POLICY CONCEPT FORM

Name and UO Title/Affiliation:	Mark McCulloch, Director of BAO Information Systems
Policy Title/# (if applicable):	IV.06.06 – Customer Information Security Program
Submitted on Behalf Of:	Business Affairs Office
Responsible Executive Officer:	Jamie Moffitt, VPFA/CFO

SELECT ONE: ☐ **New Policy** ☐ **Revision** ☒ **Repeal**

Click the box to select

HAS THE OFFICE OF GENERAL COUNSEL REVIEWED THIS CONCEPT: ☐ **Yes** ☒ **No**

If yes, which attorney(s):

Submitted to Bryan Dearinger; should have review before 10/2 PAC meeting

GENERAL SUBJECT MATTER

Include the policy name and number of any existing policies associated with this concept.

Customer Information Security Program Policy Number: IV.06.06

RELATED STATUTES, REGULATIONS, POLICIES, ETC.

List known statutes, regulations, policies (including unit level policies), or similar related to or impacted by the concept. Include hyperlinks where possible, excerpts when practical (e.g. a short statute), or attachments if necessary. Examples: statute that negates the need for or requires updates to an existing policy; unit level policy(ies) proposed for University-wide enactment; or existing policies used in a new, merged and updated policy.

Information Security Program Policy Number: IV.06.01; Information Asset Classification & Management Policy Number: IV.06.02; Unit level policy entitled "GLBA Compliance Program" authorized Feb 2019 by Roger Thompson and Leo Howell

STATEMENT OF NEED

What does this concept accomplish and why is it necessary?

This policy should be repealed. It is outdated and has been superseded by the policies listed above. It is not just duplicative and redundant.

AFFECTED PARTIES

Who is impacted by this change, and how?

None; the policy has already been superseded.

CONSULTED STAKEHOLDERS

Which offices/departments have reviewed your concept and are they confirmed as supportive? (Please do not provide a list of every individual consulted. Remain focused on stakeholders (e.g. ASUO, Office of the Provost, Registrar, Title IX Coordinator, etc.).)

Name	Office	Date
Leo Howell	**Chief Information Security Officer**	**27 Aug 2019**
Roger Thompson	**Vice President for SSEM**	**30 Aug 2019**
Kelly Wolf	**AVP and Controller**	**30 Aug 2019**

Reason for Policy

Summarizes the University of Oregon's comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act (GLBA). In particular, this document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Entities Affected by this Policy

University community

Web Site Address for this Policy

https://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/customer-information

Responsible Office

For questions about this policy, please contact the Chief Information Officer at 541-346-1702, cio@uoregon.edu.

Enactment & Revision History

03/30/16: Technical revisions made by the University Secretary and policy number revised from 01.00.12 to IV.06.06
02/08/2010 Policy number revised from 3.100 to 01.00.12
11/2003 Reviewed and Recommended by President Dave Frohnmayer

Policy

Designation of Representatives: The Vice President for Student Affairs will designate a Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

Scope of Program: The Program applies to any record containing nonpublic financial information about a student whether in paper, electronic or other form, that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student provides in order to obtain a financial service from the Institution, (ii) about a student resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student in connection with providing a financial service to that person.

Policy: The Program Officer will oversee and coordinate a comprehensive written information security program as mandated by the Federal Trade commission's Safeguards Rule and the Gramm-Leach-Bliley Act.

Elements of the Program:

1. Risk Identification and Assessment. The Institution intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- Employee training and management. The Program Officer will coordinate with institutional representatives to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area, including, 05.00.04, Student Records Policy and UO Policy 571.020, (Student Records.
- Information Systems and Information Processing and Disposal. The Program Officer will coordinate with representatives of the Computing Center to assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current Acceptable Use Policy, Records Retention Policy and procedures for Confidential Document Destruction. The Program Officer will also coordinate with the Computing Center to assess procedures for monitoring potential information security threats associated with software systems and for updating such

systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- <u>Detecting, Preventing and Responding to Attacks.</u> The Program Officer will coordinate with the Computing Center to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the Computing Center the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer in coordination with appropriate institutional representatives will, on a regular basis, evaluate safeguards to control the risks identified through such assessments and 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 Program Officer shall coordinate with those responsible for the third party service procurement activities among relevant parties (e.g. the Business Affairs Office) and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students. In addition, the Program Officer will work with the Office of the General Counsel to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Office of the General Counsel. These standards shall apply to all existing and future contracts entered into with such third party service providers, provided that amendments to contracts entered into prior to June 24, 2002 are not required to be effective until May 2004.

