Policy Identification Number	PGC-0002
Policy Title	MUSC Acceptable Use of Computing and Telecommunications Resources Policy
Classification	Enterprise-wide (all the below) University MUSC Hospital Authority (MUHA) MUSC Physicians MUSC Strategic Ventures MUSC Foundation Research
Approval Authority	Policy Governance Committee
Responsible Entity	Policy Governance Committee
Policy Owner	Policy Governance Committee

I. Policy Statement

All members of the Medical University of South Carolina (MUSC) enterprise must follow the standards set forth in the Acceptable Use of Computing and Telecommunications Resources Policy.

II. Scope

This policy applies equally to the Medical University of South Carolina and its affiliates (including but not limited to the Medical University Hospital Authority, MUSC Physicians, and MUSC Physicians Primary Care), third party consultants, contractors, vendors and any individual or entity that is provided access to the MUSC's information resources.

III. Approval Authority

Policy Governance Committee

IV. Purpose of This Policy

To identify the appropriate use and standards for MUSC computing and telecommunications resources.

V. Who Should Be Knowledgeable about This Policy

All MUSC enterprise employees, contractors, vendors, individuals or entities that are provided access to MUSC's Information resources.

VI. The Policy

A. Standards:

a. Applicability:

This policy applies to all members using MUSC computing, telecommunications and wireless resources, including but not limited to computers, computer systems and networks, medical devices, smart phones, portable digital assistants (PDA's), telephones, pagers, cellular phones and two-way radios, whether property of MUSC or not, and to all uses of those resources, whether on campus or from remote locations.

These resources are hereinafter referred to as "computing and telecommunications resources."

Additional guidelines may be established by MUSC to apply to specific computers, computer systems, networks or applications.

b. Requirements:

Legal:

An individual using MUSC computing and telecommunications resources shall comply with all federal, South Carolina, and other applicable laws; all generally applicable MUSC rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; Federal Communication Commission regulations; the MUSC Code of Conduct; the MUSC Anti-Harassment policy; and all applicable software licenses. Users who engage in communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

A member using MUSC computing and telecommunications resources shall use only those resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before accessing any computing resources. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by MUSC.

A user of computing and telecommunications resources shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely

protected. The ability to access other persons' accounts does not, by itself, imply authorization to do so.

Reasonable:

A user of MUSC computing and telecommunications resources shall respect the finite capacity of those resources (including, for example, bandwidth, disk space and CPU time) and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

Email Communications:

Each member is provided with a MUSC email address. This address is considered their official MUSC email account and all MUSC business conducted via email must use the MUSC email account and email system.

Confidential or sensitive information should not be sent through e-mail or exposed to public networks such as the Internet unless adequately secured against unauthorized access and encrypted in transit. Email sent from one musc.edu email address to another musc.edu email address using the MUSC email system is considered secure and no additional steps are needed to encrypt the message.

Personal Use:

Personal use of MUSC computing and network resources is restricted by State law. Section 8-13-700(A) of the South Carolina Ethics Code reads as follows:

"No public official, public member, or public employee may knowingly use his official office, membership or employment to obtain an economic interest for himself, a member of his immediate family, an individual with whom he is associated, or a business with which he is associated. This prohibition does not extend to the incidental use of public materials, personnel, or equipment, subject to or available for a public official's, public member's, or public employee's use which does not result in additional public expense."

Examples of inappropriate personal use include, but are not limited to:

- Interferes with the performance of the user's job or other MUSC responsibilities;
- Accessing pornographic web sites;
- Unreasonably consumes MUSC resources; or
- Is out of compliance with other MUSC policies.

Additional restrictions on personal use may be imposed in accordance with normal management or departmental responsibilities.

Representing MUSC:

Internal: Misrepresenting or willfully concealing your identity at any point on the MUSC network is prohibited.

External: A user of computing and telecommunications resources shall not state or imply that they speak on behalf of MUSC or use MUSC trademarks and logos without authorization to do so. Affiliation with MUSC does not, by itself, imply authorization to speak on behalf of MUSC.

Academic Freedom:

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The freedom to learn depends upon appropriate opportunities and conditions not only in the classroom, but on the campus as a whole. The responsibility to secure and to respect general conditions conducive to the freedom to learn is shared by all members of the academic community -- faculty, staff, and students. System and network administrators are expected to respect the University's academic freedom policies.

