HOFSTRA UNIVERSITY INFORMATION SECURITY PROGRAM

Overview: In order to protect non-public personal information and data, and to comply with federal law, including the Gramm-Leach-Bliley Act, the University has implemented certain practices in the University information environment and institutional information security procedures. The goals and objectives of this Information Security Program ("Program") are to:

(1) Ensure the security and confidentiality of nonpublic financial information;

(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 that could result in substantial harm or inconvenience to members of the University community.

In addition to this Program, the University's FERPA Policy, Acceptable Use Policy, and the University's Confidentiality Agreement & Security Policy are all incorporated by reference into this Program.

Designation of Coordinator: The University's Chief Information Officer ("CIO") is designated as the individual ("Coordinator") who will oversee, implement, and enforce the Information Security Program ("ISP"). The Coordinator may designate other representatives of the University to oversee and coordinate particular elements of the Program; references to the Coordinator in this document will refer to the Coordinator or his/her designees. Any questions regarding the implementation of this Program should be directed to the Coordinator.

Scope of Program: The Program applies to any record containing nonpublic financial information about a student or other individual who has a relationship with the University, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the University.

For these purposes, the term Non-Public Financial Information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the University, (ii) about a student or other third party resulting from any transaction with the University involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. Non-Public Financial Information may be in paper, electronic or other form. Financial products and services covered by this Program include lending funds, collecting loan payments, and facilitating the process of applying for financial aid.

Elements of the Program:

1. Risk Identification and Assessment. The University intends through this Program to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Non-Public Financial Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

The risk assessment will be in writing and include:

(a) Criteria for evaluating and categorizing identified security risks;

(b) Criteria for the assessment of the confidentiality, integrity, and availability of information systems and Non-Public Financial Information; and

(c) Requirements for describing how identified risks will be mitigated or accepted based on the risk assessment and how the ISP will address these risks.

Additional risk assessments will be performed periodically to re-examine reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

2. Designing and Implementing Safeguards. The Coordinator will work with relevant University departments to design and implement safeguards, as needed, to control the risks through risk assessment. The Coordinator will also work with departments as necessary to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures, to include, for information systems, continuous monitoring or periodic penetration testing and vulnerability assessments. Controls will be designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, Non-Public Financial Information.

3. Implementing Policies and Procedures. The Coordinator will work with relevant University departments to insure that University personnel are provided with updates and security awareness training that is updated as necessary to reflect risks identified through risk assessments and to address relevant security risks. Qualified information security personnel will take steps to maintain current knowledge of the changing information security threats and countermeasures.

4. Overseeing Service Providers. The Coordinator will work with relevant departments to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the Non-Public Financial Information, require service providers by contract to implement and maintain such safeguards, and periodically assess service providers based on the risk they present and continued adequacy of their safeguards.

5. Written Incident Response Plan. The Incident Response Plan (IRP) responds to and recovers from any material security event affecting the confidentiality, integrity or availability of Non-Public Financial Information in the University's control and addresses:

(a) The goals of the IRP and internal processes for responding to a security event;

(b) The definition of clear roles, responsibilities and levels of decision-making authority;

(c) External and internal communications and information sharing;

(d) Requirements for the remediation of any identified weaknesses in information systems and associated controls;

(e) Documentation and reporting regarding security events and related incident response activities; and

(f) The evaluation and revision of the IRP as necessary following a security event.

Evaluation and Adjustment of Program. The Coordinator will work with individual departments throughout the University to monitor, evaluate and adjust this Program in light of the results of the testing and monitoring described above, any material changes to operations or business arrangements, technology changes, emerging vulnerabilities and threats, the results of performed risk assessments, and any other relevant known factors or factors in which there is a reason to know may have an impact on the security or integrity of Non-Public Financial Information.

Reporting. The Coordinator shall report, in writing, the Hofstra University Board of Trustees, regarding the overall status of – and overall compliance with – the ISP as well as any material matters related to the ISP on at least an annual basis.

Rev. 6/2023

HU Doc#16821