



GUIDELINES

ABOR Information Security Program Guidelines

Overview

These guidelines offer guidance for information security programs to be developed, implemented, and maintained by the universities pursuant to the Board's Information Security Policy. They are based on the *Educause Effective IT Security Practices and Solutions Guide: Balancing the Need for Security and Open, Collaborative Networking* and ISO/IEC 27002. University information security programs should incorporate each of the following topics. Definitions are set forth below in Section 13.0

1.0 Internal organization

A management framework lead by an Information Security Officer or Director should be established to initiate and control the implementation of information security within the university. University leadership should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the university.

1.1 External parties

The security of the university's information and information processing facilities should be a consideration in the introduction of external party products or services or in providing access to university information systems.

2.0 Asset Classification

Each university should classify its information assets to determine which information systems, data, facilities, equipment, and personnel constitute the critical information infrastructure of the university.

2.1 Responsibility for assets

A responsible party should be identified for each critical asset, and that person will be responsible for the maintenance of appropriate controls. The implementation of specific controls may be delegated as appropriate.

2.2 Information classification

Information should be classified to indicate its sensitivity and criticality. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.



GUIDELINES

3.0 Personnel Security

Each university should take into account security responsibilities when recruiting and contracting with permanent employees, contractors and temporary staff as required in the Tri-University Personnel Guidelines on protecting university information and systems.

4.0 Physical and Environmental Security

Each university should implement procedures and physical security measures to prevent and detect unauthorized access or damage to facilities that contain information systems.

4.1 Secure areas

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.

4.2 Equipment security

Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site and equipment being disposed is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. Equipment site and disposal should also be considered. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

5.0 Communications and Operations Management

Each university should establish controls for changes to information processing facilities, systems, software, and procedures.

5.1 Operational procedures and responsibilities

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures. Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

5.2 Third party service delivery management

For agreements in which a third party may have access to sensitive or critical information or systems, the university should monitor implementation of the agreements



GUIDELINES

5.3 System planning and acceptance

To minimize the risk of systems failures, advance planning and preparation are required to protect the availability of adequate capacity and resources to deliver the required system performance.

The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

5.4 Protection against malicious and mobile code

Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

5.5 Back-up

Back-up procedures should be documented and the university should develop processes for timely restoration of back-ups.

5.6 Network security management

The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. Additional controls may also be required to protect sensitive information passing over public networks.

5.7 Media handling

Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

5.8 Monitoring

Systems should be monitored and information security events should be recorded and reported as required in Board policy and applicable law. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

6.0 Access Control

Business requirements for access control should be documented and users should be made aware of their responsibilities.

6.1 User access management

Formal procedures should be in place to control the allocation of access rights to information systems and services.



GUIDELINES

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

6.2 User responsibilities

The co-operation of authorized users is essential for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

6.3 Network access control

Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network.

6.4 Operating system access control

Security facilities should be used to restrict access to operating systems to authorized users.

6.5 Application and information access control

Security facilities should be used to restrict access to and within application systems.

Logical access to application software and information should be restricted to authorized users.

6.6 Mobile computing

To ensure information security when using mobile computing the protection required should be commensurate with the risks these specific ways of working cause.

When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied.

7.0 Information System Development and Maintenance

Each university should establish internal procedures for the secure handling and storage of its electronically-stored information to prevent unauthorized access or misuse.

7.1 Security requirements of information systems

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development or implementation of information systems.



GUIDELINES

All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

7.2 Correct processing in applications

Appropriate basic security coding controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

7.3 Cryptographic controls

A policy should be developed on the use of cryptographic controls to protect the confidentiality, authenticity or integrity of information by cryptographic means. Key management should be in place to support the use of cryptographic techniques.

7.4 Security of system files

Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

7.5 Security in development and support processes

Project and support environments should be strictly controlled.

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

7.6 Technical Vulnerability Management

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

8.0 Business Continuity Management

Each university should establish procedures for developing and maintaining disaster recovery and business continuity plans to ensure essential services and communications remain available in the event damage, loss or disruption of information systems due to an emergency or disaster.



GUIDELINES

8.1 Information security aspects of business continuity management

The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the university.

9.0 Compliance

The universities should ensure they are in compliance with current legal requirements and provide awareness and compliance training to all users.

9.1 Compliance with security policies and standards, and technical compliance

The security of information systems should be regularly reviewed.

Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

9.2 Information systems audit considerations

There should be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools.

10.0 Incident Management

Each university should implement clear procedures for reporting and handling of information security incidents. These procedures should include reporting of incidents to the ABOR Central Office as required by Board policy and other reporting as required by law.

10.1 Reporting information security events and weaknesses

Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of university assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

10.2 Management of information security incidents and improvements

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of



GUIDELINES

information security incidents. Evidence should be collected and maintained in compliance with legal requirements.

11.0 Risk Assessment

Information security programs should be based on risk assessment and developed in consideration of university priorities, staffing, and budget.

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the university. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the university or individual information systems.

Risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The information security risk assessment should have a clearly defined scope in order to be effective and should include relationships with risk assessments in other areas, if appropriate.

12.0 Definitions

- A. Architecture (See Tri-University IT Architecture)
- B. Communications: Analog and digital networks, communication processors, software, frame relays, phone switches, cabling, wiring, LAN/WAN and other items associated with communications within the college or unit, including items with potential impact on the university's communication infrastructure.
- C. Facilities: Improvements or expansions of existing facilities, as well as rentals, leases or purchase of new IT facilities.
- D. Funding Sources: All sources of funds (state, auxiliary, grant, gift, etc.) required to support personnel, capital, and operations.
- E. Hardware: Computer hardware and peripherals used on a project, including mainframes, midrange, micro- and mini-processors, laptops, hand-held devices, and peripheral devices such as disk drives and printers.



GUIDELINES

- F. Information Technology (IT) