Administrative Policy

Policy Title:	**Information Security**
Policy Number:	1614
Date Adopted:	11/25/2013
Version:	4.0
Review Cycle:	Biennially
Date Last Reviewed:	8/15/18
Office Responsible:	Information Technology
Reviewing Committee:	MAK
Related Policies:	Clinical Simulation, Electronic Accounts, E-mail, RUP, Record Retention
Related Laws:	FERPA, Michigan Freedom of Information Act, Internet Privacy Protection Act

Policy Summary: Information Security

The purpose of this policy is to define procedures and processes to protect College data generated, accessed, transmitted and stored by the College, educate users about the importance of protecting College data, ensure confidentiality, integrity, and availability of College data;, and promote compliance with local, federal and industry regulations regarding privacy, protection and confidentiality of information.

Scope

All users have a responsibility to protect College data from unauthorized generation, access, modification, disclosure, transmission and/or destruction. Users are expected to be familiar with and comply with this policy.

Definitions

Appropriate measures: Appropriate measures are defined under the “individual data type” definitions.

Approved Electronic File Transmission Methods: Include supported Secure File Transfer Protocol (SFTP) and Secure Sockets Layer (SSL) clients and web browsers, as defined or approved by information technology (IT).

Approved Electronic Mail: Includes all mail systems supported by IT.

Approved Encrypted E-mail and Files: Information must be encrypted in accordance with IT guidelines. Contact the Solution Center for assistance.

Configuration of College-to-outside-party connections: Connections shall be set up to allow other entities to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Credit Card Holder Information: This information is defined as banking information, credit card information, credit card track (magnetic stripe) information, security codes, and other data obtained as part of a payment transaction or other confidential information as described in the Payment Card Industry Data Security Standard (PCI-DSS). The PCI-DSS standards can be found at https://www.pcisecuritystandards.org/.

Expunge: To reliably erase or expunge data on an electronic device, you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.

System Administrator: Technician(s) responsible for installing, supporting and maintaining servers or other computer systems, and planning for and responding to service outages and other problems.

Domain Administrator: Technician(s) responsible for adding and deleting e-mail accounts and setting configurations associated with that domain.

Individual Access Controls: Individual access controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Macs and PCs, this includes using boot-up/login and screen saver passwords. Employees must always sign out or lock controlled access systems.

Policy Statement 1.0 DATA CLASSIFICATION

This Information Security Policy defines for College employees the levels of security required to protect data they receive or use in the course of business, and for which they are responsible. The information covered by this policy includes all information received or handled by College employees in the performance of their job duties, whether written, oral, or electronic ("College information"). It includes, but is not limited to, information that is either stored or shared electronically.

All employees must familiarize themselves with these classifications and guidelines. All College information must be classified into one of three categories: restricted, limited access or public. Based on the classification, employees must implement appropriate security measures to protect College data.

Questions about the proper classification of a specific piece of information are to be addressed to your supervisor. Questions about these guidelines are to be addressed to the information technology director.

General Rules:

1. With the exception of public information, access to College information must be
   at all times limited to only those employees who have a business reason to know such information. For example, personal information, student records, accounts, balances, transactional information, credit card holder

information and ACH (electronic check) account numbers are to be accessible only to College employees with an appropriate business need for such information.

2. College information shall only be used for College business purposes.
3. All third-party contractors who have access to the College's restricted or limited access information must follow the remote access procedures. Contractors must agree to use College information only for College business and to abide by this policy. Other policies may exist to mandate confidentiality of such information.
4. Employees must use their College e-mail address for all College business involving data covered by this policy. Because of security concerns, employee or other College e-mail addresses shall not be forwarded to a private e-mail account.
5. Until data is classified under these guidelines, data shall be treated as limited access.

1.1 Restricted Information

Restricted information is data about a person or entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or be damaging to the financial standing, employability or reputation of the person or entity. The College is bound by law or by contract to protect some types of restricted information.

