POLICY TITLE	GRAMM LEACH BLILEY ACT SECURITY POLICY
PURPOSE	RISD is required to comply with the applicable portions of the Gramm Leach Bliley Act (GLBA) related to its capacity under the GLBA definition of a financial institution. RISD complies with the privacy requirements of the GLBA through its compliance with FERPA.
SCOPE	The scope of this Policy applies to all RISD employees with access to Non-Public Financial Information, including service providers who have access to RISD's Non-Public Financial Information.
POLICY STATEMENT	This Policy memorializes Rhode Island School of Design's (RISD) efforts to ensure the security and confidentiality of records protected under the Gramm Leach Bliley Act (GLBA), through the implementation of institutional practices that protect against the unauthorized access or disclosure of protected records. This Policy incorporates by reference other RISD policies pertaining to information security, including the RISP, FERPA, GDPR, and other ITS policies specific to RISD systems.
DEFINITIONS	Meaning and interpretation of specific terms used in the policy are listed here: **GLBA:** The Gramm Leach Bliley Act and its implementing regulations. **Program Officer**: The RISD employee designated to oversee the terms of this Policy. **Non-Public Financial Information**: Non-public information provided by a RISD student or other third party to RISD, or otherwise obtained by RISD, for the purposes of obtaining a financial product or service from RISD, whether in paper, electronic, or another format.
POLICY	**RISD Representative** RISD's Chief Information Officer is designated as the Program Officer pursuant to GLBA, who is responsible for coordinating the program described under this Policy. The Program Officer may designate other RISD employees to oversee, coordinate, or implement this Policy, as needed. Questions regarding this Policy should be directed to privacy@risd.edu. **Information Security Program** 1. **Risk Identification & Assessment** RISD, through its Program Officer, will identify and assess reasonably foreseeable external and internal risks to information security pertaining to Non-Public Financial Information, including the risks of unauthorized access, disclosure, misuse, or destruction of its Non-Public Financial Information and incorporating the other elements of this Program. 2. **Information Systems Data Processing & Disposal** The Program Officer and designees will coordinate with RISD departments to inventory, assess, and monitor the storage, transmission, and disposal of Non-Public Financial Information contained in RISD systems. The Program Officer or designee(s) will coordinate with departments to ensure compliance with proper procedures for handling and disposing of Non-Public Financial Information. 3. **Detecting, Preventing, & Responding to Threats** The Program Officer and designee(s), in conjunction with Risk Assessment and other departments as needed, will evaluate RISD policies, procedures, and technological

	safeguards for methods of detecting, preventing, and responding to threats to the RISD systems storing and transmitting Non-Public Financial Information. The Program Officer or designee(s) will advise as to necessary software and hardware updates, as well as recommended physical security practices for each department. RISD's emergency response team members will coordinate with the Program Officer in the event of an emergency that impacts RISD's protection of Non-Public Financial Information. **4. Service Providers** The Program Officer, in coordination with General Counsel and all departments contracting with third party service providers who handle RISD's Non-Public Financial Information, will select third party service providers who are capable of providing reasonable, appropriate safeguards under GLBA. RISD will collect and maintain copies of service provider contracts containing representations regarding the secure handling of Non-Public Financial Information. Where possible, RISD contracts will contain standardized language pertaining to the secure handling of Non-Public Financial Information. **5. Employee Education** The Program Officer shall develop or identify training materials that support compliance with RISD information security practices under GLBA, and will make these materials available to management employees for the purposes of training employees who handle Non-Public Financial Information. **6. Review & Assessment** The Program Officer, in conjunction with General Counsel, Risk Management, Student Financial Services, and other departments as needed, will periodically evaluate and assess the risk to RISD's data security systems and practices, and will recommend and implement changes to RISD data security policies, protections, and practices when appropriate.
PROCEDURES	Procedures pursuant to this Policy may be located in the RISD Risk-Based Information Security Program.
EFFECTIVE DATE and REVISION HISTORY	This policy is effective: January 1, 2020 Next Scheduled Review: January 1, 2021
RESPONSIBILITIES	Issuing Office: ITS Responsible Officer: Chief Information Officer Individuals/offices required for review and changes: CIO, General Counsel
REQUIRED DOCUMENT APPROVALS	_____ _____ NAME: DATE: TITLE: