Status **Active** PolicyStat ID **18466047**

Origination	10/2006
Last Approved	07/2025
Effective	07/2025
Last Revised	07/2025
Next Review	07/2029
Owner	David Sliman: Chief Information Officer
Area	iTech

Acceptable Use Policy

COPY

Policy Statement

The University of Southern Mississippi (USM) is committed to protecting the information technology (IT) resources and the students, faculty, staff, affiliates, contractors, vendors, and guests from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate information technology use exposes USM to risks including, but not limited to, malware, compromised accounts of networked systems and services, compliance, and regulatory issues. Effective information security requires the participation and support of every USM student, employee, or other who handles University data and/or information technology resources.

Reason for Policy/Purpose

This policy is required to effectively communicate the University policy regarding the acceptable use of information technology resources at USM.

Who Needs to Know This Policy

This policy applies to students, faculty, staff, affiliates, contractors, vendors, and guests at USM, including personnel affiliated with third parties or individuals accessing University IT resources.

Definitions

Antivirus Software: software specifically designed to detect and remove computer viruses and malware.

Digital Millennium Copyright Act (DMCA): United States copyright law that complies with World Intellectual Property Organization treaties, specifically addresses digital access control and digital rights management, and enhances penalties for copyright infringement over the Internet.

Downloading: network trafficking of data files originating from an external network and destined for the USM network.

Higher Education Opportunities Act of 2008 (HEOA): United States legislation that reauthorizes previous legislation designed to strengthen post-secondary institutions and provide financial aid for students at colleges and universities.

Information Technology Resources: any computing device, network, or network service used for creating, reading, sharing, modifying, or storing data and information.

Malware: malicious software that is intended to damage or disable computer systems.

Password: a combination of letters, numbers, and symbols used to authenticate an individual.

Personal device: a computer, laptop, tablet, smart phone or similar device that is not owned by USM, regardless of whether the device is managed or partially managed by USM.

Spam: unsolicited bulk electronic messages.

Users: students, faculty, staff, affiliates, contractors, vendors, and guests.

Policy/Procedures

COPY

A. **Ownership and General Use**

1. University information technology resources (IT resources) are provided for users to enable, support, or enhance the mission and goals of the University. Use of IT resources by individuals unaffiliated with the University is prohibited, except for IT resources that are explicitly made available for use by unaffiliated individuals.
2. Users of University IT resources must exercise good judgment regarding incidental personal use and activity unrelated to the University's mission and goals.
3. Always use your University issued computer for University business. These devices are equipped with required security controls to help protect University data and ensure compliance with institutional and legal obligations. The use of personal devices to conduct University work is discouraged and permitted only in limited, low-risk scenarios and must follow established security requirements listed below. Any exception to this standard requires formal approval from the Information Security Office, in consultation with the Office of General Counsel and relevant leadership, to ensure that risks are understood and properly mitigated. The use of personal devices may be used to conduct University work under the following conditions:
    a. All personal devices used for USM work must comply with the University's Information Security Policy.
    b. All USM High and USM Moderate data must not be stored locally on personal devices.
    c. All USM High and USM Moderate data must be stored on USM devices or systems in accordance with the Information Security Policy.
    d. USM may implement technical controls to limit or secure the connections of personal devices to USM systems with USM High data to limit the

possibility of local data storage, data breaches, and other security incidents.

e. Any USM data stored on personal devices must be permanently deleted from the device before the device is transferred to another person, sold or otherwise disposed of.

4. USM cannot ensure individual privacy while using University managed IT resources, phone services, and Internet or network services. Data, documents, and emails created, received, or stored on University IT resources, including services hosted by a third party for use by USM, may be considered the property of USM and the State of Mississippi and might be subject to public records requests. For this reason, the privacy of personal and non-university information cannot be guaranteed if transmitted through or stored on a University IT resource or service.

B. **Responsibilities**

1. Users of University IT resources are responsible for knowing and understanding any laws, regulations, policies, or contracts that may affect or govern the resources they use or the information they access, create, or modify.
2. Users are expected to utilize IT resources with integrity and respect for other individuals, institutions, and entities.
3. Users must take necessary steps to prevent unauthorized access to University information and resources.
4. Users are responsible for the security of their account credentials, including passwords and passphrases. Users are expected to keep their credentials private and must never ask another user for their University account credentials.

COPY

C. **Acceptable Use**

1. Use of University IT resources that enables, supports, or enhances the mission of the University, fulfills the expected duties of an employee, or aids in the scholarly pursuits of a student, is generally acceptable.
2. Extracurricular activity that does not disrupt or harm the University business or exposes the University and its resources to unacceptable levels of risk is generally acceptable.
3. Use of copyrighted material for which the University or user has authorization, or which use would be considered “fair use” as defined by 17 U.S.C. § 107 and § 108, is generally acceptable.

