

SOM- Department of Obstetrics and Gynecology	TITLE: Computer Security and Data Backup	Policy: IS001
Department Guideline	Date: August 18, 2005	Rev. 0
Approvals:		
Chairman/Date	Dept. Manager/Date	

The URL for this policy is: <http://www.mcg.edu/Policies/2406.html>

Who is responsible for my PC backup?

Each employee is responsible for backing up data which is stored on their local workstations. Backups should be performed on a routine basis and clearly identified as to the date and type of data being backed up.

If clinical or patient information is backed up this information must be stored in a secured area to comply with HIPPA regulations.

Student and Resident data must also be stored in a secure area to not allow public or open access to records that should be highly confidential.

*Medical College of Georgia Administrative Policies and Procedures
Office of Primary Responsibility: Information Technology Support and Services
No. 2.4.06*

Information Systems Security and Computer Usage

The Medical College of Georgia Information Systems Security and Computer Usage Policy is to be used in conjunction with existing MCG policies and procedures. Each individual is responsible for the appropriate use and protection of information systems resources. Each manager/supervisor is responsible for appropriate enforcement of the policy in conjunction with normal supervisory activities.

1.0 PURPOSE

The purpose of this policy is to ensure that information systems resources are used in an appropriate and responsible manner consistent with the mission of the institution, and that the use of these resources is in accordance with MCG policies, procedures, federal and state law.

2.0 SCOPE

This policy applies to all information systems resources which includes all data and hardware regardless of media, the facilities containing them, and the supporting software and hardware including host computer systems, workstations, systems software, application software, datasets and communications networks either direct or remote that are controlled, administered or accessed by MCG students, faculty, employees, visitors or any other person accessing from on-campus as well as off-campus.

3.0 STATEMENT OF POLICY

The appropriate use and protection of all information systems and associated resources is expected from all users including faculty, students, employees, and visitors throughout

the institution. "Appropriate use" of information systems resources is defined as use which is for the purpose of furthering the mission of MCG.

All users of information systems resources are expected to comply with existing MCG Policies and Procedures and those of the University System. In addition, users are expected to honor copyrights and software licenses and comply with all federal and state laws including those prohibiting slander, libel, harassment and obscenity. Users must obey laws prohibiting the private use of state property. Information that is confidential by law, including educational and medical records must be protected.

Users must be aware that information stored or transmitted electronically (or via computer), including e-mail, may be subject to disclosure under open records laws. Users should have no expectation of privacy for information stored or transmitted using MCG information resources except for records or other information that is confidential by law (i.e., medical and educational records).

Information systems resources are to be used as expressly authorized by MCG administration and management.

The information systems user is responsible for the general protection of resources.

4.0 GENERAL RESPONSIBILITIES

4.1 Resource Owner

The owner of each information system resource is the manager or administrator most closely fitting the role of "natural responsibility." The resource owner of enterprise wide information systems will be declared by the appropriate steering committee or their designee during the procurement or development process. The owner is the person or group responsible for analyzing the value of the resource and its security classification. The owner specifies controls and authorizes data usage. Department heads will assume the role of owner for their department's data or will appoint a security administrator or coordinator. It is explicitly noted however that the patient is the owner of clinical data no matter where the data resides at MCG.

The responsibilities of the owner include:

- Declare ownership.
- Determine the sensitivity of the resource and classify it.
- Determine applicable issues related to law, accreditation, etc.
- Determine who should have access to the data.
- Determine the appropriate level of physical access security.
- Determine the appropriate level of logical access security.
- Mandate to the custodian or customer/client to use "virus protection software" where appropriate.
- Specify any additional security controls and communicate them to the custodian.
- Determine the requirements for business contingencies.
- Determine record retention requirements.
- Review access activities pertaining to the resource.

4.2 Custodian

The custodian is the person or group responsible for control and protection of the resource. The custodian administers owner-specified business and asset protection controls for information and data in custody. The custodian provides appropriate physical security for any hardware, software and data in custody. The custodian provides appropriate access security for any information systems resource in custody. Based on the owner's recommendation, the custodian is required to implement the appropriate level of physical access security and logical access security for those authorized to access the system and to maintain records of access privileges. The custodian provides security from other threats where appropriate and must include the use of "virus protection software". The custodian of the MCG information systems resource must obtain permission from the owner to access, copy or modify the resource in any way. The ability to access, copy or modify does not imply permission to do so.

MCG is the custodian of clinical data.

4.3 Customer/Client

The customer/client is the person who, upon authorization, uses the resource as required by assigned job function.

The customer/client is required to:

- Treat information and associated resources as valuable assets.
- Use MCG information systems only for lawful and authorized purposes.
- Observe policies and procedures as defined by management and administration.
- Protect the resource from physical or environmental compromise.
- Protect the area from unauthorized access.
- Protect passwords.
- Protect the software and files in custody from compromise.
- Use only authorized software.
- Lock up storage media containing sensitive data.
- Back up personal files and individual software.
- Report security violations.
- Recognize accountability for improper use of information systems resources.

