

GCSU

Information Security Operational Procedures

Electronic Communications Policy

INTRODUCTION

Georgia College & State University (GCSU) encourages the use of electronic communications to share information and knowledge in support of the University's mission of education, research, and public resource and to conduct the university's business. To this end the university supports and provides interactive electronic communications resources and facilities for telecommunications, mail, publishing, and broadcasting. Recognizing the convergence of technologies based on voice, video, and data networks, this Policy establishes an overall policy framework for electronic communications.

GENERAL PROVISIONS

PURPOSE

The Electronic Communications Policy is designed to:

- Establish policy on privacy, confidentiality, and security in electronic communications;
- Ensure that University electronic communications resources are used for purposes appropriate to the University's mission;
- Inform the University community about the applicability of related laws and University policies to electronic communications;
- Ensure that electronic communications resources are used in compliance with those laws and University policies; and
- Prevent disruptions to and misuse of University electronic communications resources, services, and activities.

SCOPE

This Policy applies to:

- All electronic communications resources owned or managed by the University;
- All electronic communications resources provided by the University through contracts and other agreements with the University;
- All users and uses of University electronic communications resources; and
- All University electronic communications records in the possession of University employees or of other users of electronic communications resources provided by the University.

This policy applies to the contents of electronic communications and to the electronic attachments and transactional information associated with such communications.

This Policy applies only to electronic communications records in electronic form. This Policy does not apply to printed copies of electronic records and printed copies of transactional information. Electronic communications records in either printed or electronic form are subject to federal and

state laws as well as University records management policies, including their provisions regarding retention and disclosure.

DEFINITIONS

Knowledge of the terms and definitions is important to an understanding of this Policy.

- **Compelling Circumstances:** Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies, or significant liability to the University or to members of the University community.
- **Electronic Communications:** Any communications that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or resources. For purposes of this Policy, an electronic file that has not been transmitted is not an electronic communication.
- **Electronic Communications Records:** Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or resources. This definition of electronic communications records applies equally to the contents of such resources, attachments to such resources, and transactional information associated with such records.
- **Electronic Communications Resources:** Any combination of telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, network input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications resources.
- **Electronic Communications Service Provider:** Any unit, organization, or personnel with responsibility for managing the operation of and controlling individual user access to any part of the University's electronic communications systems and resources.
- **Electronic Communications Systems or Resources:** Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.
- **Emergency Circumstances:** Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.
- **Holder of an Electronic Communications Record or Electronic Communications Holder:** An electronic communications user who, at a given point in time, is in possession of receipt of a particular electronic communications record, whether or not that electronic communications user is the original creator or a recipient of the content of record.
- **Possession of Electronic Communications Record:** An individual is in possession of an electronic communications record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an electronic communications record that resides on an electronic communications server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the possession of that addressee. Systems administrators and other operators of University electronic communications resources are excluded from this definition of possession with regard to electronic communications not specifically created by or addressed to them.

Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

- **Substantiated Reason:** Reliable evidence indicating that violation of law or University policies listed in Appendix C, Policies Relating to Non-Consensual Access, probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.
- **Time-dependent, Critical Operational Circumstances:** Circumstances in which failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertinent to personal or professional activities, or to faculty research or matters of shared governance.
- **Transactional Information:** Information, including electronically gathered information, needed either to complete or identify an electronic communication. Examples include but are not limited to: electronic mail headers, summaries, addresses and addressees; records of telephone calls, and IP address logs.
- **University Administrative Record:** A University Record that is directly related to the conduct of the University's administrative business.
- **University Electronic Communications Record:** A University Record in the form of an electronic communications record, whether or not any of the electronic communications resources utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display view, read or print the electronic communications record are owned by the University. This implies that the location of the record, or the locations of its creation or use, does not change its nature (a) as a University electronic communications record for purposes of this or other University policy, and (b) as having potential problems for disclosure under the Georgia Open Records Act.

