JOHNSON & WALES UNIVERSITY

Written Information Security Plan (WISP)

I. Objective

The objective of Johnson & Wales University (JWU) in the development and implementation of this Written Information Security Plan (WISP) is to create effective administrative, physical, and technical safeguards for the protection of personal information of JWU employees, students/alumni, and other persons as the university deems appropriate ("Protected Persons").

II. Purpose

As reasonably possible, to:

1. Maintain the confidentiality, integrity, and security of the university's records.
2. Protect against anticipated threats or hazards to those records.
3. Protect against unauthorized access to those records.

III. Scope

A. The provisions of the WISP apply to the access, creation, destruction, disclosure, security, storage, and transit of electronic and hardcopy records.

B. The university is subject to significant regulations with respect to how it collects, discloses, secures, stores, transmits, and uses personal information. In formulating and implementing the WISP, the university seeks to address a myriad of requirements under multiple laws and regulations and industry standards, including (among others):

   1. Applicable state information security requirements with respect to sensitive personal information.
   2. The Family Educational Rights and Privacy Act (FERPA).
   3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule with respect to the Employee Health Care Plan and the Health Information Technology for Economic and Clinical Health Act (HITECH) and applicable state laws governing health information.
   4. The Standards for Safeguarding Customer Information under the Gramm-Leach Bliley Act (GLBA) set forth by the Federal Trade Commission (FTC). Payment card industry (PCI) standards with respect to credit card information.

C. This policy is in addition to, but does not replace, existing university policies regarding the disclosure, privacy, and use of personal information and detection and mitigation of identity theft.

IV. Personally Identifiable Information (PII)

A. Certain personal information about Protected Persons must be protected by the university in accordance with strict security procedures set forth in laws and regulations and industry standards.

B. Definitions

   1. PII means:

a) An individual's first and last name or first initial and last name (or other information where there is a reasonable basis to believe that information can be used to identify an individual) **in combination with** any one or more of the following:
   (1) Social Security Number
   (2) Financial account number (e.g., a checking, savings, student identification number (J#), etc.)
   (3) Driver's license number or government-issued identification number (including Individual Taxpayer Identification Number (ITIN), Internal Revenue Service (IRS) identity protection PIN, or passport number)
   (4) Any numbers or information that can be used to access a person's financial accountsor financial resources, including but not limited to:
      (a) Account passwords.
      (b) Electronic identification numbers.
      (c) Internet account numbers.
      (d) Internet identification names.
      (e) PINs or other access codes.
      (f) Financial information that the university has obtained **from or about** any individual in the process of the university or a third-party financial institution offering a financial product or service to that individual.
         (i) "Offering a financial product or service" includes check cashing services, conducting collection activities, offering loans, receiving income tax information from a parent when offering a financial aid package, servicing loans, and other miscellaneous financial services.
      (g) All nonpublic information provided **by or with respect to** any student or the student's family with respect to financial aid, loans, payment plans, or such student's financial account shall be considered PII.
      (h) Digital signatures (a mathematical scheme or another agreed upon method for demonstrating the authenticity of a digital message or document).
      (i) User name or e-mail address in combination with a password or security question and answer that would allow access to a university system reasonably likely to contain other PII.
      (j) Biometric data (such as facial images (including identification video), fingerprints, voiceprint, etc.).
      (k) Parent's legal last name prior to marriage.
      (l) Employee Health Care Plan Information (i.e., individually identifiable health information of employees and their dependents, including demographic informationcollected from such individuals), that:
         (i) is created or received by the university in its capacity as administrator of the university's Employee Benefit Plan.
         (ii) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual,

or the past, present, or future payment for the provision of health care to a participant in the Employee Benefit Plan); and

(iii) is maintained in electronic media or transmitted in electronic media).

(iv) Not included within this category are medical records of employees received by the university in its capacity as an employer, workers' compensation records, student education records, and student treatment records.

(m) Medical records of students attending JWU Health Services or Counseling Services.

