PG-55 TECHNOLOGY RESOURCE ACCEPTABLE USE

Policy: PG-55 Technology Resource Acceptable Use

Approval Date: 02/26/1999

Revisions: 09/15/2005, 08/01/2006, 06/05/2008, 12/06/2018; 08/08/2019, 06/15/2024

Last Review Date: 06/15/2024

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.

EMAIL US!

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, and 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.

Definitions

MSU Managed Device - A Morehead State University (MSU) managed device refers to a computing device (such as a computer, smartphone, or tablet) that is owned and controlled by an organization or enterprise. These devices are typically provided to employees for work-related tasks and are managed centrally by the organization's IT department or designated administrators. These devices also include devices that are purchased as part of a grant opportunity that ultimately become MSU owned when the grant is complete.

BYOD Device - A BYOD (Bring Your Own Device) device refers to a personal computing device, such as a smartphone, tablet, or laptop, that is owned and operated by an individual employee rather than provided by Morehead State University.

Encrypted Communications - Encrypted communications refer to the transmission of data in a way that renders it unintelligible to anyone who doesn't possess the decryption key. Essentially, it involves scrambling the content of a message using cryptographic techniques to prevent unauthorized access or interception. Encryption is commonly used in various forms of digital communication, including emails, instant messaging, voice calls, and online transactions, to protect sensitive information such as personal data, financial details, and confidential business communications from unauthorized access or eavesdropping. Here are some common ways to encrypt data:

EMAIL US!

- Utilize a secure Wi-Fi connection (such as MSU-SECURE)
- Utilize a Virtual Private Network Connections (VPN)
- Use "Encrypt" function built into Microsoft Outlook for protecting emails.

Secure Area - A secure area is a designated physical space or location that is protected and controlled to prevent unauthorized access. The primary purpose of a secure area is to safeguard sensitive information, valuable assets, or critical infrastructure from theft, sabotage, espionage, or other security threats. Secure areas can vary widely in size and complexity,

ranging from small rooms or compartments within a building to entire facilities or compounds. Access to these areas is typically restricted to authorized personnel only, who may be required to undergo identity verification, authentication, or other security measures before entering.

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.

EMAIL US!

- Personnel must not share their Morehead State University authentication information, including:
  - Account passwords,
  - Where possible, 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, securit 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.

EMAIL US!

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.

EMAIL US!

- 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.

EMAIL US!

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)

- It is recommended that all personally owned laptops and/or workstations 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 should 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.
- In consultation with the device owner, Morehead State University OIT Leadership may choose to execute "remote wipe" capabilities for mobile devices.
- 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 by local, state or federal authorities.
- 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.

EMAIL US!

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.

EMAIL US!

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.

CONTACT HUMAN RESOURCES

Human Resources

301 Howell-McDowell
Morehead, KY 40351

EMAIL: humanresources @moreheadstate.edu
PHONE: 606-783-2097

VIEW HUMAN RESOURCES STAFF

EMAIL US!

150 University Blvd.
Morehead, Kentucky 40351

1-800-585-6781
606-783-2000

Academic Catalogs

Academic Calendars

Accreditation

Transcripts

Privacy Policy

Nondiscrimination & Title IX

Web Accessibility

MAKE A GIFT

SEARCH JOB POSTINGS

EMAIL US!

EMAIL US!