Policy

University Policy IT-04.02-11/18

TO: The University of West Florida Community

FROM: Dr. Martha D. Saunders, President

SUBJECT: UWF Information Security and Privacy Policy

Responsible Office: Information Technology Services

I. Purpose:

The University of West Florida (UWF) 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 UWF'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, UWF 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. Who Does this Govern and Who Needs to Know this Policy?

This Privacy Policy applies to all faculty, staff, students, affiliates, prospective students, contractors and sub-contractors, and associated parties who interact with UWF systems to process, transmit, or store UWF information classified as protected or private on:

A. UWF-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 who 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.

III. Information Classification and Definition of Terms:

A. Classification-

For the purpose of this policy, information will be classified as follows:

1. The **Protected** classification encompasses information deemed confidential under federal or state law or applicable regulations, UWF contractual obligations, or privacy considerations such as the combination of names with respective Social Security Numbers.

2. The **Private** classification 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 information indicating that information should be classified as public or protected.

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

B. Definitions-

1. **Personal identifiable information (PII)** means any information relating to an individual or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly – in particular, 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.

2. **Education records** are those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. See UWF Regulation 3.0.17 for more information regarding educational records at UWF.

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

4. **Data Trustees** are the Executive Vice President and the Heads of each Division at UWF; they are responsible for the major categories of university data for their respective areas.

5. **Information Systems Coordinating Group (InfoSys)** members are endorsed by a Data Trustee to manage a subset of data. The designated member is responsible for the accuracy, privacy, and integrity of a university data subset.

6. **University Unit** refers to a school or college and any departments or divisions which are a subdivision of a college or school; centers, facilities, labs, libraries, or program within a college or school, or as an independent entity; offices; associations; and administrative units.

C. Information Privacy Principles-

1. Protected or Private information must be safeguarded.

2. Employ the agreed upon conditions with third-party entities.

3. Collect only protected or private information needed to support a business process.

4. Keep protected and private information no longer than required by law or business need.

D. Consequences-

Disciplinary action for violating this policy could be taken under the UWF's current Standards for Disciplinary Action for the violation of a provision of a UWF Policy.

IV. Policy Statement:

A. Resources-

1. Departmental Information Security Representative (DISRep). Each University unit bears the responsibility to identify and classify the unit’s information and to ensure the following standards are followed for information classified as protected or private. DISReps are also expected to carry out a particular set of responsibilities:

i. Maintaining the information identification and classification documentation of unit protected or private information assets.

ii. Assessing the unit's electronic and physical controls for information classified as protected or private to ensure they meet legislated or contracted requirements.
iii. Ensuring unit staff is trained on this policy, and specific legislated or contracted privacy requirements.
iv. Ensuring that each unit staff member who handles protected or private information sign an employee statement of understanding regarding confidentiality.
v. Working with legal resources to ensure contracts or agreements contain terms to stipulate adherence to UWF policy, legislation, or contractual safeguarding provisions when protected or private information is processed, transmitted or stored by a third-party vendor.

B. Training-

UWF will make available to the DISRep, and the university in general, standardized information privacy training. This training will provide appropriate privacy training for all Faculty, Staff and students.

C. Forms-

Employee statement of understanding regarding confidentiality.

D. Procedures-

IT Security and Privacy Incident Response and Reporting Procedures.

E. Guidelines-

1. UWF Information Classification Guidelines.

2. Guidelines for the use of personal cloud computing services for UWF Business.

F. Access and Use-

1. Authorized Users of Protected or Private Information. Access to UWF information classified as protected or private requires appropriate authorization:

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

ii. For an individual not employed by UWF or third parties who are authorized to view protected or private information as part of a regulatory, academic, or business function, the sharing UWF unit must have a signed Employee Statement of Understanding Regarding Confidentiality on file for individuals or UWF data sharing terms and conditions for third parties. Additionally, background checks may be required prior to granting access to UWF protected or private information.

iii. The individual whose protected or private information is produced or displayed is authorized to access that information unless restricted by legal or contractual obligations.

iv. Legal or regulatory requirements may impact who is authorized to view UWF protected or private information access.