(n) Any combination of the above elements that would enable a person to commit identity theft without reference to a person's first name or first initial and last name; OR

b) Credit card or debit card cardholder data ("Cardholder Data"), including the expiration date, the primary account number, and the security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, personal identification numbers (PINs), and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions, in each case with or without any required access code, PIN, password, or security code that would permit access to a person's financial account.

V. **Responsibility and Accountability**

A. The DIS is responsible for:

1. Reporting in writing, regularly and least annually to the board of trustees. The report shall include the following information:
   a) The overall status of the WISP and compliance with the WISP.
   b) Material matters related to this WISP, addressing issues such as control decisions, results of testing, risk assessments, risk management, security events or violations and responses thereto, service provider arrangements, and recommendations for changes in this WISP.
2. Developing and implementing the WISP, including physical and electronic security and data handling requirements and procedures; these procedures may include the access, capture, maintenance, storage, transportation, and use of PII.
3. Completing and documenting periodic written risk assessments to identify reasonably foreseeable internal and external risks to the confidentiality, integrity, and security of PII that could result in the unauthorized access, alteration, destruction, disclosure, misuse, or other compromise of such information and determine whether any safeguards in place are sufficient to control these risks.
   a) Such written risk assessment will include the following information:
      (1) Criteria for the evaluation and categorization of identified security risks or threats.
      (2) Criteria for the assessment of the confidentiality, integrity, and availability of university information systems and PII, including the adequacy of the existing

controls in the context of the identified risks or threats.

(3) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the university will address the risks.

b) The risk assessments will review, among other things:

(1) Employee training.

(2) IT network and software design.

(3) Information system activity and identification of inappropriate useractivity.

(4) Information disposal, processing, storage, and transmission.

(5) The results of on-going testing and monitoring of safeguards and procedures.

(6) The university's ability to detect, prevent, and respond to attacks, intrusions, and system failures.

(7) An inventory of all hardware and software systems that are used to collect, process, store, or transmit PII. This inventory shall include a designation of the type of data stored on the system (education record, employee, financial, health, student, etc.).

(8) Training all employees, at least annually, who have access to PII on the elements of the WISP and issuing periodic security reminders.

(9) Ongoing testing and monitoring of the WISP's safeguards and procedures.

(10) The scope of the security measures in the WISP at least annually or whenever there is a material change in the university's business practices that may implicate the security or integrity of records or as necessary to address changing security risks.

(11) The ability of each proposed service provider to the university to implement and maintain appropriate confidentiality, integrity, and security measures for the personal information to which the university has permitted them access; requiring those service providers by contract to implement and maintain appropriate procedures and training consistent with applicable legal requirements; and reviewing the compliance of the service providers with such requirements.

(12) An inventory of types of data stored by service providers and any breach notification provisions in service provider contracts.

(13) The response to actual or suspected breaches of the integrity, confidentiality or security of PII, including utilizing the university's Incident Response Plan.

(14) Questions regarding the WISP.

(15) Any failure to comply with the WISP or its corresponding procedures.

c) Additional risk assessments will be conducted to reexamine any reasonably foreseeable internal and external risks to the confidentiality, integrity, and security of PII that could result in the unauthorized alteration, destruction, disclosure, misuse, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

4. Designing and implementing safeguards to control risks identified through risk

assessment, including by:

a) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to authenticate and permit access only to authorized users to protect against the unauthorized acquisition of PII and limit authorized users' access only to PII that they need to perform their duties and functions, or to access their own PII.
b) Identifying and managing the data, personnel, devices, systems, and facilities in accordance with their relative importance to business objectives and risk strategy.
c) Protecting by encryption all PI held or transmitted both in transit over external networks and at rest or, to the extent encryption of PII, either in transit over external networks or at rest, is infeasible, protecting PII using effective alternative compensating controls reviewed and approved by the DIS.
d) Adopting secure development practices for in-house developed applications for transmitting, accessing, or storing PII and procedures for evaluating, assessing, or testing the security of externally developed applications to transmit, access, or store PII.
e) Implementing multi-factor authentication for any individual accessing any information system, unless the DIS has approved in writing the use of reasonably equivalent or more secure access controls.
f) Developing, implementing, and maintaining procedures for the secure disposal of PII in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
g) Periodically reviewing the Record Retention and Disposal Policy and Procedures to minimize the unnecessary retention of data.
h) Adopting procedures for change management.
i) Implementing policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

5. Regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, conducting:
    a) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment.

b) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities based on the risk assessment, at least every six months, and whenever there are material changes or circumstances that may have a material impact on the university's information security program.

6. Implementing policies and procedures to ensure that employees are able to enact this WISP by:
   a) Providing employees with security awareness training that is updated as necessary to reflect risks identified by the risk assessment.
   b) Utilizing qualified information security personnel sufficient to manage information security risks and to perform or oversee the information security program.
   c) Providing information security personnel with security updates and training sufficient to address relevant security risks.
   d) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.
7. Overseeing service providers, by:
   a) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for PII.
   b) Requiring service providers by contract to implement and maintain such safeguards.
   c) Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.
8. Evaluating and adjusting the university's information security program in light of the results of testing and monitoring, any material changes to operations or business arrangements; the results of risk assessments performed under this section; or any other circumstances that the DIS knows or have reason to know may have a material impact on the information security program.

B. Data Stewards
   1. All PII covered under the WISP has a data steward. Each data steward shares responsibility with the DIS for implementing and maintaining the confidentiality, integrity, and security of the categoriesof PII set forth below:
      a) The president of the Providence campus or their designee is the steward of all PII regarding students relating to the period of their enrollment at the university, including Health Services and Counseling Services records, as well as personally identifiable financial information regarding parents/guardians of students.
      b) The vice president of enrollment management is the steward of all PII regarding applicants and prospective applicants; provided, however, that once an applicant is enrolledas a student, the president of the Providence campus or their designee becomes the steward of such student's PII.
      c) The DIS or their designee is the steward of all PII regarding alumni, donors, and prospective donors.
      d) The vice president of human resources is the steward of all PII regarding employees.

e) The vice president of auxiliary services is the steward of all PII regarding customers of practicum properties.
f) The assistant treasurer and vice president of finance is the steward of all PII regarding third party vendors who provide services to the university.
g) The DIS is the steward of all PII that does not have a designated data steward.
h) Data stewards may delegate, as deemed appropriate, any and all day-to-day administrative and operational activities to other appropriate university employees ("data managers").

C. Data Custodians

A data custodian is any individual who, by virtue of their university role or job function, possesses or has *authorized administrative level* access rights to university data, electronic or otherwise, and/or university information systems. Data custodians include all members of Information Technology (IT). Data custodians are responsible for following procedures and protocols for protecting the university's information technology resources from unauthorized access, alteration, destruction, or usage. Data custodians are also responsible for implementing and maintaining information technology security procedures in compliance with the WISP.

D. Data Users

1. A data user is any individual who, by virtue of their university role or job function, possesses or has *generalized* access to university data, electronic or otherwise, and/or university information systems, including alumni, faculty, staff, students, student employees, temporary employees, contractors, and consultants. Data users are responsible for the security and integrity of applications, data, and information stored on their workstations, laptops, or other technology used by them and/or that are stored in paper format. Data users control their accounts and data. Data users are responsible for protecting information resources in their possession from unauthorized access, alteration, destruction, or use and for implementing WISP controls and department procedures, such as unique passwords, secure storage and backup, and logging off work stations before leaving their work areas.
2. Further information and requirements for data users can be found in the university's Computer and Technology Use Policy.

VI. Reporting Attempted or Actual Loss of PII or Unauthorized Access

A. The speed with which the university can analyze, recognize, and respond to an incident can limit thedamage and cost of recovery and better safeguard our community members.

