherence to best practice technology security policies and procedures for account lifecycle management~~technology account lifecycle management~~.

~~MSU technology accounts are created to support the educational, instructional, research, and administrative activities of the University. The use of these accounts and their associated resources is a privilege that is extended to members of the MSU community. As a consumer of these services, you have access to valuable University resources, sensitive data, and internal networks. Consequently, it is imperative to maintain security with respect to MSU technology accounts for the protection of the university and its users.~~

SCOPE:
This document covers all user accounts maintained by the Office of Information Technology and MSU. Individuals covered by the policy include (but are not limited to) MSU faculty, visiting faculty, staff, students, alumni, guests or agents of the administration, affiliates, external individuals, members of the Board of Regents, and organizations accessing accounts maintained by MSU. The following statements will function as MSU's official guidelines for technology account management using the University's technology systems. All technology accounts are also subject to the PG-55 Technology Resource Acceptable Use policy and may be restricted based on those guidelines.

~~**RESPONSIBILITY:**~~

~~The Office of Information Technology is responsible for the administration of all electronic accounts and systems owned or leased by the University.~~

~~**ACCOUNT POLICY PROCEDURES:**~~

~~**Affiliate** – Access removed on termination date.~~
~~**Compromised Account-Access** removed upon detection of unauthorized access.~~
~~**Emeriti Faculty-Access** provided indefinitely.~~
~~**Employee (Involuntarily Termination)** – Access removed upon notification to OIT staff.~~
~~**Faculty** – Access removed 180 days after termination date.~~
~~**Staff** – Access removed 60 days after termination date.~~
~~**Student** – Access removed after three consecutive non-enrolled semesters.~~

~~Technology accounts included in multiple groups will follow the least restrictive (longest) access timeline.~~

~~**DESCRIPTION (INCLUDE DEFINITIONS):**~~

~~MSU technology accounts are created to support the educational, instructional, research, and administrative activities of the University. The use of these accounts and their associated resources is a privilege that is extended to members of the MSU community. As a consumer of these services, you have access to valuable University resources, sensitive data, and internal networks. Consequently, it is imperative to maintain security with respect to MSU technology accounts for the protection of the university and its users.~~

~~This policy identifies a lifecycle for each type of technology account created for MSU users. Each lifecycle has different organizational requirements for access and are deprovisioned or suspended after a given period associated with the corresponding lifecycle requirements.~~

DESCRIPTION (INCLUDE DEFINITIONS):

MSU technology accounts are created to support the educational, instructional, research, and administrative activities of the University. The use of these accounts and their associated resources is a privilege that is extended to members of the MSU community. As a consumer of these services, you have access to valuable University resources, sensitive data, and internal networks. Consequently, it is imperative to maintain security with respect to MSU technology accounts for the protection of the university and its users.

This policy identifies a lifecycle for each type of technology account created for MSU users. Each lifecycle has different organizational requirements for access and are deprovisioned or suspended after a given period associated with the corresponding lifecycle requirements.

~~**DEFINITION OF TERMS**~~

~~**DEFINITIONS**~~

DEFINITIONS

Access Removed: Inability to authenticate and/or login to MSU technology resources.

Account Management System: Computer system used to verify and authenticate login credentials.

Affiliates: Users who have a contractual affiliation with MSU but are not employees.

Compromised Account: Any account where access has been gained via nefarious means (ex. phishing, hacking, etc.).

Emeriti Faculty: Retired Faculty recognized by MSU Board of Regents for meritorious service.

Employee: All faculty and staff.

Information Systems: Any Morehead State University owned, leased, contracted, subscribed or managed system that is used in any capacity for Morehead State University.

Involuntary Termination: Unplanned or involuntary termination of an employee.

Least Privileged or Zero Trust: Privileged access users must have permissions set to the lowest level of access needed to accomplish their job function.