5.0 ACCESS CONTROLS

Access to information resources at MCG is based on "least privilege" authorization by duties and "need to know". Access must be protected at a level commensurate with its classification.

5.1 Security Classification Categories

5.1.1 Patient/Student

Patient and student oriented data are considered to be of the highest classification and therefore must be afforded the highest level of protection. Improper release of or access to these data could violate the individual's legal right to privacy under Federal or State law.

5.1.2 Sensitive Administrative

Sensitive administrative data is considered to be the next highest level of classification. Data in this category includes such items as personnel, grant and payroll information, office memoranda containing information considered confidential, and other similar information. Any manipulation of data affecting official records of the institution causes the subject data to fall into this category. Publicly accessible information subject to the "Georgia Open Records Act" must be accessed through the appropriate measures to ensure accuracy.

5.1.3 Functional Administrative

Administrative information resources such as support service reports, statistical data, records documentation, appointment schedules, routine office memoranda and other related information used to help job functions must be afforded at least a moderate level of protection. This information may have some restrictions for viewing but in any case must be protected since misuse of this type of information resource could result in loss of efficiency to the organization across departmental boundaries.

5.1.4 Other

Other information resources although possibly open for public view must still be afforded some protection from loss or damage due to the investment in resources used to create it within the department. Training materials, employee guidelines, etc. could fall into this category.

5.2 Logical Security

The appropriate level of logical access security is to be designed into the system and implemented in accordance with the level of need. Logical security refers to any programmatic controls including authorization by user-id and passwords, limiting access attempts, inactivity sign-off's, transaction journals, imbedded codes for auditing and tracking, limiting functionality by assignment, etc.

5.3 Physical Security

Many "physical security" controls such as protection from fire or other hazards are covered in other MCG policies and procedures regarding basic safety. The Medical College of Georgia requires new employees to complete a "Safety Awareness" training session as part of new employee orientation. A "Safety Guide" is published and is available from the personnel department.

6.0 RISK ASSESSMENT

The designated resource owner must decide to what degree potential losses will be insured against or controls adjusted to reduce the potential for loss.

6.1 Threats

The designated resource owner is responsible to determine what level of protection must be implemented regarding various risks such as:

- Errors and omissions
- Carelessness
- Vandalism to hardware or software, including data
- Disgruntled employees
- Damage to facility or infrastructure

- Theft
- Unauthorized use of resources
- "Viruses" or other external malicious code resulting from unauthorized software use
- Unauthorized alteration or manipulation of programs and data
- Invasion of privacy (especially student or patient data)

6.2 Backup/Recovery

All information systems data and software components must be backed up at a frequency commensurate with their security classification level. Redundancy and off site storage must be considered for the highest level of protection. ISD Operations is responsible for ensuring appropriate backup and recovery procedures are in place for all central host files. The Departmental System Administrator is responsible for ensuring appropriate backup and recovery procedures are in place for all departmental system files. The custodian of each personal computing workstation is responsible to maintain proper backups for software and data loaded on internal media.

6.3 Business Contingency

The resource owner is required to develop a business contingency plan based on loss of resource due to disaster or other unexpected circumstance.

6.4 Disaster Recovery

The departments and ISD are responsible to coordinate efforts to ensure disaster recovery procedures are in place. The resource owner must identify critical resources to be protected.

6.5 Archival

The resource owner is required to specify archive requirements at the time of system development.

7.0 AWARENESS

It is the responsibility of each manager/administrator supervising information systems access to determine the amount of awareness necessary to properly protect the resource involved.

8.0 HARASSMENT

No member of the community may, under any circumstances, use The Medical College of Georgia computers or networks to libel, slander, or harass any other person.

The following shall constitute computer harassment:

Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of harm to the recipient or the recipient's immediate family.

Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.

Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection).

Intentionally using the computer to disrupt or damage the academic, research, administrative, clinical or related pursuits of another.

Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

9.0 TRAINING

The ISD Customer Service Representative will contact System Administrators to set up in-house training. The associated department manager/administrators are responsible for setting up any additional special or outside training.

10.0 AUDITING

Internal and external periodic audits must be performed where appropriate to ensure adequacy of controls and compliance with such controls. The associated department manager/administrator will be notified in writing of audit results.

11.0 BREACH OF SECURITY

Suspected breach of security, based on the level of severity, should be reported to the appropriate resource owner and/or the MCG Chief Information Officer who are responsible to determine the best course of action to correct the situation and protect against future occurrences. Certain extreme cases may involve additional levels of review and could call for disciplinary action, up to and including dismissal, or civil or criminal penalties.

12.0 COMPLIANCE

MCG maintains the authority to impose sanctions and punishment on anyone who violates this policy. Any violation of federal or state law may be reported to the proper authority.