4. Adjustments to Program. The Program Officer is responsible for evaluating and adjusting the Program on a periodic basis based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.

Related Resources

NA

THE UNIVERSITY OF OREGON
GLBA Information Security Program (GISP)

Purpose & Objectives

This document summarizes the University of Oregon's ("Institution") information security program mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). The objectives of the program are to (i) identify and ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats to the security of covered records, (iii) protect against the unauthorized access or use of covered records or information in ways that could result in substantial harm or inconvenience to customers.

Program Sponsors

Vice President for Student Services and Enrollment Management
Chief Information Security Officer

Designation of Representatives

The UO Chief Information Security Officer provides general oversight to ensure that the program objectives are met. The Associate Director of Operations for the Office of Student Financial Aid and Scholarships (OSFAS) is designated as the Program Manager, with responsibilities for coordinating the program to ensure ongoing activities are executed to support compliance. Any questions regarding the implementation of the GISP or the interpretation of this document should be directed to the Program Manager.

Program Scope

The following are key components of the GISP program environment scope. Appendix A illustrates how these components conceptually are interconnected with each other and demonstrates data flow across the environment.

- **SENSITIVE FINANCIAL AID DATA (SFAD).** This includes any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form, which is handled or maintained by or on behalf of the Institution or its affiliates (I.e., information covered by GLBA). For these purposes, the term nonpublic financial information refers to any information (i) a student or other third party provides to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. In addition to SSN, date of birth, and other Personally Identifiable Information (PII), examples include Expected Family Contribution (EFC); Tax information including, but not limited to Adjusted Gross Income (AGI) and Untaxed income; Citizenship and veteran status; and other data elements transferred from the US Department of Education (ED).
- **SFAD ENVIRONMENT (SFADE).** This includes any computer system or network of systems that directly processes, stores or transmits SFAD.

- **SFAD CONNECTED SYSTEM**. This includes any system that can be used to directly access, modify or change SFAD.

GISP Program Elements

Risk Assessment

This element includes continuous monitoring and assessment to identify internal and external risks to the security, confidentiality, and integrity of SFAD that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The following procedures are coordinated by the Program Manager, in collaboration with the University Information Security Office.

Activity Name	Description	Frequency
GISP Risk Assessment Session	Risk assessment sessions with multiple stakeholders, including the OSFAS, ISO, and Information Services (IS) to discuss security risks related to SFAD. Identified risks are documented and appropriate mitigation controls identified and planned. Specific areas addressed as part of the risk assessment include areas listed in this table. Systematic weaknesses related to any of the items below are addressed during discussion sessions and the safeguards are adjusted as needed.	Annual
User Awareness Training	Coordination with ISO and IS to verify that users with access to SFAD are in compliance with the training requirements outlined in this program.	Continuous
IT Professional Training	Coordination with ISO and IS to verify that IT Professionals with access to SFAD, the SFADE and the SFAD Connected Systems follow the training requirements outlined in this program.	Continuous
User Access Certification	Review sample of users with access to SFAD to ensure effectiveness of the certification procedure - user access is expeditiously removed when no longer needed (e.g., employment terminations of role changes)	Annually (Ongoing Account Termination Notices)
Vulnerability Scans	Review executive summary reports of vulnerability scans to ensure that identified critical vulnerabilities are being addressed within 30 days based on vendor release and project risk-impact assessment	Quarterly
Monitoring, Detection and Response	Coordination with IS and ISO to verify that all systems within the SFADE and SFAD Connected systems environment are included in the ISO monitoring, detection and response procedure.	Continuous
Data Retention and Disposal	Coordination with the University Records Manager to verify compliance with university record retention and disposition schedule.	As needed
3rd-Party Service Providers and External SFAD Access	Coordination with the Office of General Counsel (OGC), Purchasing and Contracting Service (PCS) and ISO to review and assess risks associated with contracting terms with 3rd-party services providers and other external parties provided with access to SFAD.	Annual

Safeguards

This element outlines key safeguards in place for protecting SFAD and mitigating risks identified through the risk assessment element above. The SFADE and SFAD Connected systems are hosted and supported by the university Information Services department. The table below highlights other key controls for protecting SFAD.