Restricted information should be shared only as mandated by law or as required for administrative or educational functionality. Examples of restricted information include the following:

a. Social security number
b. Credit card holder information
c. Checking or savings or other bank account number(s)
d. Debit card number
e. Password(s)
f. Disability information
g. Health and medical information
h. Library circulation records

1.1.1 Restricted Information Guidelines

Access: Restricted access is given to authorized users who have a business need to know. Electronic access must be protected by a strong password, and users shall log out or secure the documents before leaving their stations. Departments shall promptly notify information technology regarding personnel changes.

Distribution within College: Distribution of restricted information may be done via interoffice mail stamped confidential, e-mail and electronic distribution methods (see below). Library circulation records may not be distributed. Some restricted material, in paper form (e.g., PCI data), must be carried in a secured bag or tote.

Distribution outside of College internal mail: Distribution of restricted information outside of the College inter-office mail can be sent via U.S. mail or approved private carriers. Library circulation records may be distributed only as instructed by the library director in accordance with applicable law.

Electronic distribution: Electronic distribution of restricted information must be encrypted if sent to approve recipients within the College e-mail system, supported by the College. Email must be encrypted or password protected to approve recipients outside of College premises. Transmission of data must be via a secure method, such as secure file transfer protocol. Third-party agreements with outside vendors must require encryption or password protection. Instant messages, Google Docs, Dropbox, OneDrive including Jackson College OneDrive and similar Cloud services are not to be used for electronic transmission of restricted information.

Storage: Restricted information, in paper form, must be stored in a locked drawer or other locked and secure location. It may not be downloaded or stored on computers, flash drives, or external removable media. Backup files of restricted data must be encrypted. Instant messages, Google Docs, Dropbox, OneDrive including Jackson College OneDrive and similar Cloud services are not to be used for electronic transmission of restricted information. A network drive/folder may be used if access is restricted to only those with a business need.

Disposal/destruction: Restricted data must be shredded immediately after completion of task; electronic data should be expunged/cleared immediately after use. Users must reliably erase or physically destroy media containing restricted information.

Penalty for deliberate or inadvertent disclosure: Penalty for deliberate or inadvertent disclosure of restricted data may include termination, possible civil and/or criminal prosecution to the full extent of the law.

Alleged incidents involving students should be reported to the vice president of students, and institutional effectiveness. Alleged incidents involving employees or community partners should be reported to the executive director of human resources.

Examples of How Data Can Be Lost or Compromised
• Notebook or other data storage system stolen from car. • Employee accesses system after leaving employment because passwords aren't changed. • Unauthorized person walks into unlocked office and steals equipment or files, or accesses unsecured computer. • Unsecured application on a networked computer is hacked and data stolen. • Human error in programming changes. • Data transmitted over Internet in unencrypted form. • Installing software unnecessary for College work.

Impact of Restricted Data Loss
• Loss of funding from granting agencies. • Loss of reputation. • Unauthorized tampering with enterprise data. • Increase in regulatory requirements. • Loss of critical campus or departmental service. • Individuals put at risk for identity theft. • State and federal monetary fines.

1.2 Limited Access Information

Limited access information is defined as information that is not restricted, but can be used as personally identifiable or private information. This information must be guarded due to proprietary, ethical or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use.

This information is releasable in accordance with the Michigan Freedom of Information Act. Limited access information is generally restricted to users who have a legitimate purpose for accessing such data. Limited access information must be appropriately protected to ensure a controlled and lawful release.

