THE LEADER IN GLOBAL EDUCATION

FAIRLEIGH DICKINSON UNIVERSITY

Written Information Security Program (WISP)

Responsible Office:	Office of Information Resources and Technology		Effective Date: 05/28/2024
Responsible Official:	Chief Information Security Officer	Last Revision:	12/01/2022
		Last Review:	05/13/2024

I. OBJECTIVE

The objective of Fairleigh Dickinson University ("University") in the development and implementation of this comprehensive Written Information Security Program ("WISP") is to create effective administrative, technical and physical safeguards for the protection of Personal Information ("PI") and Protected Health Information ("PHI"). The WISP sets forth the University's procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PI and PHI.

For purposes of this WISP, PI means:

1) User name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account.
2) Biometric data that can uniquely identify a person based on their physical, behavioral, or physiological characteristics. These characteristics can include:
   a) Fingerprints
   b) Palmprints
   c) Voiceprints
   d) Facial, retinal, or iris measurements
   e) Handwriting and signature
   f) Facial geometry (the shape of a person's face)

3) Someone's name and any one of the following data elements:

   A. Social Security number, Social Insurance number, National Insurance number, or equivalent;

   B. Date of birth (MM/DD/YYYY),

   C. Driver's license number, state-issued identification card number, or provincially-issued identification card number;

   D. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account;

E. Passport number;

F. Medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or health insurance information; or

G. Student/Employee (i.e., Datatel) ID number coupled with a password or security question and answer or any portion of any item in the list above that would permit access to an online account.

For purposes of this WISP, PHI includes information that is created, received, and/or maintained by the University that is related to an individual's health care (or payment related to health care) that directly or indirectly identifies the individual.

PI or PHI shall not include information that is lawfully obtained from publicly available information, or from federal, state, provincial or local government records lawfully made available to the general public.

Notwithstanding the above and irrespective of whether or not it's considered PII or PHI, one should always take care and caution to use the minimum data elements necessary to perform the business function at hand.

All University employees except those listed under section IX must complete online or in-person WISP training and test with a passing score of at least 80% every 24 calendar months.

II. PURPOSE

The purpose of the WISP is to better:

1) Ensure the security and confidentiality of PI and PHI;

2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE

In formulating and implementing this WISP, the University has addressed and incorporated the following protocols:

1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI and PHI;

2) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PI and PHI;

3) evaluated the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks;

4) designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of the regulations in this document; and

5) implemented regular monitoring of the effectiveness of those safeguards.

IV. DATA SECURITY COORDINATOR

The University has designated the Chief Information Security Officer (CISO), working together with the Chief Information Officer (CIO) and the Data Security Information Response Team (DSIRT), to implement, supervise and maintain the WISP. See Appendix II for contact information for the CISO, CIO and DSIRT. Together, they will be responsible for:

1) Initial implementation of the WISP;

2) Regular testing of the WISP's safeguards;

3) Evaluating the ability of each of the University's third party service providers to implement and maintain appropriate security measures for the PI and PHI to which the University has permitted them access, consistent with the regulations outlined in this document; and requiring such third party service providers by contract to implement and maintain appropriate security measures;

4) Reviewing the scope of the security measures in the WISP at appropriate intervals, including the review of any material change in the University's business practices that may implicate the security or integrity of records containing PI and PHI; and

5) Conducting in-person or online, synchronous or asynchronous, training sessions for all University employees, and independent contractors, including temporary and contract employees on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with University requirements for ensuring the protection of PI and PHI.

V. INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI and PHI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and effective immediately:

Internal Threats

1) The University shall only collect PI and PHI of students, their parents, alumni, donors, suppliers, vendors, independent contractors or employees that is necessary to accomplish the University's legitimate need to access said records, and for a legitimate job-related purpose, or necessary for University to comply with state, provincial, or federal regulations.

2) Access to records containing PI and PHI shall be limited to those persons who are reasonably required to know such information in order to accomplish a University legitimate business purpose or to enable the University to comply with state, provincial or federal regulations.

3) All persons who fail to comply with this WISP shall be subject to disciplinary measures, up to and including termination, irrespective of whether PI and PHI was actually accessed or used without authorization. Any such discipline shall be in accordance with processes and procedures of Human Resources and subject to any protections afforded under the University's agreement with "Office & Professional Employees International Union", the "Faculty Handbook", and similar documents.

4) Access to PI and PHI shall be restricted to authorized University personnel only.