Until determined otherwise or unless it is clear from the context, any electronic communications record residing on university –owned or controlled telecommunications, video, audio, and computing facilities will be deemed to be a University electronic communications record for purposes of this Policy. This would include personal electronic communications. Consistent with the principles of least perusal and least action necessary and of legal compliance, the University must make a good faith effort to distinguish University electronic communications records from personal and other electronic communications in situations relevant to disclosures under the Georgia Open Records act and other laws, or for other applicable provisions of this Policy.

- **University Electronic Communications Systems or Resources:** Electronic communications systems or resources owned or operated by the University or any of its sub-units or provided through contracts with the University.
- **University Record:** A "public record" includes writing or other forms of recording that contain information relating to the conduct of the public's business in materials prepared, owned, used, or retained by the University regardless of physical form or characteristics. Except for certain defined situations, such University records are subject to disclosure under the Georgia Open Records Act.

In general, records held by students, including electronic communications records, are not University records unless such records exist pursuant to an employment or agent relationship the student has or has had with the University. This exemption applies only to the Georgia Open Records Act; student electronic communications records are subject to all other provisions of this Policy, whether or not the electronic communications record is a University record.

- **Use of Electronic Communications Resources:** To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic communications with the aid of electronic communications resources. An electronic Communications User is an individual who makes use of electronic communications resources.

The act of receipt of electronic communications as contrasted with actual viewing of the

record by the recipient is excluded from the definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the electronic communications record.

RESPONSIBILITIES

IMPLEMENTATION

Each unit supervisor, in coordination with the CIO, shall develop, maintain, and publish specific procedures and practices that implement this Policy, including information on accessibility of student information, authorized users, procedures for restricting or denying access, adjudication of complaints, and other matters.

INFORMATIONAL MATERIAL

Users of GCSU electronic communications resources shall be provided with instructional material based on this.

VIOLATIONS OF LAW AND POLICY

SANCTIONS OF LAW

Both federal and state law prohibits the theft or abuse of computers and other electronic resources such as electronic communications resources, systems, and services. Abuses include but are not limited to unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operations of electronic communication resources, systems, and services. The law classifies certain types of offenses as felonies.

ALLOWABLE USE

INTRODUCTION

The University encourages the use of electronic communications resources and makes them widely available to the University community. Nonetheless, the use of electronic communications resources is limited by restrictions that apply to all University property and by constraints necessary for the reliable operation of electronic communications systems and resources. The University reserves the right to deny access to its electronic communications resources when necessary to satisfy these restrictions and constraints.

The University cannot and does not wish to be the arbiter of the contents of electronic communications. The University cannot always protect users from receiving electronic communications they might find offensive.

OWNERSHIP

All data housed at the University is the property of the University and therefore the University System of Georgia (USG). This applies whether such records are in paper, digital, or other format. Electronic communications records pertaining to the administrative business of the University are considered University Records whether or not the University owns the electronic communications resources, systems or services used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or otherwise record them. Other electronic records, not owned by the USG, may also be subject to disclosure as University records under the Open Records Act, if they pertain to the business of the University.

University electronic communications resources, systems and services are the property of the University System of Georgia. These include all components of the electronic communications

physical infrastructure and any electronic communications address, number, account or other identifier associated with the University or any unit or sub-unit of the University or assigned by the University to individuals, units, sub-units, or functions.

ALLOWABLE USERS

OFFICIAL UNIVERSITY USERS

Active University students, faculty, staff, and others officially affiliated with the University including those in program, contract, or license relationships with the University, may as authorized by the Chief Information Officer (CIO), be eligible to use University electronic communications resources and services.

PROFESSIONAL PUBLIC USERS

Persons and organizations that are not official University users, but have a professionally related need may request temporary access approval from the CIO to access University electronic communications resources or services.

GENERAL PUBLIC USERS

Persons with no affiliation with the University other than to use library or computing resources may be granted limited access to web browsers and select applications with proof of identity.

TRANSIENT USERS

Users whose electronic communications merely transit University facilities as a result of network routing protocols are not considered "Users" for the purposes of this Policy. An example of a transient user would be the Peachnet access at Macon State University that is used by GCSU.

ALLOWABLE USES

NON-COMPETITION

University electronic resources shall support the mission of the University and not be in competition with commercial providers.

RESTRICTIONS

University electronic communications resources may not be used for:

- Unlawful activities;
- Commercial purposes not under the auspices of the University;
- Personal financial gain except as permitted under applicable personnel policies;
- Personal use inconsistent with acceptable uses;
- Uses that violate other University or campus policies or guidelines

REPRESENTATION

Use of the University's name and seal is regulated by University Communications. Users of electronic communications resources must abide by this statute as well as by University and campus policies on the use of the University's name, seals, and trademarks. Users of electronic

communications resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unity or sub-unit of the University unless appropriately authorized to do so.

ENDORSEMENTS

Users of electronic communications resources must abide by University and campus policies regarding endorsements. References or pointers to any non-University entity contained within the University electronic communications shall not imply University endorsement or the products or resources of that entity.

FALSE IDENTITY AND ANONYMITY

Users of University electronic communications resources shall not, either directly or by implication employ a false electronic identity (the name or electronic identification of another). However, a supervisor may direct an employee to use the supervisor's identity to transact University business for which the supervisor is responsible. In such cases an employee's use of the supervisor's electronic identity does not constitute a false identity.

A user of University electronic communications resources may use a pseudonym an alternative name or electronic identification for oneself for privacy or other reasons, so long as the pseudonym clearly does not constitute a false identity. The gcsu.edu mail address shall be the official means of communication and the only authorized e-mail address used to conduct University business. Pseudonyms or alternative names shall be approved by University Communications.

A user of University electronic communications resources may not remain anonymous except when publishing web pages and transmitting broadcasts.

INTERFERENCE

University electronic communications resources shall not be used for purposes that could reasonably be expected to directly or indirectly cause excessive strain on any electronic communications resources, or interference with others' use of electronic communications resources.

Users of electronic communications resources shall not send or forward

- Electronic chain mail letters or their equivalents in other resources.
- Spam that exploits electronic communications systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications.
- An extremely large message or send multiple electronic communications to one or more recipients to interfere with the recipient's use of electronic communications systems and resources.
- Intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications resources.

PERSONAL USE

University users of a University electronic communications facility or resource may use that resource for incidental personal purposes that, in addition to the foregoing constraints and conditions, such use does not

- Directly or indirectly interfere with the University's operation of electronic communications resources.
- Interfere with the user's employment or other obligations to the University.
- Burden the University with noticeable incremental costs. When noticeable incremental costs for personal use are incurred, users shall follow campus guidelines and procedures for

reimbursement to the University.

- Does not constitute a commercial service.

Approved contractors or vendors using University electronic resources shall reimburse the University for the use of those resources at fair value.

The Georgia Open Records Act requires the University to disclose specified public records. In response to request for such disclosure, it may be necessary to access electronic communications records that users consider to be personal allowing the Director of Legal Affairs to determine whether they are public records that are subject to disclosure.

The University is not responsible for any loss or damage incurred by an individual as a result of personal use of University electronic communications resources.

ACCESSIBILITY

All electronic communications intended to accomplish the academic and administrative tasks of the University shall be accessible to allowable users with disabilities in compliance with law and University policies. Alternate accommodations shall conform to law and University policies and guidelines.

INTELLECTUAL PROPERTY

The contents of all electronic communications shall conform to laws and Fair Use policies of the University and USG regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks. When the content and distributions of an electronic communication would exceed fair use as defined by the federal Copyright Act of 1976 or the Digital Millennium Copyright Act, or the TEACH Act, users of University electronic communications resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.

ACCESS RESTRICTION

Access to and use of University electronic communications resources or electronic communications resources, when provided is a privilege accorded at the discretion of the University. This privilege is subject to the normal conditions of acceptable use, including procedures for initiation and termination of access. In addition, access to and users of University electronic communications resources or electronic communications resources may be wholly or partially restricted or rescinded by the University without prior notice and without the knowledge or approval of the electronic communications users when required by and consistent with law. Access to resources may be restricted when there is substantial reason to believe that violation of law or University policies have taken place, when there are compelling circumstances, or under time-dependent, critical operational circumstances. Restoration of access and use under such condition is subject to established university procedures or, in the absence of such procedures, to the approval of the CIO. Service providers may, nonetheless, restrict access to or from University electronic communications systems and resources on a temporary basis as needed in Emergency Circumstances and Compelling Circumstances in order to address an emergency or prevent damage or loss.

