

Information Security Program

Humboldt State University

I. Preamble

In order to protect critical information and data, and to comply with Federal Law¹, the campus Information Security Officer is responsible for establishing certain practices in the University information environment and institutional information security procedures. While these practices mostly affect Information Technology Services (ITS), some of them will impact diverse areas of the University, including but not limited to the Office of Enrollment Management, Fiscal Affairs, Library, University Advancement, Disabled Student Resource Center, Housing, Dining, Student Health Center, Book Store, and Extended Education as well as any third party contractors providing services on or to the campus. The goal of this document is to define the University's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program, and to position the University for likely future privacy and security regulations.

II. Definitions

Covered Data and Information for the purpose of this document include, but are not limited to, personally identifiable information (e.g., social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity and personal financial information (e.g., Student Financial Information). Covered data and information includes both paper and electronic records.

Student Financial Information is that information the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University 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 financial information include bank and credit card account numbers and income and credit histories.

Relevant Offices are those administrative units of the University that collect, process, or have responsibility for storing Covered Data and Information in a database or file.

III. Gramm Leach Bliley (GLB) Requirements

GLB mandates that the University appoint an Information Security Program Coordinator (an "Information Security Officer" in the parlance of the California State University), conduct a risk assessment of likely security and privacy risks, institute a training program for all employees

¹ The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley (GLB) 15 U.S.C. §6801

who have access to Covered Data and Information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

IV. Information Security Officer

In order to comply with GLB and in conformance with California State University policy, the President has appointed an Information Security Officer (ISO). This individual must work closely with the Office of General Counsel (OGC) as well as all Relevant Offices. The ISO is presently the Director of Information Technology Services.

The ISO must help the Relevant Offices identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Covered Data and Information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program.

V. Risk Assessment and Safeguards

The ISO must work with all Relevant Offices to identify potential and actual risks to security and privacy of information. The administrator of each Relevant Office, or designee, will conduct an annual data security review, with guidance from the ISO. This review shall identify any employees in the office who work with Covered Data and Information. In addition, ITS will conduct a quarterly review of its procedures, incidents, and responses for the purposes of improving the Information Security Program, educating the University community on network security and privacy issues, and preparing reports for the University Executive Committee. ITS procedures and responses are appropriately reflective of those widely practiced at other universities, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

In order to protect the security and integrity of the University network and its data, ITS has developed and will maintain a registry of all computers attached to the University network. This registry will include, where relevant, IP address or subnet; MAC address; physical location; operating system; intended use (server, personal computer, lab machine, residence hall machine, etc.); the person(s) or department primarily responsible for the machine; and whether the machine has special access to any Covered Data and Information.

ITS assumes the responsibility of assuring that patches for the software environments (e.g., operating system, system software, database management systems, and application packages) for centrally managed servers (e.g., human resources, financial, student administration, electronic mail, Web services, course management, and directory) are reasonably up to date, and will keep records of patching activity. ITS will review its procedures for patches to its software environments at least annually and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly. The ISO will work with all other areas of the University to develop guidelines for the maintenance and management of the software

environments of any servers connected to the campus network but located outside the central server area.

ITS will assure the physical security of all centrally managed servers which contain or have access to Covered Data and Information. The ISO will work with all other areas of the University to develop guidelines for physical security of any servers connected to the campus network but located outside the central server area. The ISO will conduct periodic surveys and audits of other physical security risks, including the storage of paper records containing Covered Data and Information in non-secure environments, and other procedures, which may expose the University to risks.

The ISO bears primary responsibility for the identification of internal and external risk assessment, but all members of the University community are involved in risk assessment. The ISO, working in conjunction with the Relevant Offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB.

Working through the Identity Management Oversight and Policy Review Committee, and with the approval of the University Executive Committee, the ISO will establish a point of authentication for each member of the University community (e.g., administrators, faculty, staff, students, auxiliary employees, and independent contractors). ITS will establish a record for that member in its Lightweight Directory Access Protocol (LDAP) database upon notification that the responsible office has authenticated the member.

The ISO will work with the Relevant Offices to develop and maintain a registry of those members of the University community who have access to Covered Data and Information. The ISO in cooperation with Human Resources will work to keep this registry rigorously up to date.

The ISO, working in cooperation with Relevant Offices, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (e.g., financial, student administration, human resources, development, etc.). ITS shall not create a user account to access Covered Data and Information without the express authorization of the appropriate responsible person or office (i.e., the “data owner” as that term is used in Humboldt State University’s Appropriate Use Policy). The ISO and the Relevant Offices will conduct audits of activity at least twice a year, and will report any significant questionable activities.

Each Relevant Office is responsible for securing Covered Data and Information in accordance with all privacy guidelines. A written security document that details the information security policies and processes will be maintained by each Relevant Office and will be made available to the ISO upon request. In addition, ITS will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic information and that guard against the unauthorized use of such information.

ITS maintains written plans and procedures to detect any actual or attempted attacks on covered systems and maintains incident response procedures for actual or attempted unauthorized access to covered data or information.

The ISO annually will review the ITS disaster recovery program and data-retention policies and present a report to the Executive Committee.

VI. Employee Training and Education

ITS will work in cooperation with Human Resources and the Faculty Development Coordinator to develop training and education programs for all employees who have access to Covered Data and Information.

VII. Oversight of Service Providers and Contracts

The University will select appropriate service providers that are given access to Covered Data and Information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to Covered Data and Information, the evaluation process shall include the ability of the service provider to safeguard Covered Data and Information. Contracts with service providers will include, to the extent possible, the following provisions: an explicit acknowledgment that the contract allows the contract partner access to Covered Data and Information; a specific definition of the Covered Data and Information being provided; a stipulation that the Covered Data and Information will be held in strict confidence and accessed only for the explicit business purpose of the contract; a guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract; a guarantee from the contract partner that it will protect the Covered Data and Information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information; a provision allowing for the return or destruction of all Covered Data and Information received by the contract partner upon completion of the contract; a stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract; a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the University, to immediately terminate the contract without penalty; a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and a provision ensuring that the contract's protective requirements shall survive termination of the agreement.

VIII. Evaluation and Revision of the Information Security Program

GLB mandates that this Information Security Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within ITS where constantly changing technology and constantly evolving risks indicate the wisdom of regular reviews. Processes in other Relevant Offices such as data access procedures and the training program also should undergo regular review. The program itself as well as the related data retention policy will be reevaluated annually by the Identity Management Oversight and Policy Review Committee.

Approved: University Executive Committee, June 12, 2003