Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

Policy

UNIVERSITY POLICY IT-04.03-05/25

TO: The University of West Florida Community

FROM: Dr. Martha D. Saunders, President

SUBJECT: Information Security and Privacy

RESPONSIBLE OFFICE: Information Technology Services

I. Purpose:

The University of West Florida (the "University") takes seriously its obligation to respect and protect the privacy of its students, alumni, faculty, and staff, and to safeguard the confidentiality of information important to the University's mission and vision. This commitment is in accordance with legislated or contractual obligations concerning the use and control of protected or private information. As the custodian of protected and private information, the University recognizes the importance of safeguarding information resources from loss, misuse, unauthorized access, or modification.

This policy is not intended to replace or supersede provisions for protected or private information that are dictated by legislation or contractual provisions.

II. Applicability:

This policy applies to all faculty, staff, students, affiliates, prospective students, contractors, sub-contractors, and associated parties who interact with University systems to access, process, transmit, or store information classified as Protected or Private on:

A. University-owned computing systems, telecommunication systems, and network assets.

B. Personally-owned computing/storage devices and telecommunication devices.

C. Computing, storage, telecommunications, or network services procured from third-party vendors, including cloud and colocation services.

University units that maintain physical locations or conduct services outside of the United States of America are also responsible for meeting applicable local, national, or regional privacy rules or regulations for those sites.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

III. Classifications, Definitions, and Additional Resources:

A. Classifications – for the purpose of this policy, information is classified as follows:

1. Protected – encompasses information deemed confidential under federal or state law, applicable international law, applicable regulations, contractual obligations, or privacy considerations. Examples of Protected information include:

   a. Social Security Numbers;

   b. Student education records and personal identifiable information as defined by the Family Educational Rights and Privacy Act (FERPA), except data which is designated "directory information" and where the student has not requested a privacy hold;

   c. Student directory information in cases where the student has requested a privacy hold;

   d. Personal health information;

   e. Financial data, including:

      i. Credit and debit card numbers;

      ii. Bank account numbers;

      iii. Data pertaining to student loans;

      iv. Data covered by the Gramm-Leach-Bliley Act (GLBA); and

      v. Data covered by the Payment Card Industry – Data Security Standard (PCI DSS);

   f. Automated license plate recognition system records; and

   g. Sensitive research data, including research data involving human subjects.

   The Protected classification used by the University may provide more protection, but not less protection, than what is required under federal or state law.

2. Private – encompasses information for which the unauthorized disclosure may have moderate adverse effects on the University's reputation, resources, services, or individuals. This is the default classification and should be assumed when there is no indication that information should be classified as public or protected. Examples of Private information include:

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

a. UWF identification numbers (UWFID)

b. Unpublished research data which is not otherwise considered sensitive

3. Public – encompasses information for which disclosure to the public poses negligible or no risk to the University's reputation, resources, services, or individuals. In addition, certain legislation may specify select information as public.

B. Definitions

Data Trustees – Division Heads, as that term is defined in UWF Policy HR-18, Hours of Work and Benefits, as it may be amended, responsible for the major categories of University data for their respective areas.

Employee Statement of Understanding Regarding Confidentiality – the form executed by a University employee that acknowledges an understanding of the requirements when handling protected or private information; this form is executed upon the initial completion of Knowledge Worker Certification.

Encryption – the encoding of data into a form that cannot be easily decoded by unauthorized parties.

Education Records – records that are directly related to a student and are maintained by the University or by a party acting for or on behalf of the University; this term shall have the same definition as defined in the Family Educational Rights and Privacy Act (see UWF Regulation 3.017, Student Education Records, for more information).

Information Systems Coordinating Group (InfoSys) – an inter-departmental group whose members are endorsed by a Data Trustee to manage a subset of data. The designated members are responsible for the accuracy, privacy, and integrity of a University data subset.

Personal Health Information (PHI) – demographic information, medical history, test and laboratory results, insurance information, and other information that is collected by a healthcare professional to identify an individual and determine what type of care that individual should receive.

Personal Identifiable Information (PII) – any information relating to an individual or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.