Control	Description	Frequency
Risk Assessment	Risk related to GLBA and SFAD is included in the IS Risk Matrix and are analyzed, prioritized and mitigated as part of the university enterprise risk management program governed by the university Strategic Enterprise Risk Management Committee (SERMC).	Continuous
Physical Security	The SFADE and SFAD Connected Systems and data storage are hosted in the university datacenters which are physically secured including access control and video surveillance. End User devices should follow ISO standards.	Continuous
User Training	All users with access to SFAD are enrolled in our GLBA User Awareness training module. This training is a component of the ISO user awareness training program, specifically designated for with access to SFAD. Specific modules include UO Core Cybersecurity Awareness module and the GLBA Training module.	Annual
IT Professional	All IT professionals with privileged access to SFAD, the SFADE or SFADE Connected Systems are enrolled in the ISO security awareness training program designated for IT Professionals. Specifically, this includes all modules in the User Training section plus the UO IT Training module.	Annual
User Access Certification	Users with access to SFAD are periodically recertified. A senior member from each user's unit is contacted to certify that that the user is still in an active UO employee and that his/her role still requires access to SFAD. Additionally, access is removed when employees leave the UO or change jobs and no longer require access as an essential job function.	Annual
Personnel Security	Background checks are required as part of the hiring process at the University of Oregon. Student workers who have access to covered data are also required to undergo a background check as of March 2018.	Hiring Process
Identification Controls	Identification Controls over SFAD, the SFADE and SFADE Connected Systems include, at a minimum: • **CMS.** Management by an ISO-approved university configuration management system (CMS) - e.g., JAMF, SCCM, Puppet, etc. • **Internal vulnerability scans.** All systems within the SFADE and SFADE Connected Systems are included in ongoing vulnerability scans. Critical vulnerabilities are addressed within 30 days of identification. • **External vulnerability scans.** All systems within the SFADE and SFADE Connected Systems (accessible externally) are included in ongoing ISO external vulnerability scans. Critical	Continuous

	vulnerabilities are addressed within 30 days of identification.	
Protection	Additional protective controls over SFAD, the SFADE and SFADE Connected System include, at a minimum: • Physical Security • System Hardening • Security Updates • Antivirus • Auto-lock consoles (servers) or computer screens (desktops or laptops) • Firewall (Host-based and/or Network) • Encryption: Data-at-Rest (for all non-server devices stored outside of university datacenters) • Encryption: Data-in-Transit • User Access Control: Unique Account • User Access Control: Least Privilege Access • User Access Control: Access Approval • User Access Control: Authentication (application and database layers) • User Access Control: Limit Failed Login Attempts (10) • User Access Control: Inactive Session Timeout (8 hours) • User Access Control: Two-Factor Authentication (for remote access or any privileged access) • User Access Control: Remote Access Security (including use of University VPN)	Continuous
Monitoring & Detection	**Logging & Monitoring**. Logs are generated and sent to the university Security Incident and Event Management (SIEM) system for correlation, event monitoring and detection. Potential incidents are investigated by ISO in collaboration with the relevant IS support staff and OSFAS. **External Threat Intelligence.** ISO monitors various external sources including vendor alerts and notifications, various information sharing analysis center (ISAC) alerts for threats or weaknesses affecting UO systems, including those in the SFADE and SFADE Connected Systems. Identified threats or weaknesses are addressed by ISO in collaboration with appropriate IS support staff. **Intrusion Detection**. The SFADE is monitored via the University Intrusion Detection System.	Continuous
	High Risk Users. Users with access to SFAD and the SFADE are high risk users under the GISP. In the event of incidents or compromises, these users receive priority treatment to reduce risks to the university.	
Incident Response	Potential incidents relating to SFAD are reported as quickly as possible to the ISO office for investigation and assessment. Confirmed incidents impacting SFAD will be reviewed by the university DSIRT (Data Security Incident Response Team) and appropriate groups are notified (including the US Department of Education).	Continuous

3rd-Party Service Providers and External SFAD Access	Third parties with external SFAD sign confidentiality agreements that are reviewed by ISO, the UO General Counsel and Purchasing and Contracting Services.	At time of initial contract(s) and subsequent renewal(s)

Reporting

The Program Manager will provide an annual report on compliance highlighting each program element above. Specifically, the report will include:

i. ***Employee training and management***. This includes summarized reports on percentage of employees who have successfully completed the mandatory awareness training, and the status of the Financial Aid annual user access certification procedure.

ii. ***Annual access reviews.*** This includes a summarized report of number of users with access to types of SFAD. It also includes dates of access reviews for Federal sites, Banner, and other connected systems, as well as certification dates for users outside the OSFAS.

iii. ***Notes.*** This section covers any changes proposed or made to the program, or other topics that need to be highlighted.

Adjustments to Program

The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.

Authorization

The GISP is sponsored and authorized by the underlying signatories.

