MONTCLAIR STATE UNIVERSITY

Responsible Use of University Computing Resources Policy Document

# *Data Classification and Handling*
# *(Safeguarding Sensitive and Confidential Information)*

## 1.0 Purpose

In the course of their routine work related activities, members of the University community will encounter sensitive and confidential information regarding other individuals, institutions and organizations. This policy establishes specific requirements for the proper classification and handling of sensitive and confidential information by members of the Montclair State University community in order to ensure that the University maintains strict confidentiality in compliance with applicable requirements and regulations of the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA) of 1974 as amended, the Health Insurance Portability and Accountability Act (HIPAA), and other applicable federal and state privacy laws. Additionally, the Policy for Safeguarding Sensitive and Confidential Information is intended to help members of the University community determine what information can be disclosed to non-employees and how, as well as the relative sensitivity of information that should not be disclosed within or outside of Montclair State University without proper authorization.

## 2.0 Scope

This policy pertains to the security and privacy of all non-public information including student information, employee information, constituent information and general University information whether it is in hard copy or electronic form. Accordingly, documents that include sensitive and confidential information such as social security numbers, dates of birth, student education records, medical information, benefits information, compensation, loans, or financial aid data, and faculty and staff evaluations need to be secured during printing, transmission (including by fax), copying, storage and disposal.
The information covered in this policy includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All University employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to secure personally identifiable information and Montclair State University Confidential information. Questions about the proper classification of a specific piece of information should be addressed to your Dean or direct supervisor. Questions about this policy document should be addressed to the Information Technology Division.

## 3.0 Sensitivity Classification of Information Assets

All Montclair State University information that is stored, processed or transmitted by any means shall be classified into one of four levels of sensitivity: Public, Internal, Confidential and Private. The sensitivity classification identifies information in terms of what it is and how access, processing, communications and storage must be controlled. If more than one sensitivity level could apply to the information the highest level (most restrictive) will be selected.

Note: A sensitivity classification shall attach to and follow the information to which it applies until such time that the classification is changed by the Data Owner/Custodian (see Glossary)

1. **Public** – (least restrictive) Information that has been declared public knowledge by University Counsel in response to a request for records under 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 University to do so, and thus may be freely distributed. The disclosure, unauthorized access, or unauthorized use of Public information would not adversely impact the University, its students or staff, the state, and/or the public. Accordingly, information made public in official University publications or on the public facing Montclair State website may be released without special authorization.

Examples of **Public** information include:

- Board of Trustees actions
- Faculty/staff bios
- Course catalogs
- Press releases and marketing materials
- Email sent to campus wide distribution lists, unless otherwise stated in the email communication
- NetIDs or email addresses (*without* corresponding password)
- Student directory information, unless a student has requested such information not otherwise be disclosed.

Sensitive information is defined by Montclair State University as any information that has not otherwise been expressly declared as Public information. Sensitive information is categorized as either **Internal**, **Confidential**, or **Private**, with corresponding increased levels of sensitivity and restrictions imposed on its handling and distribution. It is understood that some information classified as Internal/Confidential/Private may be more critical than others, and should be protected in a more secure manner in accordance with the categories identified below.

2. **Internal** – Information that is available to University 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 Montclair State business practices, consistent with applicable law. The disclosure, unauthorized access, or unauthorized use of internal information would have a limited adverse impact on the University, the State, and/or the public.

Examples of **Internal** information include:

- Financial accounting information
- Department project data such as construction plans that do not impact University security
- Unit budgets
- Purchase Orders

- Admissions metrics and statistics
- Donor contact information and non-public gift amounts
- Non-public Montclair State policies and policy manuals
- Montclair State internal memos and email, non-public reports, budgets, plans, and financial information
- Non-public contracts
- Campus Wide ID's (CWIDs) (*without* corresponding PIN or date of birth)

3. **Confidential** – Information of a sensitive nature that is available only to designated personnel or third parties with a legitimate business or educational interest in them. The disclosure, unauthorized access, or unauthorized use of confidential information would have a significant adverse impact on the University, the State and/or the public. Confidential information is information that is not available to the public under all applicable State and Federal laws, including but not limited to OPRA, the Family Educational Right to Privacy Act ("FERPA") and the Health Insurance Portability and Accountability Act ("HIPAA")

Examples of **Confidential** information include:

- Medical examiner and other non-PHI medical records
- Passport and visa numbers
- Export controlled information under U.S. laws
- Criminal investigations, Campus Police records and evidentiary materials
- Advisory, consultative or deliberative material
- Victims records
- Trade secrets and proprietary commercial or financial information obtained from any source, or information that is the subject of a non-disclosure agreement with the University.
- Documents subject to attorney client privilege
- Administrative or technical information regarding computer hardware, software and networks which would jeopardize computer security
- Emergency or security information for any building that would jeopardize security of the building or persons therein
- Security measures and surveillance techniques
- Information that would give an advantage to competitors or bidders
- Sexual harassment complaints and investigations
- Grievances filed
- Collective bargaining negotiations
- Communications with insurance carriers or risk management officers
- Information required to be kept confidential by court order
- Social security numbers, credit card numbers, unlisted telephone numbers, and driver's license numbers
- Certain pedagogical, scholarly and/or academic research records
- Test questions, scoring and other examination data
- Charitable contributions
- Admission applications
- Student records, grievance or disciplinary proceedings
- Biotechnology trade secrets
- Personnel and pension records
- Student records other than directory information

4. **Private** – (most restrictive) All personally identifiable information (PII) pertaining to individuals that is protected by Federal or State law shall be Private. The disclosure, unauthorized access, or unauthorized use of Private information would have a significant adverse effect on the University, the State and the individuals whose information was disclosed. Exposure of certain Private information may require the University to report such exposure to various Federal and State agencies and/or Financial institutions as well as the individuals whose information was exposed.

Examples of **Private** information include:

- Social Security numbers
- Health Information, including Protected Health Information (PHI) and any data covered under the Health Insurance Portability and Accountability Act (HIPAA)
- Credit card account number, or debit card number and any required security code, access code, or password that would permit access to an individual's financial account (e.g. other Cardholder data)
- Personal financial information, including checking or investment account numbers
- Driver's License numbers
- Health Insurance Policy ID Numbers
- Unlisted telephone numbers
- Student directory information that a student has requested not to be disclosed
- Student and employee ID numbers (CWIDs) combined with PINs and/or birth dates
- NetID usernames or other account names combined with unencrypted password string

## 4.0 Handling and Distribution of Information Assets

Many employees generate or are exposed to sensitive University information and personally identifiable information (PII) in the course of their jobs and use it to perform important functions. It is vitally important that all employees handle such information properly. Often, such information contains personally identifiable data that places individuals at risk of identity theft. It may also contain proprietary information, research findings or other intellectual property.

Access to non-public, sensitive information is restricted to those who have a need to know as defined by job duties and access is subject to University authorized approval. Anyone who receives non-public sensitive information has a responsibility to maintain and safeguard that information and to use it with consideration of that regard for others. Circumventing or attempting to circumvent restrictions on the use and dissemination of internal, confidential, or private information is considered a serious offense and may be subject to discipline. If such information is received in error, the recipient has an obligation to alert the sender that they have received this information in error, and to properly delete and or destroy the received copy of the information.

The release or exchange of individual or University information may only be made by University employees in accordance with the guidelines outlined below. University employees and students may not divulge information regarding the University to an outside party except for a legitimate business, research, or academic purpose. If information about the University has not been made public by the University, it should continue to be treated as sensitive.

In general, Montclair State University personnel are expected to use common sense judgment and to handle data categorized as Internal, Confidential, and Private in an appropriate manner. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should consider it **Private** by default and contact their Vice President, Dean or their designee, or direct supervisor for clarification before taking any action with regard to the information in question.

The guidelines that follow provide details on how to properly handle and/or distribute information with varying degrees of sensitivity, including acceptable electronic transfer and storage methods. Where applicable, disposal guidelines are given as well as the scope of potential penalty for deliberate or inadvertent disclosure.

Please note that these guidelines represent the most common use cases for the handling and distribution of University data and should be used as a reference only. Information in each category may necessitate more or less stringent measures of protection depending upon the specific circumstances and the nature of the information in question.

## Public information

There are no specific restrictions on the distribution or handling of public information, although University personnel must respect all copyright, trademark and intellectual property rights of any data that they distribute.

**Access:** Anyone

**Distribution within Montclair State University:** No restrictions

**Distribution outside of Montclair State University**: No restrictions

**Storage:** No restrictions

**Disposal/Destruction:** Not applicable

**Penalty for deliberate or inadvertent disclosure:** None

## Internal information

Internal information is considered non-public and should be protected from unnecessary exposure or transmission to parties outside of the University.

**Access**: Montclair State University employees, or non-employees with signed non-disclosure agreements, who have a legitimate business or academic need to know.

**Distribution within Montclair State University:** Standard interoffice mail, campus email, password-protected web site, or campus file sharing repositories.

**Distribution outside of Montclair State University**: encrypted email, password-protected file, password-protected web site to retrieve encrypted file, secure electronic file transmission with file encryption.

**Storage:** Hardcopy must be stored in a physically secure area (i.e. locked file cabinet) Information may only be stored electronically on University-owned and maintained computers or on a remote site such as a cloud storage provider that is under contract with the University for such services. Regardless of physical storage location, it is recommended  that files containing information classified as Internal be stored in an encrypted format. Acceptable forms of encryption are password protected files (i.e. Microsoft Office password protection) or a public/private key algorithm such as PGP or GnuPG.)

**Disposal/Destruction:** Shred hardcopy; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

**Penalty for deliberate or inadvertent disclosure:** Up to and including termination of employment, possible civil and/or criminal prosecution.

## Confidential information

Confidential information should be protected to prevent unauthorized access or exposure.

**Access:** Montclair State University employees whose job functions require them to have and are approved by their supervisor to have access, and University vendors or consultants who have executed non-disclosure agreements with the University.

**Distribution within Montclair State University:** Delivered direct - signature required, envelopes stamped confidential. Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm such as PGP or GnuPG or be password-protected at the application level (i.e. signed PDF or Word document.) The encrypted/password-protected files can then be sent via email and/or secure electronic file transmission.

**Distribution outside of Montclair State University:** Delivered direct; signature required; approved private carriers. Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm such as PGP or GnuPG or be password-protected at the application level (i.e. signed PDF or Word document.) The encrypted/password-protected files can then be sent via email and/or secure electronic file transmission. Third parties who are handling and/or storing Confidential information must agree to abide by the University's policies for safeguarding such information.

**Storage:** Hardcopies must be limited to the minimum number required. Hardcopies must be stored in a secure location at all times. Unless there is a critical business need, no portion of Confidential information should be stored locally on employee desktop or laptop computers beyond the Office of University Counsel. Confidential information may be stored on a University owned file server, central computing server, or on a remote site such as a cloud storage provider that is under contract with the University for such services. Regardless of physical storage location, confidential files must be stored in an encrypted format. Acceptable forms of encryption are password protected files (i.e. Microsoft Office password protection), and encrypted hard disk or folder, or a public/private key algorithm such as PGP or GnuPG.)

**Disposal/Destruction:** All hardcopy must be cross-cut shredded and disposed of in specially marked disposal bins on Montclair State University premises; electronic data should be expunged/cleared with a data scrubbing utility to ensure that portions of the original data cannot be reconstructed from the hard drive or other electronic storage medium.

**Penalty for deliberate or inadvertent disclosure:** Up to and including termination of employment, possible civil and/or criminal prosecution.

## Private information

Private information has the highest level of sensitivity and represents the most risk to the University, the State, and individuals should such information be accessed by or exposed to unauthorized parties. Therefore, University employees who handle Private information or who use systems that store, transmit, or manipulate Private data are required to maintain the privacy of such information/data at all times.