Security:

All MUSC members share in the responsibility for protecting MUSC's information systems against threats to availability, integrity and confidentiality. The owners, administrators, and users of all MUSC systems are required to understand and meet their assigned security responsibilities, as defined in this policy, and all other applicable MUSC policies.

All members should be familiar with MUSC information security practices, safeguard their system credentials, employ the appropriate physical safeguards to protect information assets, and protect the confidentiality of electronic protected health information.

B. Expectation of Privacy

MUSC computing and telecommunications resources are not private.
For example, communications made by means of these resources are subject to South Carolina Public Records Law to the same extent as they would be if made on paper. The normal operation and maintenance of MUSC's computing and telecommunications resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

a. Reason to Access Activity

MUSC may access or monitor the activity and accounts of individual users of MUSC computing resources, including individual log in sessions and communications, without notice, when:

(1) It reasonably appears necessary to do so to protect the integrity, confidentiality, availability, or functioning of MUSC generally or computing and telecommunications resources in particular, or to protect MUSC from liability;

(2) There is reasonable cause to believe that the user has violated, or is violating, MUSC policy;
(3) An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns;
(4) The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
(5) It is necessary for MUSC work and business-related reasons (e.g. a person is on vacation or sick leave and access to some files is needed to further institution business); or
(6) It is otherwise required by law.

b. Monitoring as a Job Service Requirement

MUSC may also authorize access and monitoring of an employee's or agent's actual communications over its computing and telecommunications resources where customer service is a primary responsibility of an employee's job duties. Such monitoring must be authorized by Human Resources and employees in positions subject to monitoring shall be notified of such activity.

c. Access monitoring oversight

Any access or individual monitoring, specified in B(a)(5) or for any other reason not listed in B(a) or B(b)., must be authorized in advance by three of the following individuals: Human Resources Director or designee, Legal Counsel, Chief Information Officer, and Chief Information Security Officer, or a majority thereof. The head of the unit which employs the individual will be notified of such access when appropriate. MUSC, at its discretion but subject to any applicable laws, may disclose the results of any access or monitoring, including the contents and records of individual communications, to MUSC personnel or law enforcement agencies and may use those results in appropriate MUSC disciplinary proceedings and/or legal proceedings.

C. Enforcement

Violations of the MUSC Acceptable Use of Computing and Telecommunications Resources Policy by faculty, students, and staff are treated as violations of applicable MUSC policies.

Violations of public law which involve MUSC computer and communication systems may be subject to prosecution by local, state or federal authorities.

MUSC faculty, students, or staff who knowingly violate copyright and/or license terms (for example, by making or using an unauthorized copy of a copyrighted or licensed software product) may be personally liable for their actions.

VII. The Process

The Acceptable Use Policy having already been vetted by the Information Security Committee will seek formal approval by the Policy Governance Committee. Once adopted, the policy will be posted on the

Archer Governance Risk and Compliance web site under the Information Security Office Polices until such time that a more appropriate publication site is available.

VIII. Special situations

Any exception to the Acceptable Use Policy is subject to the Information Security Office's IS-005 Exceptions to Information Security Policy and Standards Policy.

IX. Sanctions for Non-compliance

Violations of the Acceptable Use Policy by faculty, students, and staff are treated as violations of the applicable MUSC policies. Specific procedures for dealing with infractions (for example, disciplinary action and appeals processes) are detailed in the applicable Faculty Handbook, MUSC Bulletin, and/or Personnel Manuals.

Violations of public law which involve MUSC computer and communication systems may be subject to prosecution by local, state or federal authorities.

MUSC faculty, students, or staff who knowingly violate copyright and/or license terms (for example, by making or using an unauthorized copy of a copyrighted or licensed software product) may be personally liable for their actions.

