Johnson College Information Security Program Outline

Preamble

In order to protect critical information and data, and to comply with Federal Law Including the Gramm-Leach-Bliley Act (“GLBA”), the Network and Systems Department (“N&S”), in alliance with the Executive Council proposes certain practices in the Johnson College (“College”) information environment and institutional information security procedures. While these practices mostly affect N&S, some of them will impact diverse areas of the College, including but not limited to the Business Office, the Financial Aid Department, the Office of Enrollment Services, the Office of College Advancement, the Office of Student Affairs and Student Services, and many third party contractors, including food services. The goal of this document is to define the College's Information Security Program (“ISP”) as it relates to regulated and confidential information, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the College for likely future privacy and security regulations

Background

Johnson College is required by the GLBA and its implementing regulations to develop and maintain a comprehensive written ISP and to appoint a coordinator for the program. The objectives of the ISP are to (1) insure the security and confidentiality of covered information; (2) protect against anticipated threats or hazards to the security and integrity of such information; and (3) protect against unauthorized access or use of such information that could result in substantial harm or inconvenience to customers.

Definitions:

A. “Covered data and information” for the purpose of this policy includes “student and third party non-public financial information” required to be protected under the GLBA. For purposes of this Program, the College also considers covered data and information to include any credit card information received in the course of business by the College, whether or not such credit card information is technically covered by GLBA. Covered data and information includes both paper and electronic records.

B. “Nonpublic financial information” is that information the College has obtained from a student or a third party in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student or third party nonpublic financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

C. “College” shall mean and include not only Johnson College, but also any and all of its affiliate organizations.

Related Policies

This ISP is in addition to existing Johnson College policies and procedures that address various aspects of information privacy and security, including but not limited to, Family Educational Rights and Privacy Act Policy (“FERPA”) and the Computing Acceptable Use Policy.

Designation of Representatives and Scope of Program:

A. GLBA mandates that the College appoint one or more Information Security Plan Coordinators (“Plan Coordinator”). The College designates the Director of Information Technology, the Chief Financial Officer and the Vice President of Human Resources as its Plan Coordinators. These Plan Coordinators shall be responsible for coordinating and overseeing the implementation of the Program, including periodic review and updates to the Plan. Any questions regarding the plan and its implementation should be directed to the Plan Coordinators.

B. The Plan Coordinators will work with the relevant offices of the College to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; and in conjunction with these offices, assist them to design, document and implement a safeguards program, and regularly monitor and test the program.

C. The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the College, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the College or its affiliates.

Elements of the ISP

1. Risk Identification and Assessment. Johnson College's ISP identifies and assesses external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The ISP Coordinators will provide guidance to appropriate personnel in the administration, academic units, and other College units in evaluating their current practices and procedures and in assessing reasonably anticipated risks to covered information in their respective areas. The ISP Coordinators will work with appropriate personnel to establish procedures for identifying and assessing risks in the following areas:

Employee Training and Management. The ISP Coordinators will coordinate with the appropriate personnel to evaluate the effectiveness of current employee training and management procedures relating to the access and use of covered information.

Information Systems. The ISP Coordinators will coordinate with the appropriate personnel to assess the risks to covered information associated with the College's information systems, including network and software design as well as information processing, storage, transmission and disposal.

Detecting, Preventing and Responding to Attacks and System Failures The ISP Coordinators will coordinate with the appropriate personnel to evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions or other system failures.

2. Designing and Implementing Safeguards. The ISP Coordinators will coordinate with appropriate personnel to design and implement safeguards, as needed, to control the risks identified in assessments and will develop a plan to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The ISP Coordinators, in conjunction with Executive Counsel and the Director of Building and Grounds, will assist in instituting methods for selecting and retaining service providers that are capable of maintaining appropriate safeguards for covered information. The ISP Coordinators will work with the Executive Counsel to develop and incorporate standard, contractual provisions for service providers that will require providers to implement and maintain appropriate safeguards. These standards will apply to all existing and future contracts entered into with service providers to the extent required under GLBA. Service providers will have a signed and dated Vendor GBLA Letter on file with the College prior to embarking on any projects for/with the College.

4. Adjustments to Program. The ISP Coordinator will evaluate and adjust the ISP as needed, based on the risk identification and assessment activities undertaken pursuant to the ISP, as well as any material changes to Carnegie Mellon's operations or other circumstances that may have a material impact on the ISP.