5) Any PI and PHI stored shall be disposed of when no longer needed for business purposes or required by law for storage. Paper or electronic records (including records stored on hard drives or other electronic media) containing PI and PHI shall be disposed of only in a manner that complies with the regulations outlined in this document and as follows:

    a) Paper documents containing PI and PHI shall be shredded upon disposal so that PI and PHI cannot be practicably read or reconstructed; and

    b) Electronic media and other non-paper media containing PI and PHI shall be destroyed or erased upon disposal so that PI and PHI cannot be practicably read or reconstructed.

6) A copy of this WISP must be distributed to each current University employee and to each new University employee at the commencement of their employment.

7) Procedures for Terminated Employees (whether voluntary or involuntary)

    a) Terminated employees must return all records containing PI and PHI, in any form that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

    b) A terminated employee's physical and electronic access to PI and PHI shall be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled.

8) Physical Assets Protocol

    a) All assets must be secured from theft by locking up and maintaining a secure workplace, whether that work takes place in University stores, offices, at a client site, in a car, hotel or in a home.

        i) All University laptops shall be deployed with encryption capabilities enabled. End users may not disable such encryption. Exceptions to this policy are as follows:

            (1) With the explicit written authorization of the CISO;

            (2) May be disabled by OIRT personnel for temporary maintenance purposes only;

            (3) Loaner laptops temporarily assigned with the understanding they will not be used to store or access any information that is considered to be protected under this policy.

ii) All laptops should be placed in the trunk of vehicle when and wherever they are parked. If no secure trunk or other storage is available, employees should, whenever possible, keep their laptops in their possession or find a way to secure and conceal it.

iii) Laptops, PDAs, phones and other portable devices that may contain or have access to PI and/or PHI left in the office or at home over night should be kept in a locked and secure location.

iv) Employees must have assets secured or within their physical possession while on public or private transportation, including air travel.

v) Files containing PI and/or PHI are not to be stored on local computer hard drives, shared drives or other external media (which include externally hosted services such as, but not limited to OneDrive, Google, and Drop Box) without prior written authorization from the CISO. If approved, the method of storage and access to the data will be determined by the CISO during the discussion and placed in writing. (See Appendix I for more detail).

9) Access Control Protocol

a) Access to electronically stored PI and PHI shall be electronically limited to those University employees having a unique log-in ID.

b) Employees must ensure that all computer systems under their control are locked when leaving their respective workspaces. Employees must not disable any logon access.

c) Employees must log off of the VPN or Virtual Desktop (VDI) when they are not directly using those resources.

d) All Ellucian (Datatel) sessions that have been inactive for 60 or more minutes shall require re-log-in.

e) After 5 unsuccessful log-in attempts by any Ellucian (Datatel) or MS Active Directory NetID, that user ID will be blocked from accessing those systems until access privileges are re-established by University Systems and Networking.

f) Employees must maintain the confidentiality of passwords and access controls:

i) All Ellucian (Datatel) or MS Active Directory NetID passwords are required to adhere to strong password rules.

ii) All Ellucian (Datatel) or MS Active Directory NetID passwords are required to be changed every 3 months.

iii) Employees must not share accounts or passwords with anyone.

iv) Employees should not record passwords on paper or in a document or in a place where someone other than the employee might have access to it. Tip: The University has identified a password vault application (Keepass, Dashlane or

Lastpass); those interested should open a ticket with the UTAC requesting assistance on setting it up.

g) Where practical, all external or internal visitors to a department are restricted from areas where files containing PI and PHI are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containingPI and PHI are stored.

10) Educational Records
    a) The Family Educational Rights and Privacy Act (FERPA) of 1974 prohibits educational institutions from disclosing education records without the written consent of an eligible student.
    b) Limited exceptions to non-disclosure include directory information and specific school officials with a legitimate educational interest.
    c) The transmition of education records covered under FERPA must follow the same PI/PHI guidelines as depicted in Appendix I of this policy.

VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI and PHI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and effective immediately:

External Threats

1) Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes PI and PHI.

2) All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes PI and PHI.

3) To protect against external threats, all PI and PHI shall be handled in accordance with the protocols set forth above under “Internal Threats”.

4) In the event an individual inadvertently discovers he/she received PI or PHI from an external party, such PI or PHI shall be handled in accordance with the protocols set forth under “Internal Threats”.

5) There shall be secure user authentication protocols in place that:

    a) Control user ID and other identifiers;

    b) Assigns passwords in a manner that conforms to accepted security standards, or applies the use of unique identifier technologies;

    c) Control passwords to ensure that password information is secure.