Privileged Access (Elevated Access): Access that allows an individual who can take actions which may affect computing systems, network communication, or the accounts, files, data or processes of other users. Privileged access is typically granted to system administrators, network administrators or other such employees whose job duties require access to sensitive data residing on a system or network. This data can be paper or electronic data. For the purposes of this policy, application and other developers are also considered privileged.

Students: All applicants, dual-credit, undergraduate and graduate students.

Termination Date: Employment end date per the University's system of record.

POLICY

Policy Statement

Provide a comprehensive technology account management process that allows authorized individuals access to Information Systems as well as University Data.

Information Security and Compliance

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Morehead State University Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. The protection of *Confidentiality*, *Integrity*, and *Availability* are basic principles of information security, and can be defined as:

> **Confidentiality:** Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the “Principle of Least Privilege”.
>
> **Integrity:** Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
>
> **Availability:** Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Morehead State University maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures, and guidelines that:

- Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical, and technical controls.
- Provide value to the way we conduct business and support institutional objectives.
    - Comply with all regulatory and legal requirements, including but not limited to:
    - HIPAA Security Rule,
    - State breach notification laws,
    - PCI Data Security Standard,
    - Information Security best practices, including ISO 27002 and NIST CSF,

- Contractual agreements,
- All other applicable federal and state laws or regulations.

The information security program is reviewed no less than annually or upon significant changes to the information security environment.

Account Types

Standard User Accounts

Non-privileged accounts are assigned to individual accounts and will have unique usernames and passwords that comply with the university's Password Policy. The standard, non-privileged accounts are to be used for daily functions such as, but not limited to, office productivity software such as Office 365, email or internet browsing. This requirement limits exposure when operating from within privileged accounts or roles. These accounts should never be used for privileged or specialized account functions such as system administration.

Privileged or Specialized User Accounts

Privileged or Specialized User Accounts must be created by OIT and approved by Information Security and Compliance. These individually assigned accounts will conform to departmental naming conventions as spelled out in OIT departmental standards documentation. The passwords must comply with the university's Password Policy. These accounts will not be email enabled accounts, thus reducing the risk of compromise. If there is a business need for shared credentials, an approved password storage system must be used. Access to the password storage system must be controlled by the university's approved multi-factor authentication.

Information Security and Compliance will conduct an annual review of all privileged access.

The Principal of Least Privilege must be followed for all privileged and specialized accounts. The users should only have access to, and knowledge of, the data needed to do their job function.

Separation of Duties

It is the responsibility of each business unit to utilize a Separation of Duties and Rotation of Duties plan. Separation of duties is achieved by separating roles and responsibilities for a high-risk business process across multiple people. Rotation of Duties is achieved by rotating tasks periodically, so it becomes more difficult for users to collude together to engage in fraudulent behavior. These steps reduce risk to systems and university data, especially in situations where credentials become compromised.

Privileged or specialized account users' desktop or laptop computers will be university owned and must be managed by centralized university-controlled endpoint technologies. When utilizing privileged access to university systems, users must, when technically feasible, connect via the university's physical network or use the university's VPN. The VPN will be accessed using a non-privileged account as part of a separation of duties practice that prevents a compromised VPN account from obtaining elevated privileges once a VPN connection is established with the compromised credentials. Privileged access users must also use multi-factor authentication where technically feasible.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with all relevant laws, policies and regulations. In all

cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation. This would include any need to impersonate a user's role as part of an investigation or troubleshooting process.

Privileged access users shall take necessary precautions to protect the confidentiality and integrity of information encountered in the performance of their duties. If, during the performance of their duties, users observe strange activity or evidence indicating misuse, they must immediately notify their supervisor and OIT ITSC at 606-783-4357 (HELP).

Payment Card Industry (PCI) Accounts

Users responsible for processing payments in MSU financial systems, such as Colleague or the current payment provider, must adhere to the Payment Card Industry's (PCI) Data Security Standard for password expiration where it has been deemed relevant. These individually assigned accounts will conform to departmental naming conventions as spelled out in OIT departmental standards documentation. The passwords must comply with the university's Password Policy.

Service Accounts and Test Accounts

Service accounts are accounts used by a system, task, process, or integration for a specific purpose. Test accounts are accounts used on a temporary basis to imitate a role, person, or training session. These accounts will not be used for production purposes. These individually assigned accounts will conform to departmental naming conventions as spelled out in OIT departmental standards documentation. The passwords must comply with the university's Password Policy.

Account Access and Logging

Appropriate logs must be maintained in a centralized system where integrity and access can be controlled and monitored. Any additional logs must be made available to the Office of Information Security and Compliance within the Office for Information Technology (OIT) for review when requested. Logs shall be reviewed on a regular basis for malicious activity as required by university standards or regulatory compliance.

Technology Account Policy Terms

Technology accounts will be created, assigned, and maintained through the account's lifecycle as designated by the account type. These technology accounts could be categorized using multiple types and if so, the assigned technology account will follow the least restrictive (longest) access timeline for all associated types. In general, access to Information Systems via an assigned technology account is associated with the following user types (See Table 1 – Account Types):

Account Type (Office License)	Use Case	Access Removed	Individual Data Retention*
Standard User Accounts			
Affiliate (A1)	MSU Affiliate Eagle Card Issued for non-employees doing MSU Business.	Access removed on termination date.	Individual data retained for at most 30 days from date access is removed.
Compromised Account (All)	Account where access has been gained via nefarious means.	Access removed upon detection of unauthorized access.	Individual data retained during event. Account must be brought back

			into good standing.
Emeriti Faculty (A5)	Retired Faculty recognized by MSU Board of Regents for meritorious service.	Access provided indefinitely. *Account terminated if no activity occurs within a rolling 12-month period.*	Individual data retained for at most 30 days from date access is removed.
Employee (A5) - (Involuntarily Termination)	Unplanned or involuntary termination of an employee.	Access removed upon notification to OIT staff.	Individual data retained for at most 30 days from date access is removed.
Faculty (A5)	Currently Employed MSU Faculty.	Access removed 180 days after termination date.	Individual data retained for at most 30 days from date access is removed.
Retired (A1**) (Faculty or Staff)	Officially Retired as Faculty or Staff	Access removed on retirement date	Individual data retained for at most 30 days from date access is removed.
Staff (A5)	Currently Employed MSU Staff.	Access removed 60 days after termination date.	Individual data retained for at most 30 days from date access is removed.
Student (A1)	Current MSU undergraduate and graduate students.	Access removed after three consecutive non-enrolled semesters.	Individual data retained for at most 30 days from date access is removed.
Other Account Types			
Privileged or Specialized User Accounts (No License issued unless it is a requirement for the technology account ex. Azure Tenant)	System Administration or access to sensitive data	Access removed on termination date.	Individual data retained for at most 30 days from date access is removed.
Payment Card Industry (PCI) Accounts	Users Accounts associated with PCI regulated workflows.	Access removed on termination date.	Individual data retained for at most 30 days from date access is removed.
Service Accounts and Test Accounts	Test and Service Accounts for administrative and testing purposes	Removed when testing is complete, or service lifecycle has ended.	Individual data retained for at most 30 days from date access is removed.
* Individual Data Retention includes services like Office365 (Outlook Email, OneDrive, SharePoint), Enterprise Shared Hard Drive, etc. * Previously some retired accounts were grandfathered into Emeritus status and retain an A1 license in perpetuity. All other Retired accounts are removed upon retirement. Account terminated if no activity occurs within a rolling 12-month period.			

Table 1 – Account Types

Technology Account Legal Hold

At legal counsel's request, any account can be put on a legal hold status. During this period, the user account is typically deactivated, and all data is put in a non-delete status where the technology implemented permits. Once the legal hold is removed from the account, normal data retention periods apply, and individual data will be removed accordingly.