University Unit – a school or college and any departments or divisions that are a subdivision of a college or school; centers, facilities, labs, libraries, or programs within a college or school, or as independent entities; offices; associations; and administrative units.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

C. Additional Resources

Additional resources for classifications and definitions of information are available on Confluence:

1. Data Restriction Definitions provides definitions and examples of different types of data. This page is intended as a reference only and is available at https://confluence.uwf.edu/x/3YitB

2. Data Compliance and Restrictions by Service is a non-exhaustive list of services and software used at the University and the recommended security position regarding use of various types of restricted data. This page is intended as a reference only and is available at https://confluence.uwf.edu/x/14itB

3. UWF Data Phase Definitions defines different states or phases of data, including "data at rest," "data in use," and "data in transit," and provides guidance on best practices for handling data in each phase. This page is intended as a reference only and is available at https://confluence.uwf.edu/x/UQJd

IV. Policy

A. Departmental Information Security Representative (DISRep)

1. Each University Unit bears the responsibility of identifying and classifying the unit's information and ensuring the following practices are followed for information classified as protected or private:

   a. Maintain the identification, classification, and documentation of protected or private information assets within the unit.

   b. Assess the unit's electronic and physical controls for protected or private information to ensure they meet legislative and contractual requirements.

   c. Ensure unit staff is trained on this policy as well as legislative or contractual privacy requirements.

   d. Ensure that each unit staff member who handles protected or private information signs an Employee Statement of Understanding Regarding Confidentiality. Additional information on the employee statement of understanding is available at https://confluence.uwf.edu/x/wRXKE.

   e. Work with the Office of the General Counsel to ensure contracts contain terms that adhere to University policy, applicable laws, and contractual provisions when protected or private information is accessed, processed, transmitted, or stored by a third-party vendor.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

B. Access and Use – Authorized Users of Protected or Private Information

Access to information classified as protected or private requires appropriate authorization.

1. It is the responsibility of the designated Data Trustee or DISRep to authorize access to protected or private information only by users or entities as required for them to perform their assigned job duties, complete a business process, or complete contractual obligations.

2. All persons and entities that are provided access to view protected or private information as part of a statutory, regulatory, academic, or University business function must execute an Employee Statement of Understanding Regarding Confidentiality or an applicable UWF third-party access agreement. Background checks may be required prior to granting access to protected or private information.

3. An individual is authorized to access their own protected or private information unless restricted by legal or contractual obligations.

4. Legal or regulatory requirements may impact who is authorized to view protected or private information.

C. Confidentiality Statement and Privacy Training

Completion of designated training and a signed Employee Statement of Understanding Regarding Confidentiality are required for University personnel with authorization to access or process protected or private information.

1. Positions that require access to protected or private information must reflect such in the position description.

2. Each employee requiring access to protected or private information must have a signed Employee Statement of Understanding Regarding Confidentiality on file that is available for audit. This document may be stored in a digital or paper format.

3. Employees designated as having access to select protected information may be required to acknowledge and follow confidentiality controls necessary to meet specific legal or contractual privacy requirements.

4. Each University Unit must train its employees on the requirements to safeguard protected or private information. This training must occur prior to the employee's access to protected or private information or as required by law or contractual obligation. Employees must review this information and complete refresher training annually.

5. As verification of participation, each University Unit must maintain rosters of participants in online or in-person privacy training in an electronic or paper format.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

D. Approved Transfer of Protected or Private Information

1. The following actions involving protected or private information must be authorized by the responsible dean, director, department head, or designee and the related approval documentation must be maintained on file at the University Unit's office:

   a. Transferring protected or private information between University computing resources and third-party vendors or service providers.

   b. Allowing system and network administrators to access protected or private information to perform an approved action to mitigate a system problem or as part of an incident response to a privacy breach investigation.

2. ITS or the University Unit will coordinate with the Office of the General Counsel in the event of receiving a subpoena, warrant, legal order, or to meet a legal or contractual requirement for the transfer of protected or private information.