6) PI and PHI shall not be removed from the business premises in electronic or written form absent a legitimate business need and use of reasonable security measures, as described in this WISP.

a) PI and/or PHI that MUST be transmitted in electronic form shall not be sent without encryption.

b) PI and/or PHI in paper form must be secured.

7) All computer systems shall be monitored for unauthorized use or access to PI and PHI.

VII. IN CASE OF LOSS/THEFT OR SUSPECTED LOSS/THEFT

If you have reason to believe that any PI or PHI has been lost or stolen or *may* have been compromised or there is the potential for identity theft, regardless of the media or method, **you must** report the incident immediately by contacting the University Technical Assistance Center ("UTAC") at 973-443-8822. The UTAC is available 24 x 7.

VIII. OTHER APPLICABLE POLICIES

Acceptable Use Policy For Computer Usage https://it.fdu.edu/acceptable-use-policy-for-computer-usage/

Confidentiality Agreement and Security Policy https://it.fdu.edu/confidentiality-agreement-and-security-policy/

Policy for Acceptable Use of Email https://it.fdu.edu/policy-for-acceptable-use-of-email/

Data Security Information Response Plan (September 15, 2019, not published on Web)

IX. EXCEPTIONS

The following groups are exempt from taking the mandated bi-annual WISP training as described in section I of this policy:

a. Those currently not employed by the University but who are granted Net ID's with only email access (no other access to FDU IT resources or services).
b. Retired full-time faculty not employed by the University but who are granted email access for life as a retired tenured full-time faculty member.
c. Retired full-time executive emeritus not employed by the University but granted email access for life as a retired full-time executive emeriti.

Requests for other exceptions to this policy should be directed in writing to the Chief Information Security Officer. Only the Chief Information Security Officer in consultation with the DSIRT may grant such exceptions and will do so only after careful review and in writing.

X. REVIEW

This policy shall be reviewed annually by the Data Security Incident Response Team (DSIRT) at the first meeting in April.

Appendix I

Technical requirements for the storage of files containing PI or PHI regardless of where the storage occurs will include but not be limited to the following:

1) All file(s) and/or emails should be secured with AES 256bit encryption unless actively open for review or modification.
2) It is the responsibility of the person handling the PI or PHI file to securely delete any files created as a product of the manipulation of those files. As an example, temporary files created by Microsoft Office programs or any other programs would need to be securely deleted as well as the clear text versions of the original file after the encrypted version is properly created and verified.
3) Programs used for Encryption/Decryption and secure file deletion must be approved by the CISO including the methods in which they are to be used.
4) If the complete or partial PI or PHI containing file(s) are inadvertently written to a local hard drive, it is the user's responsibility to diligently make sure the contents are securely deleted.

Appendix II

DATA SECURITY INCIDENT RESPONSE TEAM (ROLES AND RESPONSIBILITIES)

The Data Security Incident Response Team membership includes the Chief Operating Officer, the Chief Information Officer, the Chief Information Security Officer, the Chief Academic Officer, the University General Counsel and the University Risk Manager. Each member of the Data Security Incident Response Team (DSIRT) has responsibilities related to the security of all the organization's sensitive information. The DSIRT members listed below have specific responsibilities with regard to the reporting and handling of data security incidents. Note that one person may serve in multiple roles.

Senior Vice President and Chief Financial Officer: Frank Barra
Daytime telephones: office: 201-692-2237; Email: fbarra@@fdu.edu

Chief Information Officer (CIO): NEAL STURM
Daytime telephones: office: 201-692-8689; Email: sturm@fdu.edu

Chief Information Security Officer (CISO): Kimberley Dawn Dunkerley
Daytime telephones: office: 201-692-7672; Email: ddunkerley@fdu.edu

Privacy Officer: Kimberley Dawn Dunkerley
Daytime telephones: office: 201-692-7672; Email: ddunkerley@fdu.edu

Senior Vice President and University Provost: Benjamin Rifkin
Daytime telephones: Office: 201-692-7093; Email: brifkin@fdu.edu

Office of the General Counsel: Steve Nelson
Daytime telephones: office: 201-692-2466; Email: snelson@fdu.edu

University Risk Manager: GAIL LEMAIRE
Daytime telephones: office: 201-692-7083; Email: lemaire@fdu.edu

Vancouver Campus Executive: Wilfred Zebre
Daytime telephone: office: 604-648-4462; Email: wilfred_zerbe@fdu.edu

Associate Vice President for MIS: Saul Kleinman
Daytime telephone: Office: 201-692-2065; Email: saul@fdu.edu