Account Type Transitions

In the event of a transfer from one account type to another account type, the data retention timelines become immediate. For example, if a staff account type transfers to a retired account, then any data that is not included in the retired account type will be removed at the initial account type timeline and the data that is associated with the new account type will still be accessible.

Responsibility

Office for Information Technology (OIT) will be responsible for the following:

- Administration of all electronic technology accounts and systems owned or leased by the University.

Users of technology resources must not:

- Obtain or use another's login credentials or otherwise access technology resources to which authorization has not been expressly given. This obligation includes using another's login credentials to hide an identity or attribute the use of data or technology resources to another user.
- Copy, install, or use any software, data, files, or other technology that violates a copyright or license agreement. No user may distribute or download copies of copyrighted material without explicit permission from the copyright owner.
- Copyright law applies to materials such as games, movies, music, or software in both analog and digital format. Users shall not download an illegally distributed file to a technology resource. Copyright holders regularly notify the Morehead State University (MSU) of infringing activity using the procedures outlined in the Digital Millennium Copyright Act of 1998 (DMCA) and other legal procedures. As a service provider, the MSU must investigate complaints and remove unlawful material. The law provides for a copyright owner to obtain the identity of a subscriber. If you illegally possess or share copyrighted materials, you may be denied access to MSU's technology resources, be subject to corrective actions via the Division of Academic Affairs and Human Resources, and possibly face civil or criminal legal proceedings and sanctions.
- Utilize technology resources to create or transmit false or deceptive information, misguided alerts, or warnings, or to participate in any other fraudulent or unlawful activities.
- Monopolize or disproportionately use shared technology resources, overload systems or networks with endless loops, interfere with others' authorized use, degrade services, or otherwise misuse or misappropriate computer time, connection time, disk space, or similar resources.
- Compromise the security of any data or technology resources or attempt to circumvent any established security measures, for any reason, (e.g., using a computer program to attempt password decoding). Users must not acquire, store, or transmit any hardware or software tools designed to compromise the security of technology resources without express written authorization by the Office of Information Technology (OIT).
- Send unsolicited mass mailings or "spamming." Mass mailings must only be sent to clearly identified groups for official purposes and may not be sent without proper authorization and coordination with MSU Marketing and Public Relations.
- Install, store, or download software to MSU technology resources unless such conduct is consistent with the University's educational and academic policies.
- Engage in any acts or omissions to intentionally or unreasonably endanger or damage any data or the security or integrity of any data or technology resources.
- Knowingly access, add, or modify any data without proper authorization.
- Utilize University technology resources to promote, solicit, support, or engage in any commercial activities on behalf of or for the benefit of any person or entity other than the University without prior authorization from the appropriate University entity.

Enforcement

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, and the Student Code.

All technology accounts assigned to grant access to specific MSU systems are subject to the removal or suspension of these accounts upon violation of the policy or due to a security incident response or action.

~~**STANDARD ACCESS PROCEDURE:**~~

~~All users given access to specific MSU systems are subject to the removal of such access upon their termination date regardless of classification.~~

APPROVED BY:

VICE PRESIDENT: _____ DATE: _____

APPROPRIATE INSTITUTIONAL REVIEW: _____ DATE: _____

PRESIDENT: _____ DATE: _____

UAR NUMBER: 405.00

TITLE: Password Policies and Procedures

ORIGINATOR(S):

Chief Information Officer in the Office for Information Technology

INITIAL ADOPTION: 10/01/2023

REVISED:

AUDIENCE: (SELECT ALL THAT APPLY)

☒ FACULTY ☒ STAFF ☒ STUDENTS ☒ VENDORS ☒ OTHER: (SPECIFY): All Users

PURPOSE:

The purpose of this policy is to establish guidelines for the creation, management, and protection of user passwords within the Morehead State University (MSU) Information Technology infrastructure. By implementing strong password practices, the university aims to ensure the confidentiality, integrity, and availability of sensitive data and systems.

