OP 01.12: USE OF INFORMATION TECHNOLOGY RESOURCES

PURPOSE

Mississippi State University's (MSU) information technology resources serve a large number of faculty, students, staff, and others. This policy addresses the responsibilities of the University and of all users of these information technology (IT) resources whether provided on premises or through cloud-based services.

POLICY

All users are required to use University IT resources in an effective, efficient, ethical, secure, and lawful manner. Use of Mississippi State University's IT resources must be consistent with the mission of the University and all applicable laws and policies. University business must be conducted using University-approved information technology resources except as otherwise authorized under this policy, another University policy, or an exception approved by the Chief Information Officer.

GUIDELINES

Security:

Each user is responsible for maintaining the security of electronically stored information, as specified in the University's Information Security Policy, OP 01.10, and associated Information Security Program. Such responsibilities include, but are not limited to:

- Accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others.
- Two-factor authentication is required as specified by the Mississippi State University Information Security Program.
- Each user should be aware of computer viruses and other malicious computer programs and take steps to avoid being either their victim or propagator. Minimally, each user must ensure that appropriate and current antivirus software is operational on all personal computers and that virus definitions are kept current.

University Business, Communications, and Web Resources:

For purposes of this policy, University-approved information technology resources include systems, services, platforms, accounts, and hosting environments provided or managed by the University, or otherwise authorized under applicable University policies and procedures.

Official Communications - University business must not be conducted through personal or other non-University email accounts unless authorized by the Chief Information Officer. Temporary use of a non-University email system may be subject to review by the Chief Information Officer, including review of measures taken to preserve applicable University records.

Email Forwarding - Automatic forwarding of University email to an external email account or service is prohibited unless authorized by the Chief Information Officer.

Websites and Internet Domains - Official University websites and web applications representing the University or operating on the University's behalf must be hosted on University-approved platforms and use University-approved internet domains unless authorized by the Chief Information Officer.

The Chief Information Officer may approve exceptions based on documented academic, research, outreach, business, partnership, legal, contractual, or technical requirements. Approved exceptions may be subject to appropriate security, data protection, records management, accessibility, or other safeguards.

Digital and Electronic Copyright Infringement:

The Higher Education Opportunity Act of 2008 34 CFR Section 668 requires universities which receive federal student aid funds to effectively combat the unauthorized distribution of copyrighted material. MSU is committed to an aggressive plan of education, deterrence, and remediation to protect MSU students, faculty, and staff, as well as the rights of copyright holders. All users of University IT resources must understand that copying, using, downloading, uploading, sharing, or otherwise distributing copyrighted material (including, but not limited to, music, movies, books, articles, and computer software) without explicit permission of the copyright owner or agent or as allowed by OP 01.20 Policy on Use of Copyrighted Works for Education and Research is a violation of federal law and MSU policy.

"Illegal download" refers to the inappropriate electronic transfer of a copyrighted material from one computer to another across a network; "Peer to Peer file sharing" means using a particular type of software designed to share electronic files or resources between two or more computers across a network. Peer to Peer (P2P) software such as BitTorrent is often used to facilitate illegal downloads and file sharing. The Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), the Business Software Alliance (BSA), and other such groups aggressively seek out potential copyright infringements perpetrated by users of P2P software, and they aggressively pursue violators. MSU maintains information regarding legal download alternatives at http://filesharing.msstate.edu/.

Usage Examples:

University IT resources must be used only in accordance with the law and guidelines defined in this and related policies. Examples of appropriate and acceptable use of IT resources include, but

are not limited to:

a. Academics

b. Research

c. Outreach and service

d. University business-related activities

Examples of inappropriate and unacceptable use of IT resources include, but are not limited to:

a. Illegal downloading or sharing of copyrighted materials, such as music, movies, and software

b. Using IT resources to harass or threaten others (see OP 91.100 and OP 03.03)

c. Downloading or displaying obscene or pornographic material/images

d. Negligently, or intentionally and without authorization, accessing or attempting to access, altering, interfering with the operation of, damaging, or destroying all or part of any IT resource

e. Use or attempted use of electronic accounts, access codes, passwords, or other electronic identification credentials assigned to others or electronically impersonating others

f. Inappropriate or unauthorized sharing, storage, transmission, or publication of intellectual property or protected data via email, web, cloud services, or other technology resources.

g. Commercial advertising or political campaigning

h. Use of IT resources for non-University business or for-profit purposes of the user or for political purposes

i. Use of IT resources in ways that adversely impact the University's IT environment or its users

Privacy:

OP 01.25 Privacy of Electronic Information defines the balance between the University's responsibilities and users' expectations of privacy when using IT resources owned or provided by MSU.

Academic Freedom:

Free expression of ideas is central to the academic process. However, the University may remove any electronic information from its systems if it is determined that:

a. The presence of the information involves illegality (e.g., copyrighted material shared inappropriately, and software used in violation of a license agreement).

b. The information in some way endangers IT resources or the information of other users (e.g., a computer worm, virus, or other destructive program).

c. The information is inappropriate because it is inconsistent with the mission of the University or is otherwise not in compliance with the legal and ethical usage governed by Federal or State law or regulation or with University or Board of Trustees policies.

d. The cost of maintaining the information is deemed prohibitive by the responsible administrative unit.

e. The owner of the information is no longer authorized for access to University resources.

Employee Personal Use:

Employees of the University are permitted incidental personal use of MSU IT resources, subject to review and reasonable restrictions by the employee's supervisor; adherence to applicable University policies and state and federal law; and as long as such usage does not interfere with the employee's accomplishment of his or her job duties and does not result in any additional costs to the University (See OP 01.19 Misuse of University Assets).

Student Personal Use:

Students of the University are permitted personal use of MSU IT resources, subject to review and restrictions as defined by law and University policy including OP 91.100 Code of Student Conduct.

Sanctions and Appeals:

Under federal law first-time offenders who commit copyright violations can face criminal penalties of as much as five years in prison and/or $250,000 in fines; they may also be sued by the copyright holder in civil court, potentially resulting in additional monetary damages and legal fees. Other illegal acts involving use of MSU's IT resources by any person may also be subject to prosecution by state and federal officials.

Anyone found to be in violation of this policy may lose access privileges to the University's IT environment, and MSU students, faculty, and staff are subject to University disciplinary policies and procedures, including:

- OP 01.10 Information Security
- OP 01.19 Misuse of University Assets
- OP 01.25 Privacy of Electronic Information
- OP 03.03 Discrimination, Harassment, and Retaliation

- http://www.honorcode.msstate.edu/policy/
- HRM 60.401 Guidelines for Employee Conduct
- OP 91.100 Code of Student Conduct
- http://filesharing.msstate.edu/

The above policies also define appeals procedures available to MSU students, faculty, and staff.

REVIEW

This OP will be reviewed every four years, or sooner if needed, by the Chief Information Officer.

REVIEWED BY:

/s/ Trey Breckenridge — 09/17/2026
Chief Information Officer — Date

/s/ David Shaw — 10/05/2026
Provost and Executive Vice President — Date

/s/ Tracey N. Baham — 10/05/2026
Associate Vice President, Institutional Strategic & Effectiveness — Date

/s/ Joan Lucas — 10/06/2026
General Counsel — Date

APPROVED BY:

/s/ Mark E. Keenum — 11/23/2026
President — Date