One piece of limited access information cannot in and of itself be used to identify anyone. Two or more pieces of information are needed. For example, a Jackson College student or employee ID number itself is useless, unless combined with a name and/or birth date. A list of salaries is useless unless combined with names and/or position titles. Examples of limited access information include the following:

a. Staff and student home addresses and phone numbers
b. FERPA directory information
c. Class lists
d. Student records (grades, test scores, attendance, enrollment and registration history, advisor's comments)
e. Payroll information
f. Beneficiary/dependent information
g. Benefit elections
h. Campus safety and security incident reports
i. Jackson College ID numbers
j. Driver's license numbers
k. Date of birth
l. Ethnicity
m. Purchasing information designated as proprietary or confidential

1.2.1 Limited Access Guidelines

Access: Limited access is given to authorized users who have a business need to know. Electronic access must be protected by a strong password, and users shall log out or secure the documents before leaving their stations. Departments shall promptly notify information technology regarding personnel changes.

Distribution within College: Internal distribution of limited information shall be done via standard inter-office mail, the e-mail system supported by the College, and electronic file transmission methods.

Distribution outside of College internal mail: Distribution of information outside of the College should be sent via U.S. mail or approved private carriers.

Electronic distribution: There are no restrictions to approved recipients within College via the e-mail system supported by the College for limited information. If this information is sent to approved recipients outside of College e-mail systems, it must be encrypted, password protected, sent via a private link, or faxed. Instant messages, Google Docs, Dropbox, OneDrive including Jackson College OneDrive and similar Cloud services are not to be used for electronic transmission of restricted information.

Storage: Individual access controls shall be implemented at the network folder or directory level for limited access electronic information. Google Docs, Dropbox, OneDrive including Jackson College OneDrive and similar Cloud services are not to be used for storage of this data unless encrypted

Disposal/destruction: Limited information shall be shredded or placed in specially marked disposal bins for shredding on College premises; electronic data must be expunged/cleared immediately after use. Users must reliably erase or physically destroy media containing limited access information.

Penalty for deliberate or inadvertent disclosure: Penalty for deliberate or inadvertent disclosure for limited access information may include termination, and possible civil and/or criminal prosecution to the full extent of the law.
Alleged incidents involving students should be reported to the vice president of students, and institutional effectiveness. Alleged incidents involving employees or community partners should be reported to the executive director of human resources.

Examples of How Data Can Be Lost or Compromised
• Staff member, wanting to be helpful, releasing information they are not authorized to share. • Faculty member posting test scores with student ID numbers or names. • Leaving class lists or gradebooks in open spaces. • Leaving a computer unattended with applications open that contain limited access information.

Impact of Limited Data Loss

- Loss of reputation.
- Loss of critical departmental service.
- Individuals put at risk for identity theft.
- Loss of grant funding.
- Loss of state funding.
- Loss of federal funding.

1.3 Public Information

Public information is information that is open to the public and that can freely be given to anyone without any damage to the College or to individuals. Public information, while subject to College posting or disclosure procedures, is available to all users and to all individuals and entities external to the College community.

Examples of public information may include the following:

a. Publicly posted press releases by college administration
b. Publicly posted schedules of classes
c. Published College catalog
d. Information authorized for posting on the College's public website
e. Online staff directory, interactive maps, newsletters, etc.
f. Board of trustees agenda and minutes

1.3.1 Public Information Guidelines:

Access: There are no restrictions for access to public information. Access is given to the public, and external and internal users.

Distribution within College: There are no restrictions to public information distributed
within the College.

Distribution outside of College internal mail: There are no restrictions to public information distributed outside of College internal mail.

Electronic distribution: There are no restrictions to electronic distribution of public information.

Storage: There are no restrictions to storage of public information.

Disposal/destruction: See Jackson College retention and disposal guidelines.

Penalty for deliberate or inadvertent disclosure: Not applicable.

2.0 ADMINISTRATIVE PROCEDURES 2.1 Classification

Documents must be classified according to the type of information contained in the document. All documents must be classified and handled according to the procedures for the highest restricted level of any information contained in the document. For

example, if a document contains both restricted and public information, the document shall be treated according to the restricted information procedures.

Questions about the classification of particular information or documents should be addressed to your supervisor. Questions about these guidelines may be addressed to the director of information technology.

