

## Data Security Policy

### I. POLICY

Institutional data is vital to support the mission of the County College of Morris and is an asset owned and maintained by the institution. The data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements.

This administrative policy sets forth the County College of Morris's standards regarding the handling and safeguarding of institutional and/or sensitive data regardless of storage location or device, this includes both on-premises and off-premises locations.

### II. PURPOSE

To establish policy for the safeguarding of restricted and sensitive data 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, applicable state laws and federal laws, and the European GDPR policy. 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 Institutional data to a storage location until the record retention requirements are met or until the records are needed again.
- B. Institutional Data: is information used by the County College of Morris for legitimate business purposes. This data can include sensitive and/or restricted data, student records, and all data required for legitimate business purposes.
- C. Authorized Users (Users): Individuals who have been granted access information in the performance of their assigned duties. Users include, but are not limited to faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of the college.
- D. Use of Data: Authorized users may have access to the data for the purpose of conducting their job duties but may not have the authority to extrapolate additional meanings from the data and make conclusions based on said data, or share data with others on and off campus, that do not pertain to their job functions.
- E. Electronic Media: All media and devices where electronic data can be stored, including, but not limited to, hard drives, magnetic tapes, diskettes, CDs, DVDs, USB storage devices, cell phones, cloud applications, and any/all other devices not listed.

- F. Electronic Messaging: A set of communication processes and tools used to relay information. Some examples are: Electronic Mail (Email), File Transfer Protocol (FTP), cell phones, handheld devices, Instant Messaging, internet chat, and other software used for communication or data transfers.
- G. Restricted Data: Data whose access is restricted or regulated by federal or state statute, e.g., HIPAA, FERPA. For purposes of this policy, restricted data is a subset of sensitive data.
- H. Sensitive Data: Data, regardless of its physical form or characteristics, the County College of Morris has determined it requires the highest level of protection, e.g., 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, grades, social security numbers, birth dates, professional research, student work, bank or credit card account numbers, income and credit history.
- I. Public Data: information that has been declared public in accordance with the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1, et seq. (“OPRA”), or by someone else who is duly authorized by the College to do so, and thus may be freely distributed. The disclosure, unauthorized access, or unauthorized use of public information would not adversely impact the College, its students or staff, the state, and/or the public. Accordingly, information made public in official College publications or on the public facing County College of Morris website may be released without special authorization.
- J. Internal Data: information that is available to College employees with a legitimate educational or business interest in them to be used for official purposes but would not be released to the public unless requested pursuant to and authorized by County College of Morris business practices, consistent with applicable law.
- K. Cloud Storage: Storage hosted in the cloud via a third-party provider. Examples include Microsoft 365, Amazon S3, and Google Cloud Storage.
- L. VDI: Virtual Desktop Infrastructure that consists of on-premises servers hosting virtual sessions for end users to access the necessary software and systems to perform job related activities.
- M. Data Trustees: Senior College officials or their designees with planning and management responsibility for defined segments of institutional data within their functional areas.
- N. Data Stewards: College officials having direct operational-level responsibility for the management of one or more types of institutional data.
- O. Data Custodians: Computer system administrators responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data.
- P. Data Users: College units or individuals who have been granted access to institutional data in order to perform assigned duties.

#### IV. DATA COLLECTION

- A. Users should collect only the minimum necessary institutional/ sensitive information required to perform college business.
- B. Department heads (Data Custodian or Data Steward) must ensure that all decisions regarding the collection and use of institutional data are following any federal and state laws, and with college policy and procedures.
- C. Data Stewards and Data Custodians are responsible for identifying and implementing safeguards for Restricted Data based on information security best practices, applicable law, industry standards and College policy, while working in cooperation with the IT Security Officer and other appropriate individuals in the Division of Information Technology Services.

#### 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 Vice President (Data Trustees). This is granted in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other institutional authority.
- C. 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 Department of Information Systems.
- F. Multi Factor Authentication should be used whenever critical systems containing sensitive data are accessed.
- G. Access shall be deactivated after a period of inactivity, not to exceed twelve (12) months.
- H. Separated employees shall lose access as of their separation date.
- I. Data access processes, procedures, and authorizations must be reviewed on an annual basis by each Data Steward to ensure that only those approved are accessing the data as authorized.
- J. Data Trustees, Data Stewards, Data Custodians or specific College units may have additional procedures for institutional data within their areas of operational or administrative control.

## VI. DATA HANDLING AND DATA TRANSFER

- A. Sensitive data must be protected from unintended access by unauthorized users.
- B. Users must guard against unauthorized viewing of such sensitive and restricted information. Users must not leave sensitive information unattended and/or accessible.
- C. Sensitive information must not be taken off campus or electronically distributed 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 or by any other digital interface even to other authorized users unless security methods, such as encryption, are employed.
- E. Users must take all appropriate measures to ensure physical protection from theft, loss, and damage regardless of the device and ownership. Some examples are: smart phone, PDA, notepad, thumb drive or laptop.
- F. Breaches, losses, or unauthorized exposures of restricted data must be immediately reported to the Executive Vice President, of Business and Finance and handled in accordance with College policy and procedures related to disclosure or exposure of personal information, as well as legal requirements imposed upon the College in the event of such disclosures.
- G. Loss or theft of College computer equipment or mobile devices must also be reported to the Office of Security and Safety. College community members must also report actual or suspected criminal activity associated with any such incident to the Office of Public Safety, or, if off campus, other appropriate law enforcement agencies.
- H. E-Mail is not a secure means to deliver information and consequently should not be used to transmit restricted data without proper encryption, passwords, or other security measures.

## VII. STORAGE OF SENSITIVE DATA

- A. Physical protection must be employed for all devices storing sensitive data. This includes physical access controls that limit physical access and viewing. User's office, labs, or work locations must be locked and any portable electronic media devices should be secured in locked cabinets or drawers.
- B. Users of laptops and other mobile computing devices need to ensure appropriate steps are taken to always protect the physical security of the device, especially when working remotely or traveling.
- C. The Director of Network and User Services & Chief Information Security Officer is responsible for overall management of the security on servers storing confidential information. The servers shall be regularly scanned for security 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. Institutional data shall not be stored on PCs, laptops or mobile devices regardless of their physical location. Institutional data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system must be stored on the college's VDI system, a network drive hosted on a server managed by the Department of Information Systems, or a cloud storage resource approved by the college.
- 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 newer version, 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 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:
1. Communicating this policy to personnel under their supervision.
  2. Ensuring that appropriate security practices consistent with the data handling requirements in this policy are used to protect institutional data.
  3. Providing education and training in data management principles to employees under their supervision.
- B. All CCM employees, regardless of their position within the institution, have a responsibility to safeguard sensitive and restricted information. It should be noted that the sensitivity level definitions were created as guidelines, and to emphasize reasonable steps that can be taken to emphasize reasonable steps that can be taken to secure personally identifiable information.
- C. User Responsibilities: Users who are authorized to obtain institutional data must ensure that it is protected to the extent required by law or policy. All data users are expected to:
1. Access institutional/sensitive data only in their conduct of college business.
  2. Request only the minimum necessary confidential/sensitive information necessary to perform college business.
  3. Respect the confidentiality and privacy of individuals whose records they may access.
  4. Observe any ethical restrictions that apply to the data they have accessed.
  5. 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.