SCOPE:

This document covers all passwords for technology accounts maintained by the Office of Information Technology and MSU. Password covered by the policy include (but are not limited to) privileged non-privileged, service and any other accounts maintained by MSU. The following statements will function as MSU's official guidelines for password management for all accounts used to access the University's technology systems.

Policy Statement

All individuals are responsible for safeguarding their provided technology account credentials. These credentials must comply with the password parameters and standards identified in this policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

Reason for Policy

Assigning unique user logins and requiring password protection are fundamental security measures implemented at Morehead State University to control access to the university network and its associated data, ensuring that only authorized users can gain entry. Compromised passwords pose a significant risk, potentially granting unauthorized individuals unintended or malicious access to information systems. It is the responsibility of individuals with university-issued credentials to actively protect their accounts from unauthorized access by adhering to this policy, thereby maintaining the confidentiality and robustness of their passwords. The password parameters outlined in this policy are designed to meet legal and regulatory requirements, including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Entities Affected by this Policy

Morehead State University Faculty, Staff, Students, Affiliates and Guests with any type of MSU information system access.

Who Should Read this Policy

All individuals provided a technology account for accessing Morehead State University Information systems.

Individual Responsibilities

It is the responsibility of individuals to maintain the security and confidentiality of their passwords. Therefore, the following guidelines must be followed when creating and protecting passwords:

- MSU Technology Account initial passwords are required to be changed as part of the account initialization process. Initial passwords must be securely transmitted to the individual.
- Under no circumstances should MSU Technology Account passwords be shared with others in any manner that violates this policy. Sharing or compromising a MSU Technology Account password is considered a security incident and must be reported to OIT.
- MSU Technology Account users, including faculty, staff, students, affiliates and guests must never share their password or request someone else's password. If asked to provide your password or grant access to another person using your credentials, it is your obligation to report this to OIT Information Security and Compliance Division using the methods outlined in the Procedures section below.
- MSU Technology Account passwords must never be written down and left in a location easily accessible or visible to others whether on paper or in digital formats. Passwords may be stored in a secure password manager, such as 1Password or LastPass, as long as the master password is kept private and meets the requirements in the Password Requirements section of this policy.
- Individuals must not remain logged into applications or systems where others could potentially use their account unknowingly.
    - To access shared workstations (e.g., student labs or classroom podiums), OIT will provide a limited-use shared account for the workstation, when required. Individual credentials must then be used for accessing applications, such as Blackboard.
    - OIT will never ask for a password. In OIT support scenarios where an MSU Technology Account cannot be used, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session. The individual should not share his/her password with the technician. All OIT support technicians are expected to abide by departmental policy and their actions may be audited upon request.
    - In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device hard drive should be backed up to a secure storage device and wiped securely prior to being handed over to an external technician. OIT will assist with any repairs by a third-party to ensure data exfiltration does not occur. Passwords should not be shared with a third-party or non-MSU affiliated support technician.
- If a password needs to be issued to a remote user or service provider, the password must be sent with proper

safeguards (e.g., shared via a secure password manager or sent via an encrypted email message).

- If a password needs to be shared for servicing, OIT Information Security and Compliance should be contacted for authorization and appropriate instruction.
- Passwords for MSU Technology Accounts must be unique and different from passwords used for other personal services (e.g., banking). It is not recommended to use an MSU technology account or similar credentials or passwords for personal accounts such as bank, shopping or social media account.
- MSU Technology Account passwords must meet the requirements outlined in this policy.
- MSU Technology Account passwords must be changed at the regularly scheduled time interval (as defined in "Password Expiration" section of this policy where applicable) or upon suspicion or confirmation of a compromise.
- Individuals with access to service accounts or test accounts must ensure the account password complies with this policy and must keep the password stored in a secure password manager.
- In the event a breach or compromise is suspected, the incident must be reported to OIT Information Security and Compliance immediately using one of the methods outlined in the Procedures section below.