B. If any data user suspects that there has been an attempted or actual breach, loss or destruction of PII, or unauthorized access, disclosure, or use, regardless of it being paper-based or electronic PII, they must promptly report the incident to Campus Safety & Security. Campus Safety & Security will in turn contact the DIS, and the DIS will determine if the breach includes an information breach and/or other threats requiring corrective action. If a data user suspects that there has been an attempted or actual breach, destruction, or loss of PII or electronic unauthorized access, disclosure, or use of PII, the user must physically

disconnect the affected device or devices from the network immediately (by unplugging Ethernet cables, disabling Wi-Fi, or unplugging network cables), or if that is not possible, logically disconnect the device or devices from the network, before or simultaneous to reporting the suspected incident. Users should not power off their devices unless the users are unable to disconnect them from the network.

C. The following information should be provided by the reporting person(s):
   1. Date and time of incident;
   2. Type of incident;
   3. Details that might assist in assessing the incident;
   4. A statement describing the impact and other relevant facts; and
   5. Contact information of the submitter.

Campus Safety & Security Office Contacts	
Providence Campus	**Charlotte Campus**
264 Weybosset Street Providence, RI 02903 Phone: (401) 598-1103	Cedar Hall South Suite 113 801 West Trade Street Charlotte, NC 28202 Phone: (980) 598-1900

D. If the data custodians, in the course of their regular duties, observe attempts and/or actual breach, destruction, disclosure, loss, unauthorized access, or use of electronic PII, or missing media of any kind that contains PII, they must notify the DIS in accordance with the Incident Response Plan. The DIS will inform Campus Safety & Security and managers in the IT department as necessary.
   1. If the DIS determines that an actual or suspected *technology* or *electronic* information security breach, destruction, disclosure, loss, unauthorized access, or use of any information, including PII, has occurred, the DIS will coordinate the response utilizing the university's Incident ResponsePlan, and if applicable, the Group Health Plan Privacy Rule Policy, and will track and document the response.
   2. If the DIS determines that an actual or suspected *non-technology* or *non-electronic* information securitybreach, loss, destruction, disclosure, unauthorized access, or use of any information, including PII, has occurred, the DIS will coordinate the response utilizing the university's Incident Response Plan, and if applicable, the Group Health Plan Privacy Rule Policy, and will track and document the response.

E. Notification Requirements
   1. When the university determines that a data breach has occurred requiring a legal notification under applicable law or PCI standards, the university must take the following actions if and as required by suchlaws or standards:
      a) Notify supervisory authorities in applicable state and federal regulatory agencies.
      b) Notify affected individuals of a breach that has affected their personal information in a timely manner using the methodology required by applicable law, and if applicable, the Group Health PlanPrivacy Rule Policy.
      c) Breach notifications must contain information that is required by applicable state and federal law.

2. The university shall determine whether a breach occurred in the manner outlined in the Incident Response Plan.

VII. **Security**

A. Access, Disclosure, and Use Restrictions

1. Access to and disclosure and use of PII shall be limited to those persons who are reasonably required to know such information in order to accomplish the university's legitimate business purpose or as otherwise required by law.
2. Service Provider Access to PII
   JWU shall not grant access or disclose PII to any person or company with whom the university has contracted until the service provider has been evaluated for its ability to maintain the confidentiality, identity theft procedures, integrity, and security necessary for PII and has agreedby written contract to implement and maintain appropriate procedures and training consistent with applicable legal requirements including, without limitation, in the case of Employee Health Care Plan Information, a Business Associate Agreement with the university for the use and disclosure of such information.
3. Social Security Numbers
   a) In addition to the limitations set forth above with respect to PII, additional precautions are required with respect to the disclosure and use of all or any part of a social security number. Do not:
      (1) Require that a consumer of goods or services disclose all or part of a social security number in connection with the sale of consumer goods or services or an application for a discount card unless required by federal law.
      (2) Make available publicly all or any part of an individual's social security number.
      (3) Print or imbed all or any part of an individual's social security number on any card required for the individual to access university services or products.
      (4) Require an individual to transmit all or any part of their social security number over the Internet, unless the connection is secure or the social security number is encrypted.
      (5) Require an individual to use all or any part of their social security number to access an Internet Web site, unless a password or unique PIN or other authentication number is also required to access the Internet website.
      (6) Print all or any part of an individual's social security number on any materials that are mailed to the individual unless state or federal law requires the social security number to be on the document to be mailed.
      (7) Print all or any part of the social security number on a postcard or mailer not requiring an envelope, or visible in the envelope without the envelope being opened.
      (8) Disclose all or any part of an individual's social security number to a third-party if there is a reason to believe that the third-party lacks a legitimate purpose forobtaining the individual's social security number.

