UMMC Policy and Procedure Manual	A-IP-SEC-GEN-PO-00002
Subject: Acceptable Use Policy	
Old Title: Information Security Acceptable Use Policy	
Revised Date: 10/13/2018	**Effective Date:** 10/9/2018
Prepared By: Richie Stonecypher	**Approved By:** Steve Waite **Reviewed By:** Kim Sterdivant

Purpose of Policy

The purpose of this policy is to set standards and expectations for University of Mississippi Medical Center (UMMC) employees and students with regard to accessing UMMC information assets.

Policy Scope

This policy applies to all workforce members, users, and all personnel affiliated with third parties who use UMMC information assets and related resources.

This policy applies to information technology administered centrally; personally-owned computing devices connected by wire or wireless to the UMMC network; and to off-site computing devices that connect remotely to the UMMC network.

Definitions

For a complete list of definitions, refer to the Glossary.

Policy Statement

A. User Responsibilities and Acceptable Use

1. UMMC provides information technology assets as resources to the UMMC workforce. It is the User's responsibility to properly use and protect those resources.

2. Use of information technology assets owned or operated by UMMC imposes certain responsibilities and obligations. UMMC considers use of IT resources to be a privilege that is granted on the condition that each user respects the integrity of IT resources and the rights of other users.
3. Users shall comply with all UMMC policies, state and federal laws, regulations, and contractual obligations when accessing UMMC information technology assets.
4. Workforce member's actions may be monitored and workforce members consent to such monitoring.
5. Users are responsible for protecting all UMMC information technology assets to which they are granted access.
6. User access to UMMC information assets shall be restricted based on need-to-know and in accordance with the minimum necessary principle.
7. Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow UMMC policies.
8. Users are responsible for the use and protection of UMMC information resources by using effective access controls (e.g., passwords) and by safeguarding those access controls.
9. Users are responsible for the security of their passwords and all data which they are authorized to access.
10. Users who are authorized to access confidential data are responsible for properly storing and securing it from unauthorized access, as well as for securing and protecting passwords and other forms of access control.
11. Copy, move, print (and print screen), and storage of sensitive data is prohibited when accessed remotely without a defined business need.
12. Users are allowed to use UMMC information technology assets:
    1. To which they have been granted authorized access.
    2. For UMMC business and research purposes only.
13. Each user bears the responsibility for knowing and complying with applicable laws, policies, and rules; for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of UMMC information technology assets.
14. Related UMMC policies that may apply to acceptable use of UMMC information assets include, but are not limited to, Human Resources personnel policies, Finance policies, Compliance and Administrative policies, all of which are subject to change.

B. Internet Access from UMMC Locations

1. Connection to the Internet, or use of a website, is a privilege and not a right. Any abuse of that privilege can result in legal and/or administrative action.
2. Internet access is granted to workforce members and visitors with the expectation that users will act responsibly and use good judgment.
3. Internet access may be monitored at any time by UMMC. Any website or online activity may be blocked if it is determined to be harmful, potentially harmful, or disruptive to the organization or other workforce members.
4. Access to the Internet shall only be permitted though the UMMC corporate firewall.
5. A separate network shall be established to provide Internet access to visitors. The UMMC corporate network must not be accessible from the visitor network.
6. Individually assigned passwords and accounts must not be shared.
7. Personal and UMMC (business) passwords must be different.
8. Users shall utilize strong passwords, which meet the following specifications:
    1. At least eight characters in length
    2. Containing at least one number and one special character
    3. Not the same as the username or email address

C. Responsibilities for Unattended Information Technology Assets

1. Users shall ensure that unattended equipment has appropriate protection.
2. Users shall log-off computing devices when the session is finished (i.e., not just switch off the PC screen or terminal) in accordance with the **Clear Desk and Clear Screen Policy**.
3. Users shall safeguard unattended information system output devices (e.g., printers) to prevent unauthorized individuals from obtaining the output.

D. Code of Conduct

Users of UMMC Information Technology Assets agree to NOT:

1. Post, use or transmit content that you do not have the right to post or use, for example, under intellectual property, confidentiality, privacy or other applicable laws.
2. Post, use or transmit unsolicited or unauthorized content, including:
   1. Advertising or promotional materials
   2. “Junk mail”
   3. “Spam”
   4. “Chain letters”
   5. “Pyramid schemes”
   6. Political campaign promotional material
   7. Any other form of unsolicited or unwelcome solicitation or advertising
   8. Infringe upon copyrighted material of any kind, including the unauthorized downloading, copying, displaying, and/or distributing of copyrighted material. All such works should be considered protected by copyright law unless specifically stated otherwise. Any use of UMMC information technology assets (e.g. network, email system, website, etc.) to access, display, send, transfer, modify, store or distribute copyrighted material (e.g., video/movies, music/audio, images, documents, software, text, etc.) is strictly prohibited.
3. Post, use or transmit content that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or otherwise interfere with or disrupt UMMC information assets.
4. Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false or misleading, incites an illegal act, or is otherwise in breach of your obligations to any person or contrary to any applicable laws and regulations.
5. Intimidate or harass one another.
6. Allow unauthorized use or attempt to use another user’s individual account, service, or personal information.
7. Modify workstations without IT approval or remove, circumvent, disable, damage or otherwise interfere with any security-related features.
8. Install or use unauthorized or malicious software, or obtain unauthorized data and software from external networks.
9. Transmit (e.g., messaging, email, texting, etc.) Confidential Data over open, unprotected wireless networks unless approved security controls such as strong encryption are in place.
10. Automatically forward Confidential Data, including Protected Health Information (PHI), to an external email address.
11. Use UMMC demographic data such as business email address for personal use (e.g., register for software, complete a web form).

12. Attempt to gain unauthorized access to UMMC information technology assets, other user's accounts, computing devices or networks connected to UMMC information technology resources, through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of UMMC information assets or any activities conducted through those information assets.
13. Impersonate another person or entity, or falsely state or otherwise misrepresent your affiliation with a person or entity without authorization.
14. Connect personnel devices to the UMMC network prior to putting appropriate safeguards in place.
15. Conduct any activities with the intention of creating and/or distributing malicious programs using the UMMC network (e.g., viruses, worms, Trojan Horses, etc.).
16. Fail to exercise appropriate caution when opening emails, attachments or accessing external web sites.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO), or designee, has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UMMC reserves the right to add, delete, or revise any provision of this Policy (with committee approval) at any time, or any other Information Security Policy without prior notice to users.

Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UMMC's computing environment is subject to loss of network privileges and any other disciplinary actions deemed appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy.

Exceptions

The process to request exceptions to information security policies is available. Request are evaluated based on the potential risks to business, as well as, security. The CISO has the ability to approve exceptions and may request compensating controls and processes. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice.

Regulatory and Standards References

HIPAA Regulatory References: HIPAA § 164.308(a)(5)(ii)(B), HIPAA § 164.308(a)(5)(ii)(D), HIPAA § 164.310(a)(1), HIPAA § 164.310(b), HIPAA § 164.310(c), HIPAA § 164.312(a)(2)(iii)

PCI References: PCI DSS v3 5.1.1, PCI DSS v3 8.5.11, PCI DSS v3 8.5.3, PCI DSS v3.1 5.1, PCI DSS v3.1 5.2, PCI DSS v3.1 8.2.4, PCI DSS v3.1 8.2.4, PCI DSS v3.1 8.2.5, PCI DSS v3.1 8.4