D. **Unacceptable Use**

1. The following activities including, but not limited to, are strictly prohibited:
    a. Use University IT resources to engage in any illegal activity under local, state, federal, or international law.
    b. Collection, storage, or distribution of pornography or material considered to be obscene, for purposes not related to University sanctioned academics, research, or legal proceedings.

c. Unauthorized copying, sharing, downloading, or other use, excluding activity that is considered “fair use,” of any material or intellectual property protected by copyright or trade secret. Protected material can include, but is not limited to, photographs or text from magazines, books, or other copyrighted sources, music, movies, and software.

d. Intentionally exposing University IT resources to malicious software.

e. Sharing access to University accounts, resources, and login information with others or allowing the use of accounts or services by others.

f. Using University IT resources to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws.

g. Effecting security compromise, where compromises include, but are not limited to, accessing data for which the user is not authorized, allowing information or resources to be available to unauthorized users, or logging into a server or account that the user is not expressly authorized to access unless these duties are within the scope of regular duties.

h. The disruption of network resources including, but are not limited to, ping floods, packet spoofing, denial of service attacks, and the forging of routing information.

i. Port scanning or vulnerability scanning is expressly prohibited unless prior notification is given to USM Information Technology Services (iTech) or these processes are within the scope of regular duties.

j. Executing any form of network monitoring that will intercept data not intended for the individual unless this activity is within the scope of regular duties.

k. Providing information about (or lists of) USM faculty, staff, or student non-directory information to parties outside the University without the express written permission of the University administration.

l. Sending email messages, including "spam" or other advertising material, to individuals who did not specifically request such material.

m. Any form of harassment via email, messaging service, forum, or social media, whether through language, frequency, or size of messages.

n. The forging of email header information in an attempt by an individual to misrepresent or hide his or her identity.

o. Creating or forwarding chain letters or other pyramid schemes of any type.

p. Use of University resources to operate software or advertise a service or product not authorized by USM for personal gain.

q. Installing software applications on University-owned equipment solely for personal use.

r. Downloading, accessing, procuring, or using prohibited technology on devices or networks owned or operated by the University of Southern Mississippi is strictly prohibited pursuant to the National Security on State

COPY

Devices and Networks Act as outlined in Miss. Code Ann. Sec. 25-53-191. For a detailed list of prohibited technologies, see the Mississippi Department of Information Technology Services' publicly available list accessible on the Mississippi Department of Information Technology Services website.

E. **Unauthorized Distribution of Copyrighted Material**

1. In compliance with the Higher Education Opportunities Act of 2008 (HEOA) [Student Assistance General Provisions 34 CFR Section 668], it is the policy of The University of Southern Mississippi (USM) to prohibit the unauthorized distribution of copyrighted material on its network while ensuring minimal disruption to educational and research activities. In support of this requirement, USM mandates the use of technology-based deterrents, educational mechanisms for informing the community about appropriate use, and procedures for addressing unauthorized activities. Disciplinary actions may include penalties such as loss of network access, as well as civil, administrative, or criminal actions. Additionally, USM conducts periodic reviews of the plan's effectiveness and, where feasible, offers legal alternatives for acquiring copyrighted material. For more information, refer to the USM Peer-to-Peer Policy.

F. **Enforcement**

1. **Students, faculty, and staff:** Any student, faculty, or staff found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion, and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.
2. **External Entities:** Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract and, as such, may be subject to grievances or penalties allowed by such a contract.

COPY

Review

The Chief Information Officer is responsible for the review of this policy every four years (or whenever circumstances require immediate review).

Forms/Instructions

N/A

Appendices

N/A

Related Information

N/A

All Revision Dates

07/2025, 09/2024, 08/2023, 09/2021, 09/2020, 12/2019, 02/2013, 11/2011, 10/2008, 04/2008, 11/2006, 11/2006, 10/2006

Approval Signatures

Step Description	Approver	Date
General Counsel	Jon Weathers: General Counsel	07/2025
Director of Compliance and Ethics	Paul Walters: Dir Compl & Ethics/Asc Gen Col	07/2025
VP of Finance and Admin	Allyson Easterwood: VP Finance & Admin/CFO	07/2025
Chief Information Officer	David Sliman: Chief Information Officer	07/2025
Associate Director of Compliance and Ethics	Amanda Butler: Asc Dir Compl & Ethics	07/2025

COPY