STANFORD UNIVERSITY
FINANCIAL SERVICES INFORMATION SECURITY PLAN

Stanford University is committed to the ongoing protection of confidential financial services information that it may collect from faculty, staff, students, alumni and others. The Gramm-Leach-Bliley Act (GLB) requires that Stanford University "develop, implement and maintain a comprehensive information security plan" to ensure the safeguarding of confidential financial services information. 15 U.S.C. sec. 6801. For the purposes of this Plan, Financial Services Information ("FSI") is information that the University has obtained in the process of offering a financial product or service, such as financial aid or a faculty-housing loan. This Plan sets the policy to ensure ongoing protection of FSI and serves as the written evidence of a Security Plan in compliance with 16 CFR 314.3(a).

I. GLB Requirements

The objectives of the GLB safeguarding provisions are to:

- protect the security and confidentiality of non-public confidential financial information;

- protect against anticipated threats to the security of such information; and

- protect against unauthorized access to or use of such information.

In order to accomplish these goals, GLB requires the following:

- Designate one or more staff members to oversee and coordinate the Information Security Plan;

- Conduct a risk assessment to identify foreseeable internal and external risks that could lead to unauthorized disclosure or misuse of confidential information;

- Implement a plan to control the risks;

- Contractually require third-party service providers to implement and maintain confidentiality safeguards; and

- Periodically evaluate and adjust the Information Security Plan to ensure ongoing protection of confidential information.

II. The Scope of FSI

Financial Services Information ("FSI") is information that the University has obtained in the process of offering a financial product or service, such as financial aid or a faculty-housing loan, or such information provided to the University by another financial institution.

III. Plan Coordinator

Stanford University's Plan Coordinator is the University's Privacy Officer, or the Chief Financial Officer if the Privacy Officer position should become vacant. The Plan Coordinator should work in cooperation with the Data Governance Board, the Office of the General Counsel, the Director of Student Financial Aid, the Director of Faculty Staff Housing, and any other relevant academic and administrative Schools and Departments throughout the University with access to FSI.
The Plan Coordinator should assist the various offices of the University with access to FSI to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of FSI; evaluate the effectiveness of the current safeguards for controlling these risks; regularly monitor and test the Plan; design and implement any necessary changes to the Plan.

IV. Identification of Risks and Risk Assessment

Stanford University recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of FSI by someone other than the owner of the FSI
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Physical misplacement of paper records
- Loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of FSI by employees
- Unauthorized requests for FSI
- Unauthorized transfer of FSI through third-parties

Stanford University recognizes that this may not be a complete list of the risks associated with the protection of FSI. Since technology growth is not static, new risks are created regularly.

In addition, from time to time, the University should conduct or oversee penetration testing. Stanford University believes the safeguards that it has put into place are reasonable and, in light of the Data Governance Board's current risk assessments are sufficient to provide security and confidentiality to FSI maintained by the University. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

V. Design and Implementation of a Safeguarding Program

Stanford University's Safeguarding Program has five key components: A) Employee Training and Management; B) Information System Security; C) Physical Security of Paper Records; D) Electronic Commerce at Stanford; and E) Disposal of Records.

A. Employee Training and Management

A background check -- consisting at a minimum of a reference check -- should be conducted before hiring any potential employee that might have access to FSI. In some cases a criminal background check may be conducted as well. This provision is in accord with the hiring policy set forth in Administrative Guide Memo, 22.1(j), http://adminguide.stanford.edu/22_1.pdf.
During employee orientation, each new employee with access to FSI should receive proper training on the importance of confidentiality of information at Stanford under the Data Classification, Access, Transmittal and Storage Guidelines,
http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html, with particular emphasis on the confidentiality of student records, student financial information, credit checks, bank accounts, tax records and any other FSI maintained by the University. Each new employee with access to FSI should also be trained in the proper use of computer information and passwords. Training should also include controls and procedures to prevent employees from providing FSI to an unauthorized individual. As appropriate, the training may include pretext calling – where a supervisor attempts to obtain FSI through the use of deceit – to highlight the importance of protecting FSI and to protect against identity theft. Training should also include the methods for proper disposal of documents that contain FSI.
Periodically as necessary, each department responsible for FSI should provide training to all employees to remind them of the importance of FSI and to ensure that the safeguarding procedures and controls are followed.
In the case of temporary workers, a supervisor should provide adequate training regarding the identification and protection of FSI to protect against disclosure.

B. Information System Security

Access to FSI through the University's computer network is limited to those employees who have a business reason to have such information. All databases containing

FSI should be protected according to the Data Classification, Access, Transmittal and Storage Guidelines.

Stanford University will take reasonable and appropriate steps consistent with current technological developments to secure FSI and safeguard the integrity of records in storage and transmission. These steps include maintaining the operating system and applications including providing appropriate patches and updates in a timely fashion. In addition, an intrusion-detection system has been implemented to detect and stop most external threats.

C. Physical Security of Paper Records

Only employees who have a business reason to have FSI should have access to any physical paper records. The records should be kept in a locked office or in locked files as reasonable. The files should be locked at a minimum of each night. Sound business practice dictates that the files should also be locked whenever an authorized employee is not present with the files.

D. Disposal of Records

The University should only keep physical paper records and electronic documents containing FSI for as long as they are being actively used by the Department, or as necessary to comply with state, federal or local law, or the University's Document Retention Policy, as provided in Administrative Guide 34.4, http://adminguide.stanford.edu/34_4.pdf.
Paper documents that are no longer required to be kept by the University should be shredded at the time of disposal. Electronic documents should be deleted and magnetic media should be erased.

VI. Oversight of Service Providers and Contracts

GLB requires the University to take reasonable steps to select and retain service providers that will maintain safeguards to protect FSI. Procurement and the Office of the General Counsel will require third party vendors to protect information according to the terms of the Data Classification, Access, Transmittal and Storage Guidelines.

VII. Review and Revision of Stanford University Financial Security Information Plan

GLB requires that this Plan be subject to periodic review and adjustment. This Plan should be reassessed by the Plan Coordinator at least annually.