(9) Record any credit card number or all or any part of a social security number obtained from a purchaser as a means of identification upon the check of the purchaser tendered in connection with a retail sale.

(10) Exceptions:

(a) Social security numbers may be included in an application or in documents related to an enrollment process, to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the social security number for the purpose ofobtaining a credit report; OR

(b) The use of all or any part of social security numbers for internal university verification or administrative purposes is permitted; OR

(c) The disclosure of social security numbers to federal, state, or local governmental entities as permitted by law.

4. Education Records
   Access to or disclosure or use of any academic, financial, residential life, student conduct, and other personally-identifiable records created or maintained by the university regarding a particular student must follow the university's FERPA policy.
5. Medical Records of Students Attending JWU Health Services and Counseling Services
   All requests for medical records of students attending JWU Health Services or Counseling Services must be referred to the appropriate campus's Health Services or Counseling Services or the Office of the General Counsel. Such medical records may **not** be accessed, disclosed, released, or transferred to **anyone** except as approved by the appropriate campus's Health Services or Counseling Services or the Office of the General Counsel. Please be aware that there are criminal and civil penalties for the unauthorized disclosure, release, or use of medical records including fines, imprisonment, and/or being personally liable for monetary damages and fines, including compensatory and punitive damages and fines.
6. Employee Health Care Plan Information
   Employee Health Care Plan Information provided to Human Resources & Payroll with respect to employees and their dependents in connection with the university's employee benefit health plans will be maintained in accordance with HIPAA, the Group Health Plan Privacy Rule Policy, and this WISP. All requests for Employee Health Care Plan Information must be referred to the vice president of human resources or their designee. Employee Health Care Plan Information shall not be used for employment-related actions and decisions.
7. Cardholder Data
   a) In addition to the limitations set forth above, additional measures are required with respect to access to, and disclosure and use of, Cardholder Data:
      (1) Any Johnson & Wales University alumni, contractor, department, employee, student, or other third party that desires to use payment card transactions under the umbrella ofthe university's name must receive prior written approval from the DIS (after consultation with the assistant treasurer and vice president of

finance).

(2) Any hardware utilized for payment card transactions under the umbrella of the university's name must be certified as compliant under the PCI standards and approvedby the DIS.

(3) Any third-party vendor who has contracted with the university to provide services and utilizes payment card transactions must certify annually to the university that they are PCI compliant.

(4) All transmissions over the university's networks of Cardholder Data must be encrypted.The IT department will monitor for unencrypted transactions. Questions regarding how to encrypt Cardholder Data must be referred to the DIS.

(5) Any storage of Cardholder Data (when and as permitted by applicable PCI standards) on or in any media (including electronic records, e-mail, paper, voicemail, etc.) at the university must be encrypted and/or stored securely. Encryption keys and software are managed by the IT department. Questions regarding how to encrypt Cardholder Data must be referred to the DIS.

(6) Under no circumstances will the university retain any security related information(CAV2\CVC2\CVV2\CID from a payment card or full magnetic stripe data from a payment card).

(7) Any physical or technology access to Cardholder Data is subject to prior written approval of the DIS and must be limited to the access that is necessary for the performance an employee to perform their required tasks.

b) Standards for the Physical Protection of PII

(1) The DIS has created written protocols for the physical security of PII. The following minimum physical security standards are implemented by the university with respect to records containing PII:

(a) Records containing PII must be kept in limited access locked cabinets or locked storage areas or containers on university premises or the premises of university contracted service providers.

(b) Each department will identify all devices in areas that are easily accessible by outsiders where PII may be contained and/or accessed and adopt security measures for the protection of PII, including relocation of such devices. This might be a fax machine that is within arm's reach, a computer screen that potentially is visible, or an inbox that contains incoming mail.

(c) Doors and windows of unoccupied or unsupervised areas should be locked if such areas contain university computers or other devices of media that access or contain PII.

(d) Open files or documents containing PII must be secured on any desk when the desk is not attended. At the end of the work day, all files and other documents containing PII must be secured.

(e) Records containing PII to be transmitted or sent between campuses or to any authorized third contractors in paper format must be transmitted in a sealed

envelope marked confidential by a method that requires tracking of the package, and the parcel must indicate that it may only be opened by the intended recipient and that the intended recipient must acknowledge receipt.

(f) Records containing PII to be transmitted within a campus must be hand-delivered, sent in a sealed transmitted in a sealed envelope marked confidential, the parcel must indicate that it may only be opened by the intended recipient and that the intended recipient must acknowledge receipt.

(g) Paper documents containing PII must be shredded (or disposed of in a manner thatcomplies with federal and state laws and university policy). Disposal methodologies for paper documents other than shredding must be approved by the DIS.

(h) All data custodians will adhere to the then current university Business Continuity and Disaster Recovery Policy requirements.

c) Each department shall limit access to PII strictly for legitimate business purposes and shall maintain procedures to enforce such access.Standards for the Electronic Protection of PII

(1) The DIS working together with the IT department has created written protocols for the electronic security of PII.

(2) The following minimum standards are implemented by the university to control electronic access to PII:

(a) Do not transmit unencrypted PII by e-mail or other electronic transmission. All records and files containing PII transmitted across public networks or wirelessly must be sent in a securely encrypted e-mail attachment.

(b) Access to electronically stored records containing PII must be electronically limited to those individuals that have a legitimate business need for such information.

(c) The DIS shall review the security of service providers as described in this WISP. Service providers who require access to university systems that contain PII are required to have written pre-approval from data stewards and the DIS. The IT department is responsible for providing and monitoring access by such parties.

(d) Password requirements (including procedures for changing, creating, and safeguarding passwords) and access controls shall be approved by the DIS and implemented by the IT department.

(e) Data stewards are responsible for assigning and authorizing rights to data users for access toPII. The data stewards utilize assignments based on the principle of least privilege, and theIT department manages implementation and oversight of assigned rights.

(f) The university must maintain reasonably up-to-date firewall protection and install anti-virus andmalware software and operating system security patches provided by vendors on all systems accessing, processing, storing or transmitting PII.

(3) The university requires the IT department to periodically assess and test the vulnerability of systems containing or accessing PII and evaluate and adjust university information security in light of the results of such assessment and testing, as well as in light of any material changes to university operations, any risk assessments, or any other circumstances that may have a material impact on the university.

(4) The IT department logs and monitors operations for all systems that access or contain PII, including for user activity that may be inappropriate or malicious.

(5) PII may only reside on hard drives, media (such as CDs computers, laptops, PDAs, thumb/jump drives, and other computer hardware and equipment), and portable devices that are encrypted and have security features as approved by the DIS. Refer questions to the DIS.

(6) All data custodians will adhere to the then current university Business Continuity and Disaster Recovery Policy requirements. For business continuity and disaster recovery purposes, all data users should save PII on university drives that are backed up to maintain the integrity of the information (e.g., the G: or H: drives).

(7) Separated Employee Procedures exist that (a) promptly remove any electronic access to the university's systems from a separated employee and (b) modify the electronic access to the university systems of any other employee whose role at the university has changed so that access is no longer needed.