In compliance with the Digital Millennium Copyright Act, the University reserves the right as determined by the CIO or their designee to suspend or terminate access to University electronic communications systems and resources by any user who violates copyright law.

PRIVACY AND CONFIDENTIALITY

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications in an academic setting. This policy reflects these firmly-held principles within the context of the

University's legal and operational obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of the University's business.

The University does not routinely inspect, monitor, or disclose electronic communications without the holder's consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may deny access to its electronic communications resources and may inspect, monitor, or disclose electronic communications under very stated policy considerations.

University policy prohibits University employees and others from "seeking out, using, or disclosing" personal information without authorization, and requires employees to take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties or otherwise.

University contracts with outside vendors for electronic communications resources shall explicitly reflect and be consistent with this and other University policies as well as all laws related to privacy.

ACCESS WITHOUT CONSENT

An electronic communication holder's consent shall be obtained by the University prior to any inspection, monitoring, or disclosing of the contents of University electronic communications records, in the holder's possessions, except as provided for below.

The University, after approval of the CIO, shall only permit the inspection, monitoring, or disclosure of electronic communications records without the consent of the holder of such records;

- When required by and consistent with law.
- When there is substantial reason to believe that violations of law or University policies, have taken place.
- When there are compelling circumstances.
- Under time dependant, critical operational circumstances.

When under the circumstances described above, the contents of electronic communications must be inspected, monitored, or disclosed without the holder's consent, the following shall apply:

Compelling Circumstances: The Electronic Communications Policy cites circumstances under which access to electronic communications may occur without the prior consent of the holder. The following are University policies that may all access without the holder's notification:

- University policies governing sexual or other forms of harassment.
- Certain portions of policies governing access to University records.
- Breach of the faculty code of conduct.
- Personnel policies for staff members.
- Collective bargaining agreements and memoranda of understanding.
- Policies applying to campus activities, organizations, and students.

Violations of other policies can normally be detected and investigated without requiring non-consensual access to electronic communications. On occasion, attention to possible policy violations is brought about because of the receipt by others of electronic communications. However, it is acknowledged that electronic communications can be forged, the true identity of the sender can be masked, and the apparent sender might deny authorship of the electronic communication. In such circumstances and provided there is substantiated reason that point to the identity of the sender, non-consensual access to the purported sender's electronic

communication may be authorized, but only to the lowest level of extent necessary for verifying unambiguously the identity of the sender, and only for major violations of the following policies:

- Policies governing sales of goods or services outside the University.
- Policies governing use of University material or property.
- Policies governing use of University credit, purchasing power, or facilities.
- Policies applying to campus activities, organizations, and students governing use of University properties for commercial purposes and personal financial gain.
- Policies governing provision of University mailing lists to others.
- Policies governing the reproduction of copyrighted material for teaching and research.
- Campus access guidelines for employee organizations.

Authorization: Except in emergency circumstances, such actions must be authorized in advance and in writing by the, the Chief Information Officer. This authority may not further be re-delegated. Authorization shall be limited to the lowest level of perusal of contents and the lowest level of action necessary to resolve the situation.

Emergency Circumstances: In emergency circumstances, the lowest level of perusal of contents and the lowest level of action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures.

Notification: In either case, the responsible authority or designee shall at the earliest possible opportunity that is lawful and consistent with other University policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken. The University will issue in a manner consistent with law an annual report summarizing instances of authorized or emergency non-consensual access.

Compliance with Law: Actions taken shall be in full compliance with the law and other applicable University policies. Advice of the University's Director of Legal Affairs must always be sought prior to any action involving electronic communications (a) stored on equipment not owned or housed by the University, or (b) whose consent is protected under the federal Family Educational Rights and Privacy Act of 1974.

Recourse: Review and appeal of action taken for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy, shall make initial contact with the University's Chief Information Officer.