G. Confidentiality Statement and Privacy Training-

1. Signed Employee Statement of Understanding Regarding Confidentiality and training are required for UWF personnel with authorization to access or process protected or private information:

i. Each UWF position requiring access to protected or private information must be reflected in the position description.

ii. For each person requiring access to protected or private information, signed Employee Statement of Understanding Regarding Confidentiality must be maintained on file unit and be available for audit. This information may be stored in a digital or paper format.

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

iv. Each unit must train its employees on the requirements to safeguard protected or private information. This training should occur prior to employee access of protected or private information or as required by legislation or contractual obligation

v. 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.

H. 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 related approval documentation or contract/agreement maintained on file at the unit's central office:

   i. Transferring protected information between UWF computing resources and third-party vendors or service providers.

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

2. Coordinate with the UWF Legal Office in the event of receiving a valid subpoena, warrant, legal order, to meet a legal or contractual order for the transfer of protected information.

I. Third-party Access to Protected or Private Information-

1. UWF 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 UWF decides to contract a third-party for the processing of protected or private information, this must be regulated in a written agreement, in which the rights and duties of UWF and the third-party contractor in addition to any subcontractors engaged by the primary third-party contractor are specified. A third-party contractor shall be selected that will guarantee the technical and organizational security/privacy measures required in this privacy policy and provide sufficient guarantees with respect to the protection of the information.

3. A third-party contractor should also be contractually obligated to process protected or private information only within the scope of the contract and the directions of UWF. Processing of protected or private information may not be undertaken for any other purpose.

J. Physical Security Access Restrictions-

1. Offices and storage facilities that maintain protected or private information locally must:

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

ii. Computer workstations processing, transmitting, or storing protected or private information must be secured by locked rooms when the workspace is unoccupied.

iii. 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 if the room cannot be secured.

iv. File cabinets containing protected or private information must be kept closed and locked when not in use or when not attended.

v. Keys used for access to resources holding protected or private information must not be left at an unattended desk.

vi. 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.

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

viii. Upon disposal, documents containing protected or private information should be shredded or placed in the locked confidential disposal bins. Electronic media containing protected or private information that is no longer needed should be physically destroyed (e.g., shred, degauss, 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.

ix. 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 external windows unless blinds are drawn down to prevent unauthorized viewing of content.

x. Portable computing devices containing protected or private information such as laptops phones, tablets, CDROMs, DVDs, USB flash drives should be secured in locked rooms, file cabinets, or locked drawers after normal work hours.

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

K. Use of Biometric Technologies-

University units implementing biometric technologies must ensure they meet any 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 with auditable procedures to secure the biometric information and privacy of the enrollees.

L. Online Collection of Protected and Private Information-

1. Campus units that collect protected or private information on their public or Intranet web pages must ensure 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 requires a link to the UWF Privacy 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 UWF understand this information will be transferred to the U.S. where it will be processed and stored under U.S. privacy standards or by applicable framework agreements.

V. Standards for Specific Information Types:

A. Public Records-

UWF faculty, staff, and contracted business partners must ensure the safekeeping of public records that have archival, administrative, or legal value. The UWF records management policy (FIN-03.02-02/14) linked under the Public Records Management website contains specific responsibilities for the retention, storage, disposal, and archival of UWF 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 production systems.

B. Student Educational Records-

1. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that ensures access and protects the privacy of student education records. Florida Statute 1002.225 requires UWF to protect applicant records and student education records, in accordance with FERPA.

    i. The disclosure of education records maintained by an educational institution.
    ii. Access to these records.

2. UWF has defined certain components of a student's education record as "Directory Information." "Directory Information" means information contained in an education record of a student 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 flag removed from their permanent academic record must contact the Office of the Registrar in writing or may submit the change online through MyUWF. UWF regulation 3.017 contains the current information designated as educational records at UWF.