(8) Destruction or erasure of electronic media and other nonpaper media containing PII that is no longer needed or required to be retained so that the information cannot practicably be read or reconstructed (including prior to reuse of such media) is required. Questions regarding the proper destruction or erasure of electronic media must be forwarded to the DIS.

(9) Each university department creates written procedures for the electronic security of each type of PII for which they are responsible in accordance with such protocols. The DIS approves, reviews, and keeps a copy of each department's information technology security procedures.

d) Separated Employees

Human Resources & Payroll will work with the DIS to take the steps outlined in the Separated Employee Procedures with respect to each employee whose employment with the university is separated for any reason (including, without limitation, resignation, termination, or other departure).

8. Subpoenas and Other Compulsory Requests

Employees or vendors who receive court orders, investigative subpoenas, and other similar requests for records should refer the matter to the Office of the General Counsel immediately.

VIII. **Training**

A. The DIS, will train all employees on information security best practices and the appropriate sensitive data handling procedures. The DIS will also issue periodic security reminders. The

DIS will provide training across departments to achieve consistent implementation and maintenance of the WISP's requirements

B. Distribution of the WISP: Each employee who will have access to PII must read the WISP document and sign a policy acknowledgement form.

IX. **Maintenance of the WISP**

A. The WISP and the related procedures are reviewed at least annually or whenever there is a security incident or a material change in the university's practices that might reasonably implicate the confidentiality, integrity, or security of records containing PII. This review will include an evaluation of the effectiveness of the administrative, physical, and technical security protections in place to determine if they are sufficient to prevent unauthorized access to, or destruction, loss, or use of, PII, including an assessment of compliance with the WISP.

B. The DIS is responsible for this review in conjunction with the data stewards and data custodians. Safeguards will be updated and added as necessary to limit risks of unauthorized access or use.

X. **Service Providers Who Will Maintain, Access or Dispose of PII**

A. Whenever the university seeks to engage a third-party service provider who will have access to, destroy or dispose of, maintain, store, or transport, PII, the DIS will evaluate the ability of that service provider to implement and maintain appropriate confidentiality, integrity, and security procedures for the PII to which the university will provide them access. This assessment will include but will not be limited to compliance with all applicable laws and the PCI standards if applicable.

B. The university must require, by written contract, each such service provider to, at a minimum, implement and maintain appropriate confidentiality, integrity, and security procedures for PII consistent with applicable legal requirements and PCI standards and confidentiality provisions for confidential information consistent with contractual obligations to third parties by which JWU is bound.

C. In addition, with respect to service providers who will: (i) Access, destroy, store, transport, or use Employee Health Care Plan Information, the university will require service providers to enter into Business Associate Agreements, as provided in the Group Health Plan Privacy Rule Policy; or (ii) Access, destroy, store, transport, or use Cardholder Data, the DIS must also:

1. Maintain a list of all such service providers.
2. Require the written contracts with such service providers to include:
    a) An acknowledgement that the service providers are responsible for the security of Cardholder Data.
    b) A provision granting JWU the right to monitor such service providers' PCI compliance status at least annually, including receipt of an audit report or annual certification.
3. Monitor such service providers' PCI compliance status at least annually.
4. Dispose of and/or destroy documents or other records that contain PII, whether in electronic, paper, or other media, the DIS must also:

a) Review an independent audit of the disposal business's operations or its compliance with applicable laws.
b) Obtain information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review.

5. Service providers who require access to university information technology systems that contain PII are required to have written pre-approval from data stewards and the DIS. The IT department is responsible for monitoring, providing, and removing access by such parties.

XI. Disciplinary Action

Disciplinary action, up to and including possible termination of employment (for employees) or dismissal from the university (for students), will be taken for any violation of this WISP or the procedures referenced herein. Anyone having any questions as to whether an action being considered is an acceptable action under the WISP should contact the DIS.

XII. Policy Owner

Director of Information Security

XIII. Effective Date and Revisions

A. Originally Issued: August 2012
B. Last Revised: April 2023