Information Systems Security Policy

MILITARY MARION INSTITUTE

MARION
MADE

Contents

Introduction

This general security policy has been developed to ensure data integrity and confidentiality for all administrative computer systems at Marion Military Institute. This document is intended to provide guidelines for the classification of data resources, and subsequent retrieval and dissemination of that data by various user groups. These guidelines will allow individual departments to approve data access authorizations for their data (in general cases). Any exceptions to user access situations covered in this general policy will be taken under special consideration by the President of the institution.

More and more institution employees have access to confidential information via computers. This security policy is not intended to obstruct the use of computers in obtaining information necessary to conduct institution, or departmental business. However, it is intended to encourage responsible use of computers and discretion in the dissemination of student and employee information.

Data Retrieval and Dissemination

Procedure

Each set of institutional data will be classified as having an “owner”. This owner will be represented by a specific individual within the institution department responsible for that data.

User profiles are specific groupings of security levels, menu access and program execution access. Each profile is user specific and user ID and password secured. User IDs and passwords are created by personnel holding an appropriate security level and possessing experience and knowledge to perform such a task in accordance with the employee’s approved job description

Enforcement of Policy

Each department is responsible for enforcing this data security policy. Institution policy states that confidential information is to be used only when necessary for institutional or departmental business. Refusal to adhere to this policy is a clear violation of the Family Educational Rights and Privacy Act of 1974. Offenders will be subject to disciplinary action and possible referral of the violation to the proper authorities

Data Sources

Original, paper copy student records are maintained by the functional areas responsible for the creation, collection, maintenance, and retention of those records. Electronic versions of each record are maintained on the institution's central computer system. Access to both record forms is controlled by the MMI staff member responsible for the area.

Note: Record integrity is maintained by restricting records creation and modification access to employees within each functional area. Employees are given user identification and password access to each computer record with specific creation, update, or read-only access to the record commensurate with the employee's job duties and approved by the President of the Institution. Control documents for all modifications to records are processed and maintained within the functional areas.

For the purposes of this policy, data types are categorized as follows:

- Student Information (Directory, Academic, and Summary)
- Student Financial Aid Information
- Administrative Financial Information
- Personnel Information
- Institutional Research Information

Within these general categories, the different types of data are broken down into subsets, and an institutional source is provided for each.

Student Information

Data Owner: Registrar

Access to student academic records is controlled by the Office of the Registrar. The permanent academic record includes all completed coursework, grades, and grade point averages. Access to academic records is provided in accordance with the Family Educational Rights and Privacy Act as amended in 1974. A paper copy of a student's record is maintained by the College for five years and stored in a locked, fireproof filing cabinet which is located in the Registrar's Office. The permanent academic record is stored in the College's student record computer system. A nightly backup tape of all electronic records is maintained with the College's data center. A weekly remote backup is stored off-campus in a Tier IV data canter. An off-campus backup tape is maintained in a safe at a local bank.

For security purposes, student academic records are divided into two categories: directory and non-directory.

Directory Information:

Directory Information, which is defined by the Family Educational Rights and Privacy Act, Sec.99.3 (FERPA) as information contained in an education record that would not be generally considered harmful or an invasion of privacy if disclosed, can be disclosed to outside persons, organizations, or agencies upon request unless the student specifies in writing to the Registrar's Office that this information is to be withheld. Directory information, as defined by Marion Military Institute under the Act, includes the following: student/cadet name; addresses (campus, home, ailing); email; telephone numbers; class level; previous institutions attended; awards; honors including the Dean's List and President's List; degrees conferred, including dates; dates of attendance names of parents; past and present participation in officially-recognized sports and activities; physical factors (e.g., height and weight of athletes); and date and place of birth

Academic Information:
Academic information, including course grades, class schedules, etc., cannot be released to third parties without the student's written permission. Academic information can be accessed, without prior permission from the student, by Marion Military Institute staff and faculty who, under the Act, have a legitimate educational interest in the student and who are acting within the imitations of their need to know. This applies even to student information even if the student has requested that no outside disclosure be made.