2.2 Training

2.2.1 Initial Training: All employees shall be trained on the procedures and guidelines pertaining to this policy. If significant changes are made to the definitions of information or the procedures required, all employees shall be informed regularly via e-mail.

2.2.2 Periodic Refreshers: All employees shall receive reminder instructions at least annually.

2.4 Violations

Violations of the security guidelines contained in this policy shall be reported immediately to the area supervisor. The supervisor shall immediately contact the director of information technology or his or her designee, to determine whether further action is needed to secure College information. The director of information technology or designee will work with the affected areas and personnel to determine the appropriate actions to be taken.

3.0 SYSTEM SECURITY

3.1 Physical Security

3.1.1 Sever Room/Data Room Access: Doors to the computer room are closed and locked at all times. A limited number of IT and maintenance staff have access, and access is only via use of the electronic fob/key card system, so that access can be tracked.

3.1.2 Remote Access: Remote access must use secure connection protocols. Remote access for server administration is limited to IT staff members with legitimate business reasons.

3.1.3 Personnel Verification: All staff members and vendors shall present a picture ID to campus security staff if requested. ID shall be worn and in public view.

3.2 Network Security

3.2.1 Firewalls: All external network traffic to and from the primary application/database servers passes through at least one firewall, which monitors and blocks unauthorized traffic. All exceptions to firewall configurations are approved by the director of information technology. Exceptions are made for

emergency situations, in which case the director of information technology is notified.

3.2.2 E-mail Filter: An e-mail filter system shall be used to significantly reduce the amount of e-mail spam. All incoming e-mail shall be scanned for malicious software.

3.2.3 Packet Shaping: Packet shaping technology shall be utilized to monitor network traffic. A packet shaping appliance throttles down unwanted protocols and allocates bandwidth where it is most needed.

3.2.4 Wireless Environment: Personal equipment on wireless connections at the College is unable to access the College's administrative network. Only College-owned devices can connect to the College administrative network.

3.3 Server Security

3.3.1 Login Accounts

3.3.1.1 IT System Administrator Accounts: System administrator privileges are granted after review of the need for such privileges. Only personnel with a business need have access to administrator accounts will be granted these accounts. System administrators are issued two accounts, one for administrative functions and one for non-administrative functions.

3.3.1.2 User Accounts: User accounts are created for each new employee and have minimal access privileges (e-mail, e-Services, network access, etc.).
Additional access privileges are granted on an as-needed basis.

3.3.1.3 Password Policy: Unique passwords are issued at the creation of an account. All passwords shall be changed in accordance with the account policy. Users shall not share passwords, in order to prevent unauthorized access to College systems.

The College password guidelines can be viewed on the information technology page:
http://www.jccmi.edu/informationtechnology/default_password.htm

3.3.1.4 Generic Accounts: Various campus departments maintain guest accounts that provide access to the Internet and limited access to non-College users, for campus computing resources. All such accounts must be managed by an employee who is responsible for ensuring that they are used appropriately and as intended. (See also: Electronic Accounts Policy.)

3.3.2 File/Directory Access: Permissions on system files shall be as restrictive as possible while still allowing users to be effective.

3.3.2.1 Database Files: Database files are accessible only to the system and database administrators.

3.3.2.2 Code Files: Access to code files is restricted to programmers and system administrators.

3.3.2.3 Output/Report Files: Read-only access to reports is restricted to employees who have the business need to see the report information, and who are properly authorized.

3.3.3 Data Backup

3.3.3.1 Backup Tapes: Servers are backed up every day with established backup procedures. Backup media is stored in a limited access, secured room and off site at another College location. Backups are encrypted.

3.3.3.2 Personal Data Files: It is the responsibility of each department and employee to assure that the confidentiality, preservation, and integrity of sensitive data (restricted or limited) within the College's policies. This includes the secure distribution, storage and destruction of sensitive data on personal media.

3.3.4 OS Patches: Operating systems are patched on a regular basis, or specifically when there are major security/stability issues. Other installed software is likewise patched either on a regular basis or when a specific security/stability bug report is released.

3.3.5 Server Ports: College servers are generally not configured to access the Internet.
Only necessary ports are open to allow software to function.

3.4 Database Security

Database security applies to the access of data stored in a database management system (DBMS) such as Unidata, MySQL and Microsoft SQL Server.

3.4.1 User Accounts: User accounts can be managed either in the application or by the DBMS. In the first case, the user security is built into the application and requires the administrator to employ application utilities to manage user accounts. In the second case, the users log directly into the database and the database administrator (DBA) uses database features to maintain database security.

3.4.1.1 Account Creation and Termination: User accounts are either created by the database administrators, or automatically through business application logic. Colleague account creation requires a request from a validated supervisor and its implementation must be preceded by appropriate training. Colleague accounts are created by DBAs while Moodle accounts are typically generated through the business logic for

students and faculty. Similarly, account termination is either generated by direct DBA action or automatically through application logic or external processes that attach to the database.

3.4.1.2 Password Complexity and Expiration: All accounts must have a College ID and a login password. Passwords are stored and encrypted in system tables. Automatic password expiration rules and password retry attempt limits are in accordance with College standards. Reset requests require identity verification.

3.4.1.3 Timeouts: Idle connection timeouts are another aspect of electronic security, especially in situations of public computer use. Idle timeout for College services have standard timeout from five minutes to 30 minutes. Timeout rules vary depending on user status and the nature of the application.

3.4.1.4 Auditor and Contractor Accounts: On occasion, the need arises for auditors or private outside contractors to have access to databases. Jackson College's policy is to create such accounts with the access required, but to either lock them or drop them after the work is performed. All outside auditors and contractors sign confidentiality and nondisclosure agreements before access is granted.

3.4.1.5 Restricted Access Accounts: Certain database accounts are used for data ownership. These accounts contain tables or stored procedures used by the application. Only database administrators or application developers can log into these accounts. Since they are permanent accounts, their login access is carefully restricted by the database administrators.

3.4.2 Database Object Access: Database objects include tables with data, views on those tables and stored procedures. Access to database objects is normally via the application and depends on the user's application security privileges. However, direct access is authorized and granted to a small number of users for reporting troubleshooting purposes.

3.5 Application Security: Applications often serve as the delivery mechanism through which personal data and other sensitive information is transferred online. Unsecured or poorly written applications can be exploited to bypass security measures or used to transfer information that is easily intercepted.

College applications are developed following industry best practices. SSL and SFTP protocols are used for access and transmission of restricted and limited access data.

3.6 Desktop Security

3.6.1 Standard Windows Image: Standard images have been created that are deployed on all new computers and are used to refresh existing computers. The use of standard images prevents the installation of unneeded services.

3.6.2 Virus Protection: Antivirus software is utilized to protect systems from viruses. The software is automatically updated frequently.

3.6.3 Automatic Updates: Windows updates are controlled via an internal server. Updates are set to install at shutdown, or they may be installed manually via a system tray icon.

3.6.4 Remote Desktop Access: Windows remote desktop functionality is available for administrators and faculty. All internal users have access to remote desktop while on campus. If there is a need for remote access for staff off-campus, it must be approved by human resources.

3.6.5 Cardholder Data Desktop Access: Two-factor authentication is used for machines accessing the cardholder data environment.

3.7 Detection and Auditing Procedures

The IT department maintains and routinely updates of its internal audit procedures and control procedures.

Date Of Change	Version	Description of Change	Responsible Party
11/25/13	1.0	Policy Created	J. Jones
03/26/2014	2.0	NA	
12/10/2015	3.0	Update Style Guide	D. Schissler
02/14/18	4.0	Minor Changes	J. Jones