**Access:** Montclair State University employees whose job functions require them to have and are approved by their supervisors to have access, and University vendors or consultants who have executed non-disclosure agreements with the University.

**Distribution within Montclair State University:** Delivered direct - signature required, envelopes stamped Private. Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm such as PGP or GnuPG. The encrypted/password-protected files can then be stored on a central IT file server such as MSUFiles and access granted to authorized individuals using NetID group share permissions. Alternatively, secure temporary file storage with email notification to authorized users via the MSU FileHawk service may be used to provide access to Private information. Private information should not be sent via email attachment unless there is no other viable transmission method, and then only if the email message and any attachments are encrypted per-recipient using PGP or GnuPG. Password-protecting a file at the application level (ex. PDF or Word document) is not sufficient protection for Private information.

**Distribution outside of Montclair State University:** Delivered direct; signature required; approved private carriers. Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm such as PGP or GnuPG before transmission to an authorized entity outside of the University. File transmission of encrypted data should occur using a secure protocol such as SFTP, HTTPS, or SSH. Alternatively, secure temporary file storage with email notification to authorized users via the MSU FileHawk service may be used to provide access to Private information. Private information should not be sent via email attachment unless there is no other viable transmission method, and then only if the email message and any attachments are encrypted per-recipient using PGP or GnuPG. Password-protecting a file at the application level (ex. PDF or Word document) is not sufficient protection for Private information.

**Storage:** Hardcopies must be limited to the minimum number required. Hardcopies must be stored in a secure location at all times. No Private information may be stored locally on employee desktop or laptop computers, tablet, phone, or on any non-University device. Instead, Private information must be stored on a University owned file server, central computing server,or on a remote site such as a cloud storage provider that is under contract with the University for such services. Regardless of physical storage location, files containing Private information must be stored in an encrypted format. Acceptable forms of encryption include an encrypted hard disk or folder or a public/private key algorithm such as PGP or GnuPG. Password-protecting a file at the application level (ex. PDF or Word document) is not sufficient protection for Private information.

**Disposal/Destruction:** All hardcopy must be cross-cut shredded and disposed of in specially marked disposal bins on Montclair State University premises; electronic data should be expunged/cleared with a data scrubbing utility to ensure that portions of the original data cannot be reconstructed from the hard drive or other electronic storage medium.

**Penalty for deliberate or inadvertent disclosure:** Up to and including termination of employment, possible civil and/or criminal prosecution.

## 5.0 Guidelines for Protecting Information Stored Electronically

All employees and users of networked computing devices on Montclair's network are responsible for protecting the University's information because their machines provide potential gateways to private information stored elsewhere on the network. Therefore, whether or not they deal directly with sensitive University information, employees should take the following steps to reduce risk of unauthorized disclosure of the University's information:

- Familiarize yourself with all University computing and security policies and Social Media Policy, and understand their implications for the information for which you are responsible.
- Immediately advise your supervisor of any suspicious activity on your computer or a suspected information system security compromise and report the event to the University Help Desk for follow-up action.
- Be mindful of how you are sharing or transmitting sensitive information across the network.
- Do not share sensitive information via unencrypted/unsigned email. Unencrypted and unsigned email is not secure; it can be forged, and it does not afford privacy.
- Do not publish sensitive information to unsecured web sites. All sensitive information on web sites must be encrypted and password protected.
- Do not collect Confidential or Private information with web forms that are not secured via https connection with a valid SSL certificate.
- Be certain your machine is always protected from viruses and other malware. Install anti-virus software on your computer and ensure that the software is set to automatically update its virus definitions regularly. (the Information Technology Division distributes the Sophos Antivirus tool at no charge. Please contact the University Help Desk for more information)
- Take precautions not to send anything by e-mail that you wouldn't want disclosed to unknown parties. Recipients have been known to distribute information to unauthorized recipients or store it on unsecured machines, and viruses have been known to distribute archived e-mail messages to unintended recipients.
- Theft of Montclair State electronic computing equipment must be immediately reported to the University's Police Department; loss or suspected compromise of Montclair State sensitive data must be immediately reported to the Security Official within the Information Technology Division or the University Compliance Officer, or the University Privacy Officer, as applicable.
- Ensure that functions that enable data sharing on an individual workstation are either turned off or set to allow access only to authorized personnel.
- Be aware that information stored on laptop computers, tablets, smart phones and other similar mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure. Even networks using encryption are vulnerable to intruders.
- Information that is categorized as Confidential or Private shall not be stored on a personal laptop, desktop, tablet, phone, or other end-user device.
- Confidential and Private information should only be stored on centrally-managed IT servers or on a cloud service provider with whom the University has a contractual relationship for such service.
- Employ passwords that comply with the University's Password Management Policy.