X. Related Information

A. Conflicting policies

N/A

B. Related policies

1. College of Medicine Student Laptop Use Policy
   http://academicdepartments.musc.edu/com/hndbk/policies/College%20of%20Medicine%20Student%20Laptop%20Use%20Policy
2. Department of Public Safety Computer Administration Policy
   http://academicdepartments.musc.edu/vpfa/publicsafety/Manual/PP53%20Computer%20Administration.pdf
3. College of Health Professions Computer Use Policy
   http://academicdepartments.musc.edu/chp/current_students/CHP-Student-Policies-Handbook-Apr%202015.pdf
4. MUSC Information Security Policies
   https://grc.musc.edu

C. Existing policies requiring retirement

1. MUSC Computer Use Policy
   http://academicdepartments.musc.edu/ocio/policies/cup.pdf

D. Relevant laws/statutes/regulatory requirements

Regulatory, Certification and Compliance Drivers

MUSC Entity	Regulatory	Industry Standards, Certification and Accreditation
MUHA	HIPAA, State of SC ISO, Meaningful Use, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Contractual	PCI DSS, NIST, ISO, ITIL
MUSCP	HIPAA, State of SC ISO, Meaningful Use, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Contractual	PCI DSS, NIST, ISO, ITIL
University	HIPAA, FERPA, State of SC ISO, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Contractual	PCI DSS, NIST, ISO, ITIL
Foundation	State of SC ISO, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Contractual	PCI DSS, NIST, ISO, ITIL

E. References, citations

Code of Laws - Title 8 - Chapter 13 - Ethics, Government Accountability, And Campaign Reform
http://www.scstatehouse.gov/code/t08c013.php

Policies and Procedures | Department of Administration - State of South Carolina
http://www.admin.sc.gov/technology/information-security/policies-and-procedures

PCI DSS Quick Reference Guide version 3.1. (2015, May).
https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf
Section 12.3

U.S. Department of Health & Human Services (2003, February 20)
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf
Section 164.308(a)(1) and 164.310(b)

National Institute of Standards and Technology Special Publication 800-53 Rev. 4 (2013, April)
PL-4 Rules of Behavior
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Page F-141

Electronic Communications Privacy Act of 1986
https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

LII / Legal Information Institute
https://www.law.cornell.edu/uscode/text/18/1030

F. Other

None

G. Appendices

None

XI. Key Words

None

XII. Communication Plan

The Acceptable Use Policy will be posted on the Archer Governance Risk and Compliance web site under the Information Security Office Polices until such time that a more appropriate publication site is available. The Information Security Office will coordinate with Communications Committee to send a formal communication to all of MUSC.

XIII. Approval Body

The Policy Governance Committee

XIV. Definitions

Confidential information/data is information whose unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on MUSC, its customers or employees. Confidential information may be shared with parties who have a relationship with MUSC, if they have signed a non-disclosure agreement, and have a need to know. This data classification is further defined in the 6.0 Data Stewardship and Information Classification Policy; Section 6.2 Information Classification; ISO-S-0024 Data Classification Level standard.

Enterprise: The Medical University of South Carolina and its affiliated organizations, such as the Medical University Hospital Authority and the MUSC Physicians.

Managers (of Users): MUSC members who have management, sponsorship, or supervisory responsibility, including deans, department chairs, directors, department heads, and supervisors. Faculty who supervise teaching and research assistants are included.

Public information/data is information that can be disclosed to anyone. It would not violate an individual's rights to privacy. Knowledge of this information does not expose MUSC to financial loss, embarrassment or jeopardize the security of MUSC assets. This data classification is further defined in the 6.0 Data Stewardship and Information Classification Policy; Section 6.2 Information Classification; ISO-S-0024 Data Classification Level standard.

Restricted information/data is characterized as sensitive information that is intended for a very limited group of individuals who should be specified by name. This level contains information, which if disclosed would provide access to business secrets and could jeopardize important interests or actions of MUSC or its clients and would be to the serious personal or financial detriment if revealed to unauthorized persons. This data classification is further defined in the 6.0 Data Stewardship and Information Classification Policy; Section 6.2 Information Classification; ISO-S-0024 Data Classification Level standard.

Sensitive Information/Data: Any information/data classified as Confidential or Restricted.

System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information. A system includes hardware (e.g., workstations, servers, and portable devices), software, applications, databases, or any other device that performs similar functions. (Systems also include specialized systems such as industrial controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.)

User: A person or entity authorized to use a MUSC information technology resource.

XV. Policy Owner(s) and Contact Information

Name	Email	Title
Richard Gadsden	gadsden@musc.edu	Information Security Officer
Matt Jones	jonemd@musc.edu	Senior Information Security Analyst

XVI. Approval

Dr. David J. Cole, President MUSC