Academic information not available from the student administrative software database should be requested from the Office of the Registrar.   Requests for information from students or from agencies or individuals outside of the institution should also be referred to the Office of the Registrar.

Summary Student Information:
The Office of Institutional Research is the official source of aggregate or summary student information, such as enrollment or credit hour data intended for on or off campus dissemination.   Requests for reports and analyses involving summary student data to be produced through the student administrative software database will be developed in conjunction with the Offices of Institutional Research and the Registrar. This ensures that reports and analyses are based upon the most accurate information and will enhance the consistency and integrity of information generated by institutions and departments.

Student Financial Aid Information

Data Owner: Director, Financial Aid Office
The Financial Aid Office is the official source of information on students receiving financial assistance from various aid programs, including grants, scholarships, and loans.   All requests for this type of information should be addressed to the Director of Financial Aid.

Administrative Financial and Accounting Information

Data Owner: Comptroller
The Comptroller is the official sources of financial information on the institutional budget, purchases and expenditures, and institutional personnel. All requests for any of these types of financial information should be submitted to the Comptroller..

Personnel Information

Data Owner: Director, Human Resources and Compliance
Information concerning specific job positions (classifications, descriptions, etc.) is maintained by the Office of Human Resources and Compliance.   All requests for employee information (excluding payroll information) should be sent to the Director.

Institutional Research Information

Data Owner: Director, Institutional Research
Institutional research information includes data on student enrollment, space utilization, credit hour production, surveys, governmental and accreditation reports, etc.   The official sources for this type of information is the Office of Institutional Research, and all requests for such information should be submitted to the Director.

Classification Standards

Data Classification

Data classification indicates what the user is able to do with the data. Specific restrictions are outlined and enforced by individual departments responsible for the data. Specific levels of access clearance include the following:

1. Full Control
2. Change
3. Read Only

Various user classifications will have access to data through one or a combination of these permission levels. Each user ID is restricted by the data that the user has been granted to access, i.e., their permissions granted will provide them the ability to access a limited number of forms. If a user tries to access data inappropriate to his/her clearance level, a security violation message will appear on the screen.

Data should not be downloaded to other storage medium without permission from the departmental owner of that data. Individual users will be held responsible for any violation of this procedure.

Security

Departmental Security

Each department will designate an “owner” for the data it maintains. Appropriate procedure for retrieval and dissemination of institution data will be followed as outlined in the previous section, Data Retrieval and Dissemination.

Departments storing data subject to institution regulations are responsible for ensuring that all such data is protected in accordance with institutional regulations. This applies to all such data from any source, whether electronically transferred from the administrative systems, or entered by the individual department from printed documents.

Specifically, departments must ensure that access to individual workstations or servers containing this information or access to output generated from departmental systems, is restricted to individuals authorized to access the data. Password security on individual stations or servers is not sufficient to ensure compliance; any such systems on which regulated data is stored must also be in secure, supervised areas, such as departmental or individual offices.

Backup tapes, disks or copies of data on printed or electronic media must be similarly protected. Under no circumstances shall confidential data or access to it be granted to personnel from other departments or non-institution personnel without express written authorization from the appropriate administrative office. Any unauthorized storage and/or reproduction of confidential institution data (e.g., grades, transcript files, etc.) is strictly prohibited.

Physical Security

Marion Military Institute has the responsibility of administering, protecting, and monitoring all computers, software, and networks owned or licensed by the college whether on or off campus, with the exception of privately owned computers in the possession of individuals for their personal use. Authorized personnel may monitor computer activity, including electronic mail, for the purpose of maintaining system performance and security. Users are expected to cooperate with investigations of violation of college policy.

Access to academic and administrative computing facilities is not available to anyone who is neither an employee nor an active student except by express written permission of the President of the College. Marion Military Institute reserves the right to require users to refrain from using any program or property of the college.

Using or attempting to use any computer or information technology resource of Marion Military Institute signifies the following:

- The user agrees to comply with the provisions of this Acceptable Use Policy.
- The user accepts responsibility for knowing the contents of this policy statement. Failure to read or acknowledge this statement will not be an excuse for noncompliance.
- The user accepts that failure to comply with this policy may result in temporary or permanent denial of access to computer or information technologies, or in some cases may result in college disciplinary action or legal action.
- Copies of the Acceptable Use Policy are available in the Cadet Handbook and on the College website.

Department/division heads are responsible for ensuring the physical security and responsible use of computers located in departments and offices under their authority. The following policy statements should be made available and/or posted prominently so that all personnel working with computers know the extent of their responsibility.

1. Computers will be located in physically secure areas which can be locked when not in use.
2. Access to computers will be limited to individuals engaged in official institution business.
3. Use of computers by student workers should be restricted to those cases in which student workers are absolutely necessary to supplement regular institution staff members. Student workers should be thoroughly instructed in the proper and responsible use of computers.
4. Each individual with access to administrative information is assigned his/her own user id (username) and password. The owner of the code should not pass on this information to anyone else; the owner is responsible for any misuse of his/her sign-on credentials.
5. Under no circumstances will the aforementioned codes be posted on or near computers
6. Computers which are “signed on” should never be left unattended.
7. Requests for improvement of computer security, as well as suspected violations, should be addressed to the Director of Information Technology.

Computers which are routinely used by individuals not cleared for access to such data are inappropriate locations for confidential data (e.g. computers in student labs or other public locations.) Placing confidential information on systems of this nature constitutes a clear violation of institution regulations.

Because of the possibility of theft and discovery of data, neither portable computers (notebooks, laptops, etc.) nor portable storage devices, including USB keys and portable disks, should be used to store sensitive or regulated data, unless such data is encrypted.

If a computer with communications software is used to access institution information systems, no information specific to your access to the system (such as sign-on codes or passwords) shall be encoded in the communications package nor otherwise stored within that computer. This means that the sign-on process cannot be fully automated, but will require keyboard entry of appropriate codes and passwords at sign-on time.

If the communications package has been acquired from the Information Technology Department, copies shall not be given to any other individuals or departments. Any such requests should be submitted directly to the Office of Information Technology.

Data Security

Any individual who accesses institution data, through a computer or a report, is responsible for the confidentiality of that data. Likewise, any individual who stores institution data on a personal computer will be held accountable for the confidentiality of that information.

Web Servers and Departmental Servers

Marion Military Institute is a State Institution and institutional web publications
have the same character as a written publication of the institution. These web publications include division, department, or program sub-web pages and Facebook and other social networking pages that in any way represent or reflect upon the institution. The following are the official guidelines for the Marion Military Institute web sites and Internet related material.

All web content published by Marion Military Institute must:

- be approved by the Office of the President or designee;
- present content that describes the institution accurately for the current semester;
- reflect positively upon the institution as an institution of higher learning in visual appearance and editorial tone;
- further the institutional mission and goals of the institution;
- be consistent with all policies, rules, regulations, and guidelines of the institution, including but not limited to those published in the *Catalog*, *Faculty and Staff Handbook,* and State Board Policy;
- obtain approval through the appropriate institution channels for any news releases or public announcements;
- be consistent with local, state, and federal laws, including copyright law;
- be consistent with principles of professional, educational, and creative ethics;
- be generated by software supported by the institution;
- be designed to load quickly on computers of varied ages, Internet connections, and browsers.

Electronic Mail System Security

MMI's email services are hosted by Microsoft and Google. All professional employees of the institution should have an active institution email account. Any employee of the institution may obtain an email address by contacting the Office of Information Technology.

Electronic mail poses additional risks in the handling of confidential data. Data may quite readily be transmitted to unintended recipients through misaddressing or similar error. In addition, the routine maintenance of mail systems may require or inadvertently lead to viewing of some pieces of mail by mail systems administrators. The Office of Information Technology will respect the privacy of all such mail and will not reveal the contents of such mail to any other parties. However, if activities in violation of law or institution regulations are discovered through this procedure, the I.T. Department may report such information to appropriate authorities.

Departments are advised that information subject to confidentiality regulations should not be transmitted via electronic mail without prior written approval from the appropriate administrative offices.