3. EU General Data Protection Regulation. The European Union General Data Protection Regulation is a privacy law that applies to the personal identifiable information collected in or from the European Union (EU), or that is related to goods or services offered in the EU. The GDPR requires that UWF process personal data lawfully, fairly and in a transparent matter. The personal data collected by UWF must be collected for specified, explicit and legitimate purposes.

4. UWF collects or processes personal data for:

    i. Legitimate interests pursued by UWF or third parties in providing education, employment, research and development, and community programs.

ii. For the performance of a contract.

iii. Compliance with legal obligations to which UWF is subject.

5. UWF is taking measures to protect personal identifiable information that is subject to the GDPR.

C. Social Security Numbers-

1. UWF collects and stores Social Security Numbers (SSNs) 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, General Counsel, IT Security Team, or designated approver to meet an official business process.

2. UWF requires all entities 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 UWF automated systems that serve the Enterprise Resource Planning (ERP) student, financial, and human resource systems.

iii. SSNs must not be stored on UWF-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 UWF business activities.

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

v. SSNs or partial SSNs should never be displayed in areas such as public locations 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 internal UWF network, Internet, or a

wireless carrier's network requires the encryption of the transferred documents between the users computing device and UWF 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.

D. Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLB)-

1. UWF 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, and the collection of payments from students, parents, patients and customers via check, money order, wire transfer, Automated Clearing House (ACH) and credit/debit card. GLB (Public Law 106-102) applies to any record handled or maintained by - or on behalf of - UWF or its affiliates that contains protected financial information about a student or other third-party who has a relationship with UWF.

2. GLB safeguarding provisions pertain to any record containing protected financial information whether in paper, electronic or other form, which is handled or maintained by or on behalf of the UWF or its affiliates. For these purposes, the term protected financial information shall mean any information (i) a student or other third-party providers in order to obtain a financial service from UWF, (ii) about a student or other third-party resulting from any transaction with UWF 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 UWF's security policy (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

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

E. Branded Credit/Debit Card Transactions-

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

F. Research Information-

University units conducting research must be aware of appropriate privacy restrictions for information transmitted, stored, or processed as part of research projects. Research projects are 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) and 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 to any device used to transmit, store or process protected or private research information.

VI. Privacy Violations and Incident Reporting

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

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

2. 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.

3. 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.

B. It is the responsibility of each UWF student, staff, contractor, or faculty member to immediately report suspected or confirmed incidents to their supervisor or contract administrator including accidental incidents. 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 UWF ITS Help Desk. The Dean, Director, Department Head, or Inspector General must inform the IT Security Team of any suspected or confirmed privacy breaches within 24 hours. Refer to the UWF Incident Response Guidelines for further incident handling procedures.

VII: Authority and Related Documents:

The Florida Constitution, Article IX, Section 7; the Florida Board of Governors Regulations 1.001 and 3.0075; Chapters 119 and 257; Sections 1002.21, 1002.22, 1004.22(2), 1006.52, 1012.91; 1002.225; Chapter, 1B-24, 1B-26.003; Florida Administrative Code Chapter 501.171; the Florida Information Protection Act (FIPA); Family Educational Rights and Privacy Act (FERPA); the European Union General Data Protection Regulation (GDPR); the Americans with Disabilities Act (ADA); Privacy Act of 1974, as amended; 15 U.S.C. 6801, implemented by 16 CFR Part 314, the Gramm-Leach-Bliley Act (GLB Act) ; and the Federal Trade Commission (FTC) Rule on "Standards for Safeguarding Customer Information" Payment Card Industry Data Security Standard (PCI DSS).

Approved by: _____ **Date:** 11-1-18
Dr. Martha D. Saunders, President

History: IT-04.02-10/18 with substantive and procedural changes; IT-04.01-03/16 University of West Florida Information Security and Privacy Policy, adopted March 2016.