E. Third-party Access to Protected or Private Information

1. The University may choose to contract with a third-party for the collection, storage, or processing of information, including protected or private information. The third party may offer services in the form of hosting, outsourcing, or private/public cloud computing services.

2. If the University contracts with a third party for the processing of protected or private information, the agreement shall be in writing and describe the rights and duties of the University, the third-party contractor, and any subcontractors engaged by the primary third-party contractor. The selected third-party contractor shall guarantee the technical and organizational security and privacy measures required in this policy and provide sufficient guarantees with respect to the protection of the information.

3. The third-party contractor shall be contractually obligated to process protected or private information only within the scope of the contract and at the direction of the University. The third-party contractor shall not process protected or private information for any other purpose.

F. Physical Security Access Restrictions

1. Individuals who work in offices, home offices, other remote locations, and storage facilities that maintain protected or private information locally must:

   a. Ensure that all protected or private information in hardcopy or electronic form is secure in the work area at the end of the day or when they are expected to be gone for an extended period.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

b. Computer workstations that access, process, transmit, or store protected or private information must be secured in locked rooms when the workspace is unoccupied.

c. If the room cannot be secured, any protected or private information should be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

d. File cabinets containing protected or private information must be kept closed and locked when not in use or when left unattended.

e. Keys used for access to resources holding protected or private information must not be left unattended.

f. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

g. Printouts containing protected or private information should be immediately removed from the printer in unsecured areas.

h. Upon disposal, documents containing protected or private information should be shredded or placed in locked confidential disposal bins. Electronic media containing protected or private information that is no longer needed should be physically destroyed (e.g., shredded, degaussed, crushed) or wiped by electronic methods to render the information unreadable and unrecoverable as stipulated in National Institute of Standards and Technology-Special Publication 800-88 Revision 1 Guidelines for Media Sanitization.

i. Whiteboards containing protected or private information should be erased unless they are in secured areas. In addition, whiteboards with protected or private information should not be facing cameras or external windows unless blinds are drawn down to prevent unauthorized viewing of content.

j. Portable computing devices containing protected or private information such as laptops, phones, tablets, removable disks, or USB flash drives should be secured in locked rooms, file cabinets, or locked drawers after normal work hours; should require a password when that is an option; and should be encrypted.

2. Additional physical privacy controls may also be required by law or contractual obligation for specific information items.

G. Protected or Private Information Use in Social Media

The same laws, policies, rules of conduct, and etiquette that apply to all other activities at or concerning the University govern the use of social media. Faculty and staff should safeguard all protected or private information by only posting what they have permission to post by law, policy, or explicit statement.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

Further guidelines are available in University Policy PA-02, Social Media, as it may be amended.

H. Use of Biometric Technologies

University Units implementing biometric technologies must ensure they meet relevant privacy and biometric laws and regulations as they may relate to the acquisition and retention of biometric information. In addition, the University Unit must ensure that its use meets a defined business need and utilizes auditable procedures to secure the biometric information and privacy of the enrollees.

I. Online Collection of Protected and Private Information

University Units that collect protected or private information on their public or intranet web pages must ensure that:

1. Technical controls provide encryption of Protected information communicated between a user's browser and a web-based application through the use of secure protocols (e.g., HTTPS, TLS/SSL, etc.). In addition, any storage of protected or private data on publicly accessible servers must be encrypted. University websites collecting protected or private information require a link to this policy.

2. Prospective students, current students, faculty, staff, and interested parties residing outside of the United States and providing protected or private information electronically to the University understand this information will be transferred to the United States where it will be processed and stored under United States privacy standards or by applicable framework agreements.

J. Standards for Specific Information Types

1. Public Records

Faculty, staff, and contracted business partners must ensure the safekeeping of public records that have archival, administrative, or legal value. University Policy FIN-03, Records Management, as it may be amended, contains specific responsibilities for the retention, storage, disposal, and archival of University records. Archived information classified as protected or private information must be maintained with the same safeguarding controls, such as encryption, that are legislated or contracted for in production systems.

