Confidential Information Policy

Scope: Who is Covered by this Policy?

Employees

Policy

Miami University collects, stores, and distributes large amounts of information essential to the performance of University business. This information represents a valuable University asset. Although a large portion of University information is public, a portion of our information is protected by state and federal laws. To comply with these laws and protect the University community, the University has the right and obligation to protect, manage, secure, and control information (whether in hard copy or stored as electronic data) in its possession.

Information protected by federal or state law may not be shared with unauthorized persons~~.~~ or posted online at a site that can be accessed by unauthorized persons. These laws include the Federal Privacy Act which protects social security numbers, the Family Educational Rights and Privacy Act (FERPA) which protects personally identifiable student records, the Gramm-Leach-Bliley Act (GLBA) which protects consumer financial information, and the Health Insurance Portability and Accountability Act (HIPAA) which protects personal health information. All employees, faculty and staff, bear responsibility for protecting confidential information from unauthorized disclosure. *This is true whether this information is stored on paper, a network computer, on a laptop, on a personal digital assistant (PDA) or other device.*

Information that is protected by law may only be disclosed to authorized persons. Examples of confidential information include:

- ~~social~~Social security numbers
- ~~disability~~Disability status

- ~~health~~Health and medical information
- ~~student~~Student advising records
- ~~student~~Student grades
- ~~student~~Student disciplinary records
- ~~consumer~~Consumer financial information
- Banner student identification numbers
- ~~trade~~Trade secrets
- ~~credit~~Credit and debit card numbers
- coursework produced by students

Social security numbers are primarily used for student financial assistance and employment tax-related matters. If unique identification of an individual is required, an identifier other than a social security number should be used. The recommended identifier is the Banner Plus number. An appropriate security plan and the written consent of the Information Security Officer are required before any University office is permitted to collect and/or maintain social security numbers.

Each faculty and staff member must assume responsibility for protecting confidential information from unauthorized exposure. This means you must do the following:

1. ~~understand~~Understand and follow Miami's Responsible Use of Computing Resources policy;
2. ~~consult~~Consult the Information Security Office if you are uncertain whether certain information is confidential;
3. ~~consult~~Consult the Information Security Office if you are uncertain how to safeguard confidential information;
4. ~~understand~~Understand and follow the Miami University Computing Security Policy;
5. ~~protect~~Protect your computer password and change it according to standards published by the Information Security Office in the ~~IT Services Knowledge Base~~IT Services Knowledge Base;
6. NOT provide access to confidential information to any other person unless authorized to do so.

Ohio law requires the University to take certain actions in the event of unauthorized disclosure of confidential information. You must report any suspected disclosure of confidential information to unauthorized persons to the Information Security Officer (Call 529-9252 immediately and report that you suspect that confidential information has been disclosed). *In addition to reporting the theft of any laptop, personal digital assistant or other device that contains confidential information to the appropriate law enforcement authorities, you must immediately report the loss/theft of any laptop, personal digital assistant or other device that contains confidential information to the Information Security Office.*

Related Form(s)

Not Applicable.

Additional Resources and Procedures

Websites

~~IT Services Knowledge Base~~

IT Services Knowledge Base

FAQ

Not Applicable.

Policy Administration

Next Review Date

7/1/2023

Responsible Officers

- Assistant VP for Security Compliance & Risk Management
- General Counsel

Legal Authority

- FERPA
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act

Compliance Policy

Yes

Recent Revision History

Amended July 2019

Reference ID(s)

- MUPIM 3.22
- OAC 3339-3-22

Reviewing Bodies

Administrative