ROGER WILLIAMS UNIVERSITY
Written Information Security Program

Objective

Roger Williams University ("RWU") has developed the following Written Information Security Program (the "Program") to address the requirements of the Regulations set to protect the personal information of all University personnel, including faculty, staff and students. Our University hosts individuals who not only reside in the State of Rhode Island but also reside all around the nation and also internationally. This Program allows us to ensure that we are in compliance with all applicable laws and regulations that govern University personnel.

The Program's goal is to set forth effective administrative, technical and physical safeguards for personal information, to provide an outline to assure the ongoing compliance with the Regulations, to protect personal information from unauthorized access, use, modification, destruction or disclosure, and to position RWU to comply with future privacy and safety regulations as such may develop.

Personal information for purposes of this Program shall mean: the first name and last name or first initial and last name of an individual in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number, state-issue identification card number or tribal identification number; or (c) financial account number, credit card number, 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, or deposit or savings account number; (d) medical or health insurance information; and/or (e) a username or email address in combination with security code, access code or password or security question and answer that would permit access to an online account; provided however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

The safeguards set forth in this Program are meant to protect the security and confidentiality of personal information, and to protect against any anticipated threats or hazards to the security or integrity of personal information.

Information Security

In order to further comply with applicable Regulations, we have appointed an Information Security Officer who will be responsible for the following:

- Implementing the Information Security Policy.

- Training employees who have exposure to personal information through their work at RWU on the various aspects of the Program, at least annually.

- Obtaining certification of attendance to and understanding of such training by the employees.

- Conducting regular testing and evaluation of the Program's safeguards.

- Verifying the ability of third party recipients of personal information to comply with the Regulations.

- Reviewing the Program, its scope and its effectiveness at least annually or at such time as a material change in business practice occurs that implicates the security of personal information and upgrading information safeguards as necessary to limit risk.

Risk Assessment

The Information Security Officer will conduct a risk assessment. The initial risk assessment will seek to reveal the following potential and actual risks to the security and privacy of personal information:

- Unauthorized access of personal information by an employee not entitled to the information.

- Compromised system security as a result of unauthorized access by a third party.

- Interception of personal information during transmission.

- Unauthorized access to paper files containing personal information.

- Unauthorized access to personal information through mobile personal devices.

The Information Security Officer will discuss findings and recommendations resulting from the periodic reviews with relevant RWU personnel.

The Chief Security Officer will evaluate RWU's security practices to determine where improvement is necessary to limit risks, including, but not limited to, ongoing employee training, employee compliance with security policies and procedures, means for detecting and preventing security system failures, and the upgrade of safeguards, if necessary, to limit risks.

Safeguards

In an effort to address the internal and external risks revealed during the risk assessment, RWU has implemented the following policies and procedures:

1) *General Safeguards*

RWU will limit the amount of personal information collected to that necessary to achieve legitimate business goals and to comply with state and federal laws and regulations. RWU will limit access to personal information to those people with a need to know to accomplish legitimate business goals and to comply with state and federal laws and regulations. RWU will monitor its security systems for breaches of security.

Upon the occurrence of an incident requiring notification under state law, the Information Security Officer will assemble the Incident Response Team and the Incident Response Procedure will be followed. Mandatory post-incident review by RWU following any actual or suspected breach of security, and documentation of the actions RWU takes in response to such breach, including any changes RWU makes to its business practices relating to the safeguarding of personal information will be conducted and documented.

RWU will restrict visitor access where personal information is stored. Visitors will be prohibited from visiting unescorted any area within RWU's premises that contains personal information.

2) *Employee Safeguards*

RWU will post a copy of the Program in areas in which it will generally be seen by employees. Each employee will:

- Promptly or upon the commencement of hiring, as the case may be, and once a year thereafter, participate in employee training about the Program and upon successful completion of the training, certify to attending training and understanding the terms of the Program and the importance of protecting personal information.

- Have access to, and follow, privacy and security policies

- Report any suspicious or confirmed unauthorized access, use or disclosure of personal information.

- Comply with the Program at all times.

- Be subject to disciplinary action for violation of this Program.

Employee training will, among other things, address issues relating to:

- Proper access, use and disclosure of personal information.
- Proper disposal of personal information.
- Proper safeguards for maintaining, transmitting and storing personal information.
- Logging-off computers.
- Locking files and doors.
- Limiting access to offices.
- Properly handling and protecting mobile devices and removable media.
- Password management.

Employees will be prohibited from storing, accessing or transporting personal information outside the premises of the business, unless in accordance with RWU policies.

Access to personal information by terminated employees will be revoked as soon as possible following termination, and terminated employees will be required to return all personal information in their possession; moreover, all passwords to computer systems will be promptly disabled, all access to electronic files, physical files, email, voicemail and internet access will be promptly blocked, all keys will be surrendered and all forms of identification that permit access to RWU's premises or information will be returned. Terminated employees will be required to execute an agreement whereby they agree to honor all obligations with respect to maintaining the confidentiality of personal information handled during the course of their employment, to the extent not already contractually bound to do so. The University does require certain non-union professional and managerial employees to enter a confidentiality agreement upon hire, the conditions of which survive post-separation.

3) Non-Electronic File Safeguards

All tangible files containing personal information will be in a locked room or cabinet or stored securely offsite. Each department will control the distribution of their keys and will keep

track of the number of keys issued. RWU will limit access to offsite storage facilities containing personal information to those employees with a need to access the files, and RWU will periodically request an access log to monitor who is accessing such files. When sending personal information via carrier, RWU will use overnight carriers with tracking and, if sending electronic information, encrypt the information to the extent technically feasible.

4) Electronic File Safeguards

Access to all electronic files maintained on RWU's servers or RWU's hardware that contain personal information will be limited to those employees with a need to know.

Moreover, RWU has set forth the following protocols to further protect personal information in electronic form. RWU will, to the extent technically feasible:

- Secure the services of a contract consultant to annually run intrusion testing.
- Install firewall protection and operating system patches on all computers with personal information.
- Install up-to-date versions of security agency software.
- Encrypt personal information that is transmitted across public networks.
- Encrypt all personal information stored on a laptop or other mobile or removable device.
- Limit access to the computer system using complex logins and alphanumeric passwords that require changing every 90 days and require passwords and limited access to e-files containing personal information.
- Require re-logging after passage of inactive time.
- Prohibit posting or sharing of passwords by employees.
- Lock users out after (6) failed log-in attempts.
- Check websites and software vendor websites for alerts about new problems and implement such vendor approved patches as soon as practical.
- Maintain control of user IDs and other identifiers.

- Maintain passwords in a location and/or format that does not compromise the security of the data the password protects.

- Prohibit the continued use of default passwords by employees (i.e. force employee to change passwords).

- Maintain a reasonably secure method of assigning and selecting passwords or the user of unique identifier technologies such as biometric s or security tokens.

- Terminate any access to personal information by terminated employees.

- Use secure computer and Internet user authentication protocols (i.e. control of user identifications and other identifiers).

- Divisional units are responsible for safeguarding paper files.

5) Third Party Vendors

When using third-party vendors for services that necessitate the sharing of personal information, RWU will:

- Request, when possible, the right to audit the policies and procedures of third-party vendors used to comply with the Regulations.

- Obtain a copy of the third party vendor's written information security program designed to comply with the Regulations.

- Contractually require implementation and maintenance of privacy and security measures and a Written Information Security Program by the third party vendor.

Disposal

RWU has implemented a Data Storage and Record Retention policy and schedule. When disposing of files containing personal information [i.e. Data Classification = Protected and Sensitive], RWU will follow its policy and schedule, which will include:

1. Shredding all hardcopies of files containing personal information when such information is no longer required or needed to be maintained by RWU.

2. Destroying all electronic files containing personal information when such information is no longer required or needed to be maintained by RWU, including the destruction of residual electronic data on computers and other electronic devices.