- Secure your passwords, and restrict access to them. Passwords written on a post-it in a work area, placed under a keyboard, or stored in an unlocked desk drawer are not safe from unauthorized access.
- Never share your passwords or accounts.
- Restrict file sharing on your computer to mitigate the risk of unintentionally granting access to unknown parties.
- Apply system updates for your desktop systems and department servers' operating systems and their integrated network services (e.g., e-mail and web browsers) in a timely manner.
- Keep local applications updated and patched.
- Encrypt sensitive files. Use IT Security-approved encryption methods only.
- Ensure that remote access (from off campus) connections are done securely using HTTPS, SSH or VPN.

## 6.0 Enforcement

Any student or employee of the University found in violation of this policy is subject to disciplinary proceedings including suspension of system privileges, expulsion, termination of employment and/or legal action as may be appropriate and in accordance with the applicable employment handbook, collective bargaining agreement, and student code of conduct applicable to the individual's relationship to the University.

## 7.0 Glossary of Relevant Terms and Definitions

**Access Controls**
Access Controls are methods of electronically and/or physically protecting files from being accessed by people other than those specifically designated by the owner.

**Campus Email**
The University's official email system (mail.montclair.edu) operated by the Information Technology Division.

**Data Custodian**
The **custodians** of data are employees, departments, colleges, research centers, and extension offices responsible for the integrity, confidentiality and availability of the data. It shall be the responsibility of the owner or custodian of the data to classify the data. However, all individuals accessing data are responsible for the protection of the data at the level determined by the owner/custodian of the data. Any data not yet classified by the owner/custodian shall be deemed **Private**.

**Data Owner**
The entity to which the data belongs. For example, a person owns his/her social security number, date of birth, and address.

**Encryption**
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Montclair State University is done via a license. GnuPGP is freely available for most platforms.

**Encrypted email**
Electronic mail that has been encrypted and digitally signed using a public-key algorithm such as PGP/GPG.

**Expunge**
To reliably and irretrievably erase data from a storage medium such as magnetic disk or tape, or from electronic media such as flash memory. In most cases special software utilities are required to repeatedly overwrite data with random values to make subsequent retrieval of the original data impossible.

**Personally Identifiable Information (PII)**
The term "PII," refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

**Physical Security**
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

**Secure Electronic File Transmission Methods**
Includes Secure FTP (sftp), SecureCopy (scp) and SecureShell (ssh) protocols.

**Unencrypted data ("clear text")**
Unencrypted data is able to be viewed as-is without the need for a password or software key and is often referred to as clear text.

## 8.0 Related Policies & Links

Montclair State Policy on Responsible Use of Computing
Password Management Policy
Social Media Policy

See also:

1 **Gramm-Leach-Bliley Act (GLBA)**
US Senate Banking Committee, Financial Services Modernization Act, Summary of Provisions - http://banking.senate.gov/conf/grmleach.htm
2 **Family Educational Rights and Privacy Act ( FERPA)**
US Department of Education, Final regulations (4/16/2004) - http://www.ed.gov/legislation/FedRegister/finrule/2004-2/042104a.pdf

**Revision History**
rev 1.0 11/13/13 Initial release
rev 1.1a 11/2/15