Feby 13, 2019

Roger Thompson, Vice President for Student Services and Enrollment Management   Date

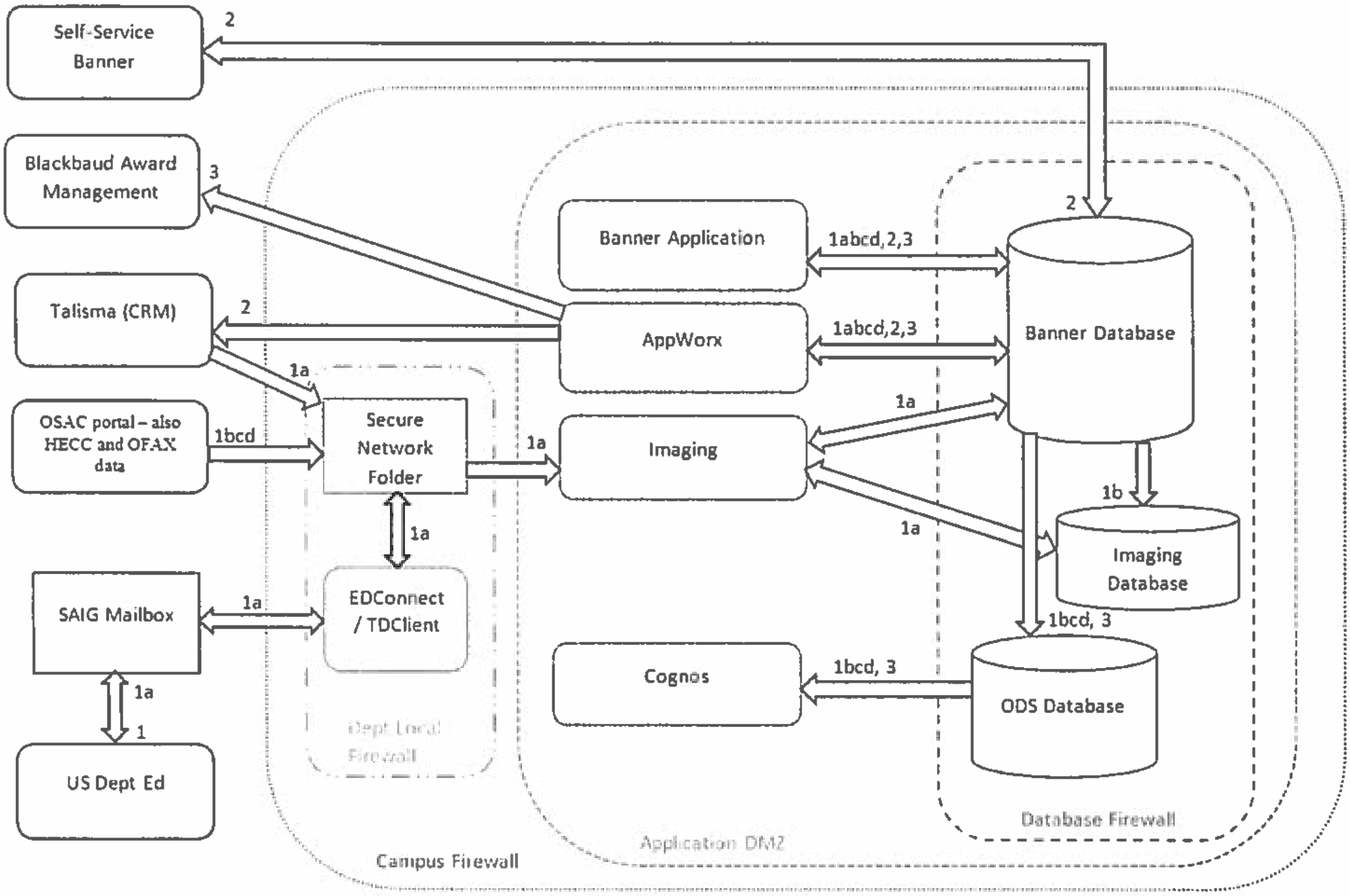
LHowell   2/13/19

Leo Howell, Chief Information Security Officer   Date

Appendix A

Data Flow & Application System Architecture (or Network) Diagram

Application System Architecture



SFAD Elements Included

1a. SSN, name, DOB, address, some files include Parent(s) SSN, name and DOB as well. Other files may also include citizenship status and tax information.
1b. SSN, name, DOB
1c. SSN, name, EFC, AGI, year in college
1d. SSN name, DOB, class registration, degree sought
2. Name, award information*, EFC, and outside scholarships
3. Name, DOB, address, citizenship status, test scores, GPA

*Information about some awards can identify a student's level of need

References

National Association of College and University Business Officers (NACUBO) - www.nacubo.org
National Association of Financial Aid Administrators (NASFAA) www.nasfaa.org