POLICY NUMBER:	VII-5
POLICY TITLE:	Miami Dade College Information Security Plan
LEGAL AUTHORITY:	Family Educational Rights and Privacy Act; Copyright Act of 1976; Florida Computer Crimes Act, Chapter 815, Florida Statutes; Florida Public Records Act, Chapter 119, Florida Statutes; Gramm-Leach-Bliley Act, 1999, 15 U.S.C. Section 6801, *et seq.*
DATE OF LAST REVIEW:	6/21/2005, 6/19/2007, 7/21/2009, 7/19/2011, 7/16/2013 and 9/17/2024
DATE OF BOARD ACTION:	9/16/2003, 6/19/2007, 12/14/2021 and 9/17/2024

Role of Information and Information Systems

Miami Dade College (MDC) is critically dependent on information and information systems. If important information were to be disclosed to inappropriate persons, the College could suffer serious losses. The positive reputation that Miami Dade College enjoys is also directly linked with the way that it manages both information and information systems. For example, if private student information were to be publicly disclosed, the organization's reputation would be harmed. For these important business reasons, executive management working in conjunction with the District Board of Trustees has initiated and continues to support an information security effort. One part of that effort is the definition of these information security policies.

Team Effort

To be effective, information security must be a team effort involving the participation and support of every person at Miami Dade College who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of all people and the steps they must take to help protect Miami Dade College information and information systems. This policy and any other College policy and procedures describe ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Involved Persons

Every College employee must comply with the information security policies found in this and related information security documents. Employees who knowingly violate this and any other information security policy statements will be subject to disciplinary action up to and including termination.

Involved Systems

This Policy applies to all computer and network systems owned or administered by the College inclusive of all operating systems and applications, including voice. The policy's scope is limited to information processed by computer and network systems and does not address the security of information in other forms, such as paper.

Primary Departments Working on Information Security

Guidance, direction, and authority for information security activities are centralized for all College organizational units in the Office of Information Security and Compliance (OISC). OISC is responsible for establishing and maintaining organization-wide information security policies and procedures and shall recommend the use of best practices which may be the reference standards for certain aspects of the information security program. Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of OISC in conjunction with the Internal Audit Department. Investigations of system intrusions and other information security incidents are the responsibility of OISC in conjunction with Internal Auditor. Employee disciplinary matters resulting from violations of information security requirements are handled by supervisors working in conjunction with the Human Resources department. Student Deans shall be responsible for disciplinary matters concerning students, in accordance with College policy and procedure.

Three Categories of Responsibilities

To coordinate a team effort, the College has established three categories, at least one of which applies to each employee. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security. More detailed information about these responsibilities can be found in College procedures and guidelines.

Consistent Information Handling

Miami Dade College information, and information that has been entrusted to the College, must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its classification, no matter what its stage in the life cycle from origination to destruction.

Need to Know

Access to information in the possession of, or under the control of, the College must be provided based on a need-to-know basis. Information must be disclosed only to people who have a legitimate business need for the information. At the same time, employees must not withhold access to information when the Owner of the information instructs that it be shared. To implement the need-to-know concept, the College has adopted an access request and Owner approval process, which the College shall define in College Procedures. Employees must not attempt to access sensitive information unless the relevant Owner has granted them access rights.

Compliance Statement

Prior to using College Computing Resources, all employees must sign a compliance statement prior to being issued a user ID. A signature on this compliance statement indicates that the involved user understands and agrees to adhere to College policies and procedures related to computers and networks, including the instructions contained in this Policy.

Release of Information to Third Parties

Unless it has specifically been designated as public, all internal College information must be protected from disclosure to third parties. Third parties may be given access to internal information of the College only when a demonstrable need to know exists, when a College non-disclosure agreement has been signed, and when such a disclosure has been expressly authorized by the relevant Miami Dade College information Owner. Additional College procedures and guidelines shall detail the handling of information by third parties, the disclosure process, and the processes surrounding the loss of information by third parties.

Physical Security to Control Information Access

Access to every office, computer machine room, and other College work area containing sensitive information must be physically restricted to authorized personnel. When not in use, sensitive information must always be protected from unauthorized disclosure. Additional College procedures and guidelines shall define the steps that should be taken to secure information from unauthorized disclosure.

Internal Network Connections

Users may be required to utilize multi-factor authentication approved by OISC when a user is authorized to access certain College applications with sensitive programs, data, or websites. When being authorized access to certain Miami Dade College applications because of sensitive data particular programs or sites carry you may be required to use a multi-factor authentication approved by OISC. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system. Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered. Multi-user systems throughout the College must employ automatic log-off systems that automatically terminate a user's session after a defined period of inactivity.

Network Changes

All changes to College computer networks must be documented in a work order request, and approved in advance by the Information Technology Department, except in the case of an emergency. All emergency changes to College networks must be made only by people who are authorized by the Information Technology Department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees but also to vendor personnel.

External Disclosure of Security Information

Information about security measures for College computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless approved by the Office of Information Technology.

Mandatory Reporting

All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize College information or information systems must be immediately reported to OISC.

Information Security Plan

Pursuant to the requirements of the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act) (GLBA), 15 U.S.C. Section 6801 *et seq.*, the College has created an Information Security Plan ("Plan") designed to safeguard information required to be protected under the GLBA ("GLBA Protected Information"). This includes non-public financial information in any form, about a student or other third party who has a relationship with the College that is handled by or on behalf of the College. The Plan shall: (a) designate the Information Security Coordinator; (b) set forth procedures to identify and assess the risks of exposure, and (c) outline administrative, technical, and physical safeguards for GLBA Protected Information. The Plan shall be set forth in detail in applicable College procedure.

Michael Bilbao	9/17/2024
CHAIRMAN	**DATE**