Responsibilities of Systems Processing Passwords

All MSU OIT systems, including servers, applications, and websites that are hosted by or for MSU must be designed to accept passwords and transmit them with proper safeguards.

- Passwords must be prohibited from being displayed when entered.
- Passwords must never be stored in clear, readable format (encryption must always be used).
- Passwords must never be stored as part of a login script, program, or automated process unless the password is encrypted or tokenized.
- Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.
- Password hashes (irreversible encoded values) must never be accessible to unauthorized individuals.
- Where possible, salted hashes (irreversible encoded values with added randomness) should be used for password encryption.
- Where any of the above items are not supported, a variance request should be submitted to OIT Information Security and Compliance for review. Appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to readable passwords.

Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts (except for passcodes defined in section Mobile Devices) where passwords are:

- Passwords must be at least 12 characters long.
- Not contain the user's MSU-ID that exceed two consecutive characters
- Passwords must not be the same as the user's name, email address, or any other personal information or made up of common words affiliated with Morehead State University. (i.e., Eagl3$1234, M$u@2023!, etc.)
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

Password Expiration

With the implementation of Multi-Factor Authentication, most users are not required to change their passwords at fixed intervals. Some account types, such as privileged users, must still adhere to regular password changes as defined below. However, in all cases, OIT Support staff reserves the right to reset a user's password in the event a compromise is suspected, reported, or confirmed. This helps prevent an attacker from making use of a password that may have been discovered or otherwise disclosed.

Account Types

Standard Users

Standard users consist of:

- MSU faculty
- MSU Staff
- MSU Students
- MSU Affiliates
- Guests

Passwords must be changed upon suspicion or confirmation of compromise.
New passwords must comply with the criteria in the Password Requirements Section of this policy.

Privileged/Specialized Accounts

Privileged or Specialized accounts are provided to users with elevated access to administer information systems and applications (other than to a local device), most often in the Office of Information Technology (OIT) Division. Such users have administrator access via a shared account or to multiple systems at MSU. These accounts are at a higher risk for compromise.

- Shared Privileged domain accounts must be stored in the OIT Approved Privileged Account Management (PAM) system (or password vault) and these shared passwords should be rotated regularly.
- Privileged accounts that cannot be stored in the PAM system must have their passwords changed every ninety (90) days.
- Passwords must not be reused for at least six (6) generations.
- Passwords must not be changed more than one (1) time per day.
- At least four (4) characters must be changed when new passwords are created.
- New passwords must comply with the criteria in the Password Requirements Section.

Payment Card Industry (PCI) Accounts

Users responsible for processing payments in MSU financial systems, such as Colleague or the current payment provider, must adhere to the Payment Card Industry's (PCI) Data Security Standard for password expiration. As of this policy update, the requirements are below:

- Passwords must be changed every ninety (90) days.
- Passwords must not be reused for at least four (4) generations.
- Passwords must not be changed more than one (1) time per day.
- At least four (4) characters must be changed when new passwords are created.
- New passwords must comply with the criteria in the Password Requirements Section.

Service Accounts and Test Accounts

Service accounts are accounts used by a system, task, process, or integration for a specific purpose. Test accounts are temporarily used to imitate a role, person, or training session. Passwords for service accounts and test accounts must be securely generated in accordance with this policy, distributed securely to the account owner, and stored securely in the OIT approved PAM system.

- Passwords must be changed upon suspicion or confirmation of compromise.
- Passwords must be changed when an account owner leaves the institution or transfers into a new role.
- Passwords must comply with the criteria in the Password Requirements Section.

Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations vary based on the type of user, as defined below.

Standard Users

Standard user accounts have the following lockout policy:

- Accounts will lockout after eighteen (18) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for fifteen (15) minutes unless the OIT Help Desk is contacted, and the user's identity is verified for the account to be unlocked sooner.