2. Student Education Records

a. The Family Educational Rights and Privacy Act (FERPA) (20 USC §1232g; 34 CFR Part 99) is a federal law that ensures access and protects the privacy of student education records. Section 1002.225, Florida Statutes, requires the University to protect applicant records and student education records in accordance with FERPA.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

FERPA governs:

i. The disclosure of education records maintained by an educational institution; and

ii. Access to those records.

b. The University has designated certain components of a student's Education Record as "Directory Information." Directory Information consists of information contained in an Education Record that would not generally be considered harmful or an invasion of privacy if disclosed. These items are classified as public information unless a student has chosen to restrict their directory information through the Privacy section in their MyUWF account, which places a privacy hold on the student's account, including Directory Information. Students who wish to have their privacy hold removed from their permanent academic record must contact the Office of the Registrar in writing or submit the change online through MyUWF. UWF Regulation 3.017, Student Education Records, as it may be amended, designates Directory Information.

3. EU General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR) is a privacy law that applies to the personal identifiable information collected from citizens or residents of the European Union (EU) or that is related to goods or services offered in the EU. The GDPR requires that the University process personal data lawfully, fairly, and in a transparent manner. Personal data that is collected must be collected for specified, explicit, and legitimate purposes.

The University collects or processes personal data for:

a. Legitimate interests pursued by the University or third parties in providing education, employment, research and development, and community programs.

b. For the performance of a contract.

c. Compliance with legal obligations to which the University is subject.

The University takes measures to protect personal identifiable information that is subject to the GDPR.

4. Social Security Numbers

a. Social Security Numbers (SSNs) are collected and stored as needed and as permitted by law. University Units and their employees are only permitted to collect or store SSNs when necessary to meet a state or federal requirement or the unit has obtained written approval from the President, Provost, Vice President,

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

General Counsel, IT Security Team, or other designated approver for the SSN to be used in an official business process.

b. The University requires all entities to maintain privacy controls over SSNs to meet legal, contractual, or good privacy practice requirements, including:

i. UWFIDs are to be used instead of SSNs for routine university business.

ii. Collection, storage, or processing of SSNs is restricted to systems that serve the student, financial, and human resource Enterprise Resource Planning (ERP) systems.

iii. SSNs must not be stored on University-owned personal computing devices or transferred to vendor storage services, including cloud computing resources, unless appropriate management approval and execution of an information sharing agreement is granted for mission-critical University business activities.

iv. SSNs must not be stored on University-owned or personal portable storage devices or mobile computing devices.

v. SSNs or partial SSNs should never be displayed in areas where it is not possible to restrict access to only those approved to view SSNs.

vi. Any approved business process requiring the transfer of electronic documents containing SSNs over the University network, internet, or a wireless carrier's network requires the encryption of the transferred documents between the user's computing device and University information processing equipment.

vii. Any required mailing of paper documents containing SSNs must be done in a manner that reduces the risk of displaying SSNs before the document is opened.

viii. Where possible, SSNs should be truncated to only the last four digits.

5. Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999

a. The University generates, receives, and stores many financial documents and records classified as protected. This includes, but is not limited to, information about the awarding and issuance of loans to students, as well as the collection of payments from students, parents, and customers via check, money order, wire transfer, Automated Clearing House (ACH), and credit or debit card. The GLBA applies to any record handled or maintained by or on behalf of the University or its affiliates that contains protected financial information about a student or other third party who has a relationship with the University.

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

b. GLBA safeguarding provisions pertain to any record containing protected financial information, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the University or its affiliates. For these purposes, the term "protected financial information" shall mean any information (i) a student or other third party provides the University in order to obtain a financial service from the University, (ii) about a student or other third-party resulting from any transaction with the University involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. In particular, safeguarding provisions of this policy and the University's security policy (a) ensure the security and confidentiality of covered records, (b) protect against any anticipated threats or hazards to the security of such records, and (c) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

c. All University contracts with providers who are responsible for processing, transferring, or storing GLBA-protected information will be required, under the terms of the contract, to stipulate implemented safeguards that adhere to and comply with the provisions of the Gramm-Leach-Bliley Act.

6. Branded Credit or Debit Card Transactions

The University will collect and use information obtained from branded credit or debit card transactions (VISA, MasterCard, American Express, and Discover) only for business purposes upon approval by the Controller's Office. The credit card information will be safeguarded in a confidential manner as defined in the PCI DSS Compliance section of the University Compliance and Ethics web page at https://uwf.edu/PCIDSS, and as specified in the merchant agreements as contractual obligations. Such obligations include compliance with the Payment Card Industry - Data Security Standard (PCI DSS).

7. Research Information

University Units conducting research must be aware of appropriate privacy restrictions for information accessed, transmitted, stored, or processed as part of research projects. Research project data is also a required component of a University Unit's yearly data classification, risk assessment, and risk mitigation planning. Legal privacy restrictions include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA), International Traffic in Arms Regulations (ITAR), The Belmont Report (1979), 2.1 Code of Federal Regulations Title 45 Part 46: The Common Rule concerning the protection of human subjects, other federal or state legal requirements, and contractual research information privacy restrictions. In addition, University Units must protect the privacy of protected or private research information with appropriate information privacy and security controls such as those published by the National Institute of Standards and Technology (NIST), ISO, or Federal Information Security Management Act (FISMA). Required information privacy and security controls extend

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

to any device used to access, transmit, store, or process protected or private research information.

K. Privacy Violations and Incident Reporting

1. Privacy violations occur when a University student, staff, contractor, or faculty member violates this policy, specific legal privacy requirements, or contractual obligations. For the purpose of this policy, there are three primary classifications of privacy violations:

   a. "Incidental disclosure" occurs when an unauthorized party overhears or sees protected or private information during a permitted use or disclosure in a work space.

   b. "Accidental disclosure" occurs when privacy control weaknesses allow unauthorized access to protected or private information. Privacy control weaknesses include human error or a fault in privacy control procedures that leads to a loss of ability to limit access to protected or private information to only authorized users.

   c. "Intentional disclosure" occurs when privacy controls are overridden to allow unauthorized access or disclosure of protected or private information. This can be done with or without malicious intent.

2. It is the responsibility of each student, staff, contractor, or faculty member to immediately report suspected or confirmed disclosure incidents to their supervisor or contract administrator, including accidental disclosures. If the supervisor or contract administrator is unavailable or if there is a potential conflict of interest, the report should be directed to the dean, director, department head, IT security team, or through the ITS Help Desk. The dean, director, or department head, must inform the IT security team of any suspected or confirmed privacy breaches within 24 hours. Refer to the Incident Response guidelines located at https://confluence.uwf.edu/x/eoU8Ag for further incident handling procedures.

L. Emergency Situation

The ITS Director, the Chief Information Security Officer (CISO), or both, upon verbal or written approval from the President or Provost, have the authority in an emergency situation to take immediate action that is required to secure the University's network or respond to a security breach. Any such action shall be reported to the President and Provost at the earliest opportunity.

Approved by: Signed by: Martha Saunders D54A387C376848D... **Date:** 05/01/2025

Dr. Martha D. Saunders

Docusign Envelope ID: 04AE9404-F8F5-4077-9726-CE4396D83D25

Authority: The Florida Constitution, Article IX, Section 7
BOG Reg. 1.001 and 3.0075
Chapters 119 and 257, Florida Statutes
§§501.171, 1002.21, 1002.22, 1004.22(2), 1006.52, 1012.91, and 1002.225, Florida Statutes
Chapter 1B-24, 1B-26.003, Florida Administrative Code
The European Union General Data Protection Regulation Privacy Act of 1974
The Gramm-Leach-Bliley Act, 15 U.S.C. §6801, implemented by 16 CFR Part 314
Payment Card Industry Security Standards Council (PCI SSC). (2023, September 20) Payment Card Industry Data Security Standard (PCI DSS) v4.0. https://www.pcisecuritystandards.org/document_library/

Cross Ref.: UWF Regulation 3.017, Education Records
UWF Policy PA-02, Social Media
UWF Policy FIN-03, Records Management

History: Adopted March 2016; revised October 2018 and May 2025

Last Review: May 2025