

STANFORD UNIVERSITY CONFIDENTIAL FINANCIAL INFORMATION SECURITY PLAN

Stanford University is committed to the ongoing protection of confidential financial information that it may collect from faculty, staff, students, alumni and others. The Gramm-Leach-Bliley Act¹ (GLB) mandates that Stanford University “develop, implement and maintain a comprehensive information security plan” to ensure the safeguarding of confidential financial information. For the purposes of this Plan, Confidential Financial Information (“CFI”) shall be that 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. In addition, this Plan shall apply to any credit card or bank account information received in the course of business by the University, regardless of whether the transaction is covered by GLB. This Plan sets the policy to ensure ongoing protection of CFI 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 CFI

Confidential Financial Information (“CFI”) shall be that 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. In addition, although not mandated by GLB, this Plan shall apply to

¹ 15 U.S.C. sec. 6801

any credit card or bank account information received in the course of business by the University, regardless of whether the transaction is covered by GLB. Examples of CFI include bank and credit card account numbers, income and credit histories, personal tax returns and social security numbers. CFI includes both paper and electronic records.

III. Plan Coordinator

Stanford University's Plan Coordinator is the University's Executive Director, Technology Strategy & Support, or if that position becomes vacant, such other individual designated by the Director of Internal Audit. The Plan Coordinator should work in cooperation with the Office of the General Counsel, The Director of Information Technology, the Controller, the Director of Risk Management, the Registrar, the Director of Faculty Staff Housing, and any other relevant academic and administrative Schools and Departments throughout the University with access to CFI.

The Plan Coordinator should assist the various offices of the University with access to CFI to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of CFI; 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. The Plan Coordinator should also work with the Office of the General Counsel, the Procurement Department, the Registrar and other relevant Schools and Departments to identify third-party providers who may have access to CFI so that the University secures contracts with third-party providers to ensure the protection of CFI.

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 CFI by someone other than the owner of the CFI
- 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 CFI by employees
- Unauthorized requests for CFI
- Unauthorized transfer of CFI through third-parties

Stanford University recognizes that this may not be a complete list of the risks associated with the protection of CFI. Since technology growth is not static, new risks are created regularly. Accordingly, the University should actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group

and SANS for identification of new risks. 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 Internal Audit's current risk assessments are sufficient to provide security and confidentiality to CFI 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 CFI. 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 CFI should receive proper training on the importance of confidentiality of student records, student financial information, credit card numbers, credit checks, bank accounts, tax records and any other CFI maintained by the University. Each new employee 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 CFI to an unauthorized individual. As appropriate, the training may include pretext calling -- where a supervisor attempts to obtain CFI through the use of deceit -- to highlight the importance of protecting CFI and to protect against identity theft. Training should also include the methods for proper disposal of documents that contain CFI.

Periodically as necessary, each department responsible for CFI should provide training to all employees to remind them of the importance of CFI 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 CFI to protect against disclosure.

B. Information System Security

Access to CFI through the University's computer network is limited to those employees who have a business reason to have such information. Each employee with access to CFI is assigned a user name and password. All databases containing

CFI should be password-controlled. Only employees with the need to have access to such information should have access to the password-controlled CFI.

Stanford University will take reasonable and appropriate steps consistent with current technological developments to make sure that all CFI is secure and to 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, and a protocol has been developed by the Office of Technology Strategy & Support to react to intrusions into the University's computer network.

To the extent reasonably available, encryption technology should be utilized for both storage and transmission of all CFI. All CFI should be maintained on servers that are behind a University firewall. All firewall software and hardware maintained by ITSS should be kept reasonably current. In addition, the University has a number of policies in place to provide security to its information systems.

C. Physical Security of Paper Records

Only employees who have a business reason to have CFI 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. Electronic Commerce at Stanford

The University has established appropriate guidelines for conducting online electronic commerce transactions, as provided in Administrative Guide Memo 65. All electronic commerce programs should be in compliance with <http://adminguide.stanford.edu/65.pdf>

E. Disposal of Records

The University should only keep physical paper records and electronic documents 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 CFI. Contracts entered into prior to June 24, 2002 should be modified to include an appropriate commitment to safeguarding CFI by May 2004. Any post June 24, 2002 contract should be modified to include the commitment to safeguarding CFI. The Plan Coordinator will work with the Office of the General Counsel to put such agreements into place.

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

GLB mandates that this Plan be subject to periodic review and adjustment. With respect to the security of information resources, the technology is constantly evolving so the expectation is that the Office of Technology Strategy & Support will constantly monitor the technology and make adjustments as necessary to preserve the infrastructure. The remainder of the processes required by this Plan should be reassessed by the Plan Coordinator at least annually.