Privileged/Specialized Accounts
Privileged or Specialized Accounts have the following lockout policy:

- Accounts will lockout after twelve (12) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for fifteen (15) minutes unless the OIT Help Desk is contacted, and the user's identity is verified for the account to be unlocked sooner.

Payment Card Industry (PCI) Accounts
Payment card industry (PCI) users have the following lockout policy:

- Accounts will lockout after six (6) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for thirty (30) minutes, unless the OIT help Desk is contacted and the user's identity is verified so the account can be unlocked sooner.

Service Accounts and Test Accounts
These accounts will have the following lockout policy:

- Accounts will lockout after eighteen (18) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the OIT Help Desk is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

Mobile Devices
Mobile devices accessing or storing MSU data, such as smartphones and tablets, shall be registered with OIT and managed by the mobile device management (MDM) platform. The following minimum password policy is in effect for all mobile devices, where passwords or PINs are:

- At least six (6) digits; and
- No repeating or sequential digits (e.g., 111111, 123456, or 101010)

Biometric authentication (e.g., facial or fingerprint recognition) on mobile devices may be used to unlock the device, but a compliant password must still be established.

A mobile device will erase after ten (10) invalid password attempts. The device manufacturer may automatically impose time limitations after several unsuccessful password attempts before the wipe is triggered. OIT Support Staff can assist in resetting device passcodes.

Recommendations for Creating Compliant Passwords
To create a password that is compliant with the parameters specified in this policy, use one of the methods below.

Use a Passphrase
A passphrase is similar to a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases based on commonly referenced quotes, lyrics, or other sayings are easily guessable. While passphrases should not be famous quotes or phrases, they should also not be unique to you as this may make them more susceptible to compromise or password-guessing attacks.

- Choose a sentence, phrase, or a series of random, disjointed, and unrelated words
- Use a phrase that is easy to remember

- Examples:
    - Password: When I was 5, I learned to ride a bike.
    - Password: fetch unsubtly unspoken haunt unopposed
    - Password: stack process overbid press
    - Password: agile stash perpetual creatable

Use a Secret Code

A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four-character types in order to meet the password complexity requirements.

- Use a phrase that is easy to remember
- Capitalize the first letter of every word
- Substitute letters for numbers or symbols
- Incorporate spaces or substitute with a different character
- Example:
    - Phrase: "When I was five, I learned how to ride a bike."
    - Password: WhenIwa$5,Ilh0wt0rab1k3.

Password Reset Options

Various options are available to assist users with changing a forgotten or expired password. The preferred and fastest method is by using the Microsoft Office 365 Self-Service Password Reset System. This system requires that you have 2 forms of identifiable communication methods to validate your account without knowing your current password. If you know your password and just wish to change it, that can be accomplished by using the Microsoft Office 365 portal under your profile settings. You must also be enrolled in Microsoft Multi-Factor Authentication (MFA). It is recommended that you also have a personal email address in your Microsoft Profile to use this system to reset your password. You can always contact the OIT helpdesk, and they can assist you with resetting or changing your password or updating your personal email address, but you must provide multiple forms of proof of identity.

Reporting a Suspected Compromise or Breach

If you believe your password has been compromised or if you have been asked to provide your password to another individual, including OIT, promptly notify any of the following support teams:

OIT Information Security and Compliance
Email: blueteam@moreheadstate.edu

OIT Help Desk
Phone: (606) 783-4357 (HELP)

Enforcement

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, and the Student Code.

All technology accounts that are assigned to grant access to specific MSU systems are subject to the removal or suspension of these accounts upon violation of the policy.

APPROVED BY:

VICE PRESIDENT: _____ DATE: _____

APPROPRIATE INSTITUTIONAL REVIEW: _____ DATE: _____

PRESIDENT: _____ DATE: _____