Data Security Policy

I. POLICY

Institutional data is information that supports the mission of County College of Morris. It is a vital asset and is owned by the College. Institutional data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth the college's standards with regard to the handling and safeguarding of institutional data.

II. PURPOSE

To establish policy for the safeguarding of restricted and sensitive data relating to students and CCM personnel that is created, received, maintained or transmitted by the College. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all college policies and applicable state and federal laws. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.

III. DEFINITIONS

A. Archiving/Storage: The act of physically or electronically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.

B. Institutional Data: Institutional data is information that supports the mission of County College of Morris. It is a vital asset and is owned by the College. Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with established institutional policies and practices. Sensitive Data as defined in this section is a subset of Institutional Data.

C. Authorized User: Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include, but are not limited to faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of the college.

D. Electronic Media: All media on which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs and USB storage devices.

E. Electronic Messaging: A set of communication processes used to relay information among the users of computers. Electronic Messages take many forms. Examples: Electronic Mail (Email), FTP, cell phones, Instant Messaging and internet chat.

F. Restricted Data: Data whose access is restricted by federal or state statute (i.e. HIPAA, FERPA). For purposes of this policy, restricted data is a subset of sensitive data.

G. Sensitive Data: Data, regardless of its physical form or characteristics, with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination. Examples include: passwords, intellectual property, on-going legal investigations, medical or grades

information protected by FERPA or HIPAA, social security numbers, birth dates, professional research, student work, bank or credit card account numbers, income and credit history.

IV. DATA COLLECTION

A. Users should collect only the minimum necessary institutional/sensitive information required to perform college business.

B. Department heads must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with college policy and procedure.

V. DATA ACCESS

A. Only authorized users may access, or attempt to access, sensitive information.

B. Authorization for access to sensitive data must be authorized by the department head, and is typically granted in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other official authority.

C. Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform college business.

D. Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

E. Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the CCM Information Systems department.

VI. DATA HANDLING AND DATA TRANSFER

A. Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.

B. Sensitive data must be protected from unintended access by unauthorized users. Users must guard against unauthorized viewing of such information which is displayed on the user's computer screen. Users must not leave sensitive information unattended and accessible.

C. Sensitive information must not be taken off campus unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.

D. Sensitive data should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.

E. Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive or laptop.

VII. STORAGE OF SENSITIVE DATA

A. Physical protection must be employed for all devices storing sensitive data. This shall include physical access controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be

locked and any easily transportable devices should be secured in locked cabinets or drawers.

B. Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the College.

C. Information Systems managed servers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed up.

D. Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.

E. It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system should be stored on a network drive hosted on a Information Systems managed server.

F. Electronic media storing restricted/sensitive data must be protected by password security. To the extent possible, these devices must employ encryption methods.

VIII. DATA RETENTION AND DISPOSAL

A. **Retention of Records Containing Restricted and Sensitive Data:** A "schedule" describing the records and the official retention period is required by the State of New Jersey for each type of record created or maintained by a public institution. The County College of Morris uses the following guidelines and statutory procedures for records retention.

1. State of New Jersey "County Community Colleges General Records Retention Disposition Schedule".
2. New Jersey Permanent Statute Title 47 (Public Record Law).

B. **Archiving**: Institutional records, including sensitive information records, which are no longer being used for active college business, are to be archived until retention requirements have been met.

1. Departments determine the criteria for inactive record status in their areas, based upon need for the records, available storage space, and public law.
2. All inactive records are to be sent to the Records Management Department for storage in the College Records Archive until their legal retention requirements have been met in a controlled environment protected against unauthorized access, damage, and loss.
3. Only primary (original records) are to be archived. Duplicates (copies) of records should be destroyed.

C. **Records Disposal:** The proper destruction of public records is essential. All official public records shall be destroyed once their retention period has expired. This pertains to the destruction of paper records as well as those that are microfilmed, imaged or are electronic. No records that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.

1. The destruction of all official college records is coordinated through the Records Management Department. No individual employee of the College shall destroy, purge or discard any official college public record.
2. The authorized methods of destruction for non-electronic records are burning where authorized or shredding. The authorized methods of

destruction for electronic records are wiping utilizing the US Department of Defense standard for cleaning and sanitizing electronic media, DOD 5220.22M, or physical destruction of the electronic media

IX. RESPONSIBILITY

A. **Supervisory Personnel**: Every County College of Morris employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for the following:

- Communicating this policy to personnel under their supervision.
- Ensuring that appropriate security practices, consistent with the data handling requirements in this policy are used to protect institutional data.
- Providing education and training in data management principles to employees under their supervision.

B. User **Responsibilities**: Users who are authorized to obtain institutional data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

- Access institutional/sensitive data only in their conduct of college business.
- Request only the minimum necessary confidential/sensitive information necessary to perform college business
- Respect the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to data to which they have access.
- Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

X. COMPLIANCE

Compliance with this data protection policy is the responsibility of all members of the County College of Morris community. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to CCM's information technology resources during investigation of an alleged abuse. Violations may also be subject to prosecution by state and federal authorities.