ACCEPTABLE USE OF INFORMATION AND TECHNOLOGY RESOURCES POLICY

Policy Number: 3050
Effective Date: 4/2026
Review Date: 4/26, 10/06, 4/03

1. Purpose

This policy establishes expectations for the responsible and secure use of the College of Southern Maryland's ("CSM" or "College") information and technology resources. It is intended to protect the confidentiality, integrity, and availability of College systems and data while supporting the College's educational and operational mission.

2. Scope

This policy applies to all College employees, faculty, contractors, volunteers, and students. Departments and divisions that hire independent contractors who use the College's technology resources must bind those individuals to the requirements of this policy by contractual agreement.

This policy applies to all College technology resources, including hardware, software, cloud-based systems, software-as-a-service (SaaS) platforms, third-party hosted environments, mobile communication devices, and external systems used to conduct College business or store College data.

Use of College technology resources while teleworking or working remotely is subject to this policy and the College's Telework Policy.

3. Definitions

Information and Technology Resources

All systems, devices, applications, cloud services, network infrastructure, and data repositories owned, managed, or authorized by the College for business or educational purposes. This includes on-premises and third-party hosted systems.

Authorized User

Any individual granted explicit access to specific College systems or data based on business need. Authorization is limited to approved purposes and may be modified or revoked at any time.

Sensitive Data

Information that requires protection due to legal, regulatory, contractual, or institutional requirements,

including but not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), financial data, authentication credentials, and non-public College information.

Security Incident
Any actual or suspected unauthorized access, use, disclosure, modification, destruction, or disruption of College systems or data, including phishing attempts, malware infections, or loss of College-issued devices.

Multi-Factor Authentication (MFA)
An authentication method requiring two or more verification factors to gain access to College systems.

Incidental Personal Use
Occasional limited personal use that does not interfere with College operations, violate law or policy, or create institutional risk.

Right to Monitor
The College's authority to access, review, log, archive, or monitor activity on College systems without prior notice.

4. Policy Statement

CSM is committed to ensuring the responsible, secure, and lawful use of its information and technology resources. This policy establishes standards for use that protect College data, support operational continuity, and uphold applicable legal, contractual, and accreditation requirements.

5. Use Standards and Monitoring

A. Monitoring

Use of College information and technology resources is subject to monitoring, logging, and review. Users do not have an expectation of privacy when using College systems or networks. The use of passwords or other access controls does not imply privacy from authorized College monitoring.

The College retains authority over institutional data accessed, stored, transmitted, or processed on personally owned devices when used for College business.

The College may monitor, access, collect, archive, or review system activity and data as necessary to protect security, ensure operational continuity, comply with legal or contractual obligations, and support institutional needs.

B. Personal Use

College technology resources are provided primarily for business and educational purposes. Limited incidental personal use is permitted provided it does not interfere with job performance, violate law or policy, create security risk, or materially consume institutional resources.

C. Acceptable Use Standards

All users of College information and technology resources must:

- Promptly report suspected security incidents, unauthorized access, phishing attempts, or potential compromise of College data to Information Management and Technology (IMT).
- Protect Sensitive Data and other non-public College information.
- Use only those systems and data for which they are authorized and only for approved business or educational purposes.
- Comply with all applicable laws, contractual obligations, and College policies.
- Use technology resources in a manner that supports operational stability and does not disrupt system availability or performance.

Users may not:

- Access, attempt to access, or use systems, data, or accounts without authorization.
- Introduce malicious code, interfere with security controls, or attempt to bypass authentication mechanisms.
- Use College resources to engage in unlawful, discriminatory, harassing, or fraudulent activity.
- Install or use unauthorized software, applications, or tools on College-managed systems.
- Impersonate another user or misrepresent identity.

System configuration changes, installation of software, or modifications that impact security, supportability, or performance require approval from IMT.

D. Protection of Technology Resources

The College implements technical and administrative safeguards to protect the confidentiality, integrity, and availability of its information and technology resources. Users are responsible for safeguarding the systems and data to which they are granted access.

Users must:

- Protect authentication credentials and not share passwords or other access mechanisms with others.
- Comply with password and authentication requirements established by IMT.
- Comply with multi-factor authentication (MFA) requirements for access to College systems and sensitive data.
- Promptly report suspected credential compromise or unauthorized access.
- Refrain from entering, storing, or transmitting sensitive information or CSM Data into any systems or services that are not owned, distributed, provisioned, and/or protected by the College of Southern Maryland, including but not limited to AI technologies and platforms.

IMT may enforce technical controls, including but not limited to access restrictions, monitoring, and authentication mechanisms.

6. Roles and Responsibilities

Information Management and Technology is responsible for administering and enforcing the technical requirements of this policy, in coordination with Compliance and Risk Management and Human Resources.
Questions regarding interpretation or application of this policy may be directed to IMT or Compliance and Risk Management.

7. Enforcement and Compliance

Suspected violations of this policy must be reported to a supervisor, Compliance and Risk Management, or Human Resources. Violations may result in disciplinary action, up to and including termination of employment, enrollment, and/or access, in accordance with College policies. Contractors and vendors who violate this policy may have access suspended or terminated and may be subject to contractual remedies.

The College, through the President or designee, may temporarily suspend, restrict, limit, or block access to one or more technology resources before initiating or completing disciplinary proceedings if it is deemed necessary to protect the integrity, security, or functionality of the College's technology resources or to shield CSM from potential liability.

8. Related Policies and References

GA 3009 Electronic Communication

GA 3011 Free Speech and Expression Policy

GA 3023 Mass Electronic Mail (Email) Distribution

HR 4130 Protection from Discrimination, Harassment and Retaliation

HR 4155 Telework Policy

HR 4035 Progressive Discipline

9. Review and Revision Process

This policy will be reviewed at least annually, or more frequently as needed, to ensure ongoing compliance with applicable laws, regulations, and institutional requirements. Revisions will be made as necessary to maintain alignment with College of Southern Maryland standards and best practices.