Risk-Based Information Security Program (RISP)

I. OBJECTIVE

The objective of Rhode Island School of Design ("RISD") in the development and implementation of this comprehensive risk-based information security program ("RISP") is to create effective administrative, technical and physical safeguards for the protection of Protected Information ("PI"). The RISP sets forth RISD's procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PI, and is intended to comply with the relevant provisions of the Rhode Island Identity Theft Protection Act of 2015 and the Gramm Leach Bliley Act ("GLBA").

For purposes of this RISP, "PI" means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual, when the name and data elements are not encrypted or are in hard copy, paper format:

- Social Security number;
- Driver's license number or state/tribal-issued identification card number;
- Financial account number, or credit or debit card number, in combination with any required security code, access code, personal identification number or password, that would permit access to an individual's financial account;
- Passport number;
- Medical history, or medical treatment or diagnosis by a healthcare professional or health insurance information, including payment records for treatment, to the extent considered confidential under Rhode Island law;
- Username or email address coupled with a password or security question and answer that would permit access to an online account;
- Records (in)directly identifying an individual, created for the purposes of an individual's health care treatment from RISD health care services, including payment for health care services;
- Information obtained from a person or otherwise provided to RISD in the course of offering a financial product/service by RISD, such as students loans or financial aid; or,
- Information RISD is required to keep confidential by contract or RISD policy.

PI 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.

II. PURPOSE

The purpose of the RISP is to better:

- Ensure the security and confidentiality of PI through the use of safeguards, risk assessments, overseeing service providers, and updating information security procedures;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- 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 the RISP, RISD 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;

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

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

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

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

IV. INFORMATION AND DATA SECURITY COORDINATOR

RISD has designated the Chief Information Officer as Information and Data Security Coordinator ("IDSC") to implement, supervise and maintain the RISP. The IDSC, or designee(s), will be responsible for oversight of:

a. Implementation of the RISP, including ongoing compliance, operational procedures, and review along with related policies;

b. Training employees with access to PI as appropriate for their roles and duties;

c. Regular testing of the RISP's safeguards;

d. Evaluating the ability of each of RISD's third party service providers to implement and maintain appropriate security measures for the PI to which RISD has permitted them access, consistent with the regulations; and requiring such third-party service providers by contract to implement and maintain appropriate security measures;

e. Reviewing the scope of the security measures in the RISP at least annually, or whenever there is a material change in RISD's business practices that may implicate the security or integrity of records containing PI; and

f. Conducting training sessions for all owners, managers, employees, and independent contractors, including temporary and contract employees who have access to PI on the elements of the R ISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with RISD's requirements for ensuring the protection of PI.

V. INTERNAL RISKS

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

Internal Threats

- RISD shall only collect PI of students, their parents, alumni, donors, suppliers, vendors, faculty, staff or employees that is necessary to accomplish RISD's legitimate need to access said records, and for a legitimate job-related purpose, or as necessary to RISD to comply with state or federal regulations or its contractual obligations.

- Access to records containing PI shall be limited to those persons who are reasonably required to know such information in order to accomplish RISD's legitimate business purpose or to enable RISD to comply with state or federal regulations or its contractual obligations

- Documents containing PI should not be made publicly available outside of RISD without prior consultation with the IDSC.

- Access to PI shall be restricted to active RISD users and active third-party user accounts with RISD's permission only.

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

    - Paper documents containing PI shall be either redacted, burned, pulverized or shredded upon disposal using RISD disposal services so that PI cannot be practicably read or reconstructed; and

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

    - If a RISD employee believes that a PI record should not be disposed, the employee should consult with the IDSC before disposal about whether the record should be retained for a longer period.

- A copy of this RISP must be distributed to each current RISD employee with access to PI and to each new RISD employee with access to PI at the commencement of their employment. It shall be the employee's responsibility for acknowledging that the employee has received a copy of this RISP and will abide by its provisions.

- <u>Procedures for Terminated Employees</u>

    - Terminated employees must immediately return all records containing PI, in any form, that may at the time of such termination 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.)

    - A terminated employee's physical and electronic access to PI must 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; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

- All persons who fail to comply with this RISP may be subject to disciplinary measures, irrespective of whether PI was actually accessed or used without authorization.

- All security measures shall be reviewed at least annually, or whenever there is a material change in RISD's business practices that may reasonably implicate the security or integrity of records containing PI. The IDSC shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

- <u>Physical Assets Protocol</u>

    - All assets must be secured from theft by locking up and maintaining a secure workplace, whether that work takes place in RISD's stores, offices, client site, a car, hotel or a home. RISD employees must not leave open files containing PI unattended.

        - All laptops must be placed in the trunk of vehicle when and wherever they are parked. If no secure trunk or other storage is available, employees must keep their laptops in their possession.
        - Laptops, PDAs, and other portable devices left in the office or at home over night should be kept in a locked and secure location.
        - Employees must have assets secured or within their physical possession while on public or private transportation, including air travel.
        - An employee's failure to adhere to this and other security policies of RISD may result in disciplinary action and, in case of preventable loss or theft, employee's replacing all assigned equipment at their own expense.
        - PI should not be stored on the local drive; it should be stored through secure VPN or encrypted device to the RISD network or other RISD-approved secure storage.

- <u>Access Control Protocol</u>

    - Access to electronically stored PI shall be electronically limited to those RISD employees having a unique log-in ID, and to third party users who have been granted permission by RISD to access specific PI.

    - RISD employees should always use the RISD network, RISD secure wireless network, or RISD VPN when performing work involving PI.

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

    - Employees must log off of the VPN when they are not directly using those resources.

    - Employees must maintain the confidentiality of passwords and access controls:

        - All passwords used for RISD's systems and laptops are required to adhere to strong password rules.
        - All passwords used for RISD's systems and laptops are required to be changed every 6 months.
        - Employees must not share accounts or passwords with anyone.
        - Employees must not record passwords on paper or in a document.

    - Where practical, all visitors who are expected to access areas other than common public space or are granted access to office space containing PI should be required to sign-in at a designated reception area where they will be assigned a visitor's ID or guest badge unless escorted at all times. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times.

    - Where practical, all visitors are restricted from areas where files containing PI are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing PI are stored.

- RISD's employees are required to report suspicious or unauthorized use of PI to the IDSC immediately.

- Pursuant to RISD's Incident Response Plan, whenever there is an incident that requires notification under Rhode Island state breach notification statute or regulation, the technology incident response team (TIRT) will immediately conduct a mandatory post-incident review of events and action taken, if any, with a view to determining whether any changes in RISD's security practices are required to improve the security of PI for which RISD is responsible.

VI. EXTERNAL RISKS

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

External Threats

- 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.

- 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.

- All PI stored on laptops or other portable devices shall be encrypted, as must all records and files transmitted across public networks or wirelessly. Encryption means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key. Transmission by RISD email alone is not considered encrypted over a public network.

- Employees must not email any student, parent, alumni, donor, supplier, vendor, faculty, staff or employee information or documents containing PI without encryption.

- There shall be secure user authentication protocols in place that:

    - Control user ID and other identifiers;

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

    - Control passwords to ensure that password information is secure.

- PI shall not be removed from RISD premises in electronic or written form absent a legitimate business need and use of reasonable security measures, as described in this RISP.

- All RISD systems shall be monitored for unauthorized use or access to PI.

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

If you have reason to believe that any PI has been lost or stolen or *may* have been compromised or there is the potential for identity theft or institutional harm, regardless of the media or method, report the incident immediately by contacting IT Service Desk (401.454.6106) during normal working hours and Public Safety (401.454.6376) after hours to report the incident.