PRIVACY PROTECTIONS AND LIMITS

PRIVACY PROTECTIONS

Personal Information: Both federal and state laws provide privacy protections for some information that identifies an individual.

Student Information: Users of electronic communications systems and resources shall not disclose information about students in violation of the federal Family Educational Rights and Privacy Act of 1974 (FERPA), and the University policies that provide guidance in meeting FERPA requirements.

Electronically Gathered Data Except where otherwise provided by law, users of University electronic communications systems and resources shall be informed whenever personally identifiable information other than transactional information will be collected and stored automatically by the system or resource. In no case shall electronic communications that contain personally identifiable information about individuals, including data collected by the use of "cookies" or otherwise automatically gathered be sold or distributed to third parties without the explicit permission of the individual. Any other distribution of such information shall be consistent with University policy.

PRIVACY LIMITS

Public Records: Records of electronic communications pertaining to the business of the University, whether or not created or recorded on University equipment, are University records subject to disclosure under the Georgia Open Records Act, other laws, or as a result of litigation.

Possession of University Records: University employees are expected to comply with any University request for copies of records in their possession that pertain to the business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on University electronic communications resources.

Unavoidable Inspection: During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmission or observe certain transactional information to ensure the proper functioning and security of University electronic communications resources and services. On these and other occasions, systems personnel might observe the contents of electronic communications. Except as provided elsewhere in University policy or by law, they are not permitted to seek out the contents or transactional information where not germane to the foregoing purposes, or disclose, or otherwise use what they have observed. Such unavoidable inspection of electronic communications is limited to the lowest level of invasive inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information, except insofar as such disclosure equates with good faith attempts to route an otherwise undeliverable electronic communication to its intended recipients.

Except as provided above, systems personnel shall not intentionally search electronic communications records or transactional information for violations of law or policy. However, as required by law or University policy, they shall report violations discovered inadvertently in the course of their duties.

Back-up Services: Operators of University electronic communications resources shall provide information about back-up procedures to users of those resources upon request.

SECURITY

The University attempts to provide secure and reliable electronic communications resources. Operator of University electronic communications resources are expected to follow sound professional practices in providing for the security of electronic communications records, data, application programs, and systems under their jurisdiction based on the guidelines provided.

SECURITY MECHANISMS

Unless otherwise authorized by other provisions of University Policy, no person shall breach or attempt to breach any security mechanisms used by the University to protect electronic communications resources or facilities, or any records or messages associated with these resources or facilities.

AUTHENTICATION

Electronic communications service providers shall maintain currency with technologies supported by the University and implement them in accordance with established policy.

AUTHORIZATION

Service providers shall implement and employ authorization technologies commensurate with the security requirements of the service, application, or system.

ENCRYPTION

Transit: Electronic communications records shall be encrypted during transit across

communications networks.

Storage: Records subject to disclosure under the Georgia Open Records Act or required to be accessible for defined periods of time to comply with policy or law shall be stored in an unencrypted format.

RECOVERY

Providers: University wide electronic communications resources shall implement recovery practices adequate to ensure rapid recovery from security intrusions and service interruptions.

AUDIT

Providers of electronic communications resources shall implement and employ cost-effective audit technologies and practices to help identify security violators and speed up recovery from security violations. The use of such audit technologies and practices shall not conflict with other provisions of University policy.

RETENTION AND ARCHIVING

RETENTION

Electronic communications records are subject to University records management policies. Electronic communications messages, logs, or records of a business or official nature shall be deleted or erased after a period of 14 days unless protected by law, policy, statute, or required for continued business operations.

ARCHIVING

Electronic communications records that have been identified as having lasting or historic value to the University shall be properly preserved by the appropriate Administrative Office or official University archivist.

BACK-UP

The University does not maintain central or distributed electronic archives of all electronic communications sent or received. Electronic communications are normally backed up, if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may incidentally at time serve the latter purpose. Operators of University electronic communications resources are not required by this policy to routinely retrieve electronic communications from such back-up facilities for individuals.

Information Technology
Campus Box 050
Milledgeville, GA 31061-0490
(478) 445-1196

Revised: 03/16/09