University of Arizona
Security Program

I. Introduction

The Gramm-Leach Bliley Act (GLBA) requires financial institutions, including colleges and universities, to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information issue. The scope of this Act covers primarily financial institutions but also organizations containing financial functions including colleges and universities.

The University of Arizona currently has a comprehensive security program with several coordination roles, procedures and resources already well established

II. Objective

The objectives of this security program is:

- to ensure the security and confidentiality of personal information;
- to protect against any anticipated threats or hazards to the security or integrity of such information; and
- to protect against the unauthorized access to or use of such information that could result in substantial harm or inconvenience.

III. Program Coordination

University Information Security Officer (UISO) - responsible for overseeing security and privacy issues within the University including:

- Coordinating of University systems data access and network and computer security
- Conducting an annual assessment on privacy and security issues and submitting a formal report
- Acting as coordinator and contact person for privacy and security issues
- Overseeing implementation of the recommendations on privacy and security (beginning with the Final Report of the Information Security Advisory Council)
- Chairing the Information Security Advisory Board

Information Security Advisory Board (ISAB)

The objectives of the Information Security Advisory Board are to:

- Oversee development and updating of policies on privacy, security, access, and disclosure, using the Guiding Principles in the Information Security Council's Report.
- Recommend policies to the President or the Information Technology Policy Group, as appropriate.
- Endorse and encourage implementation of campus-wide standards and processes to improve information security.
- Advise the Information Security Officer in resolving concerns and disputes.

- Be a sounding board regarding privacy and information security issues.
- Engage the campus community in open discussion of privacy and security concerns for purposes of general education.

Security Incident Response Team (SIRT) – the mission of this group is to provide campus coordination of action and information concerning breaches of computer and network security.

System Support Analyst - assists the Security Officer and ISAB with Standards, Policy development and training and awareness programs.

IV. Risk Assessment and Safeguards

Security Incident Response Team

- Monitors in-bound Internet traffic for intrusion attempts
- Assists departments with repairing computing systems that have been hacked
- Issues notifications and takes appropriate actions to protect the Universities networked resources from Internet worms
- Performs vulnerability scans of departmental networks, and identification of unknown modems

Business Continuity and Disaster Recovery

- Established an off-campus computing recovery site with facilities for ensuring operation
  - University's bi-weekly payroll processing and printing
  - NetID validation
  - Virus protection updates
- Data back-ups for departmental servers located in the recovery site

Other

- Virus protection update service for enterprise systems and departmental servers is provided
- The following technologies were implemented and ensure the security the University's data network:
  - Virtual Private Network (VPN) capability for off-campus and wireless access to our network
  - Reflexive access-list capability for departmental control over in-coming network traffic
  - Web-accessible mechanisms for ensuring the validity of vendor supplied program updates
- Research and resolve all security and privacy incidents reported
- Information Security and Privacy web page (www.arizona.edu/security) to be a single point of reference for the University with external information security resources, project plans, status reports, and opportunities for providing input and feedback

V. Employee Training and Education

- Created and maintain an Information Security / Privacy Web Page (http://w3.arizona.edu/~security) that includes:
  - Polices, Proceedures, Guidelines, Standards and other Related Documents
  - Prevention advice
  - Virus and Hoax information
  - News and Current Events

- Publish a variety of security and privacy related articles in CCIT newsletter

- Purchased and made available to campus affiliates the SANS Institute Step-by-Step Security Guides available at ()

- Developed and published the following pamplets for the University community:
  - Privacy Basics: Guide for Protecting Personal Information
  - Security Basics: Guide for Securing Your Personal Computer
  - Risk Reduction: Guide for Computer Protection and Prevention

- Created FAQ's: *Information Security and Privacy* (http://w3.arizona.edu/~security/faqs.htm)

- Utilization of a security and privacy awareness consultant to help with a campus wide security and privacy awareness and training program.

  - Faculty, staff and Students with access to university systems and data are aware of, and use, appropriate security measures to protect university systems and data.

VI. Oversight of Service Providers and Contracts

- Specific security related language should be included in all RFP's and contracts with third parties when the vendor will have access to university data. If you are unsure whether you need to include such language in a contract contact Procurement and Contracting for advice.

  See section IV of UA's Guidelines for Collection, Use and Disclosure of Personal Information (http://w3.arizona.edu/~security/guidelines.htm) for more information on what should be included.

VII. Evaluation and Revision of this Program

An ABOR sponsored effort to conduct a security assessment by a private consultant. The intention is to establish a baseline to measure future enhancements and management of computer and network security.

Primary focus is:

- Security assessment through network scanning and other means
- Allow UA to gain an in-depth knowledge of the consultant's technical and operational capabilities and more specifically how these capabilities might be leveraged by the University to support our academic mission.
- Report on findings
- Recommendations based on findings

- A helpful checklist for security assessment is available at (http://w3.arizona.edu/~security/Security_Assessment_Checklist.pdf). Departments should pay attention to the items highlights in blue.

VIII. Policies

Over the past several years this program with input and help from many groups on campus has produced policy, guidelines and support procedures that address the items mentioned.

- Currently, Faculty and staff are informed through various media on security and privacy related guidelines, procedures, policies, principles, and other related important statutes.

  Minimally everyone should read and understand the following documents
  - Acceptable Use of Computers and Networks at UA
  - http://w3.arizona.edu/~security/uaacceptableuse.htm
  - Electronic Privacy Statement
    http://w3.arizona.edu/~security/uaelectprivstmt.htm
  - Employee access to institutional data
  - http://w3fp.arizona.edu/dataadmn/access.htm
  - Guidelines for Collection, Use and Disclosure of Personal Information
    http://w3.arizona.edu/~security/guidelines.htm
  - HIPPA
    http://www.irb.arizona.edu/hipaa.html
  - University of Arizona Policy on Release of Student Information
    http://www.registrar.arizona.edu/ferpa/

A comprehensive list of guidelines, procedures, policies, principles, and other related links can be found on the Policy and Procedures page of the Security and Privacy page at http://w3.arizona.edu/~security/pandp.htm.

A security policy is being developed to communicate user-based responsibilities for protecting university systems, data and related campus resources.

Supporting security system administration standards and user guidelines are being developed to help university employees responsible for IT and departmental security.

Questions regarding the implementation of the Program or the interpretation of this document should be directed to the University Information Security Officer or his or her designees.