STETSON LAW

Student Financial Information

A. In General

The College of Law receives and holds confidential information of various sorts, some of which the College is precluded by law from divulging, except in limited circumstances. The College of Law holds other information confidential as a matter of policy and in the interest of privacy protection for our campus community. This policy is specifically directed toward student financial information required to be protected under the federal Gramm Leach Bliley Act ("the Act").

B. Financial Information Security Policy under the Act

1. Definitions

a. **"Covered data and information"** includes student financial information required to be protected under the Act. Covered data and information includes paper and electronic records.

b. **"Student financial information"** is that information the College of Law has obtained from a student in the process of offering a financial product or service, or information provided to the College by another financial institution. Offering a financial product or service includes offering student loans or financial aid to students, receiving income tax information from a student or a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 C.F.R. §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers, in paper and electronic format.

2. Requirements:

The Act mandates that the College of Law appoint a Financial Information Security Policy Coordinator to conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust this policy periodically. To comply with the Act, the College of Law has designated the Associate Vice President for Budget and Finance as the Coordinator. The Coordinator will closely work with the Offices of Information Technology, Registrar, Financial Aid, College Relations, Business Office, and Human Resources and other relevant academic departments throughout the College of Law.

3. **Coordinator Responsibilities:** The Coordinator will identify and maintain a list of departments and areas of the College of Law with access to covered information within the scope of the Financial Information Security Policy. The Coordinator will also ensure that (a) risk assessments and monitoring, as set forth below, are carried out for each department or area that has covered data and (b) the appropriate controls are in place for the identified risks.

4. **Risk Assessment and Safeguards:** The Coordinator will identify risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction of the information, or that could otherwise compromise the information. The Coordinator also will assess the sufficiency of any safeguards in place to control these risks. Risk assessments will include, but will not be limited to, employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures. The Coordinator will ensure that risk assessments are conducted at least annually and more frequently where required. The Coordinator will work with the College of Law's Director of Information Technology to conduct the system-wide risk assessment. In so doing, the Coordinator may use outside consultants to assist in this assessment, so long as all contracts with the consultants contain appropriate controls for the security and protection of data as provided below. The Coordinator will provide copies of complete and current risk assessments for College of Law and unit-specific risks at least annually to the Dean of the College of Law, with copies to the Business Office and Office of Information Technology.

5. **Service Providers:** The College of Law may, from time to time, appropriately share covered data with third parties. Appropriate activities may include collection activities, transmission of documents, destruction of documents or equipment, or other similar services. Reasonable care will be taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

6. **Program Maintenance:** The Coordinator, working with responsible units and offices, will evaluate and recommend adjustments to this policy in light of the results of testing and monitoring described above, as well as any material changes to operations or business arrangements, and any other circumstances which may reasonably have an impact this policy.

Cross-references: Privacy of Student Records, Confidentiality Policy; Computer and Network Use Policy, Data Security and Identity Theft Program, Banner Data Standards, Student Rights and Responsibilities Form.

Administrative policy adopted October 26, 2009. Administrative revision, October 22, 2015.

_____

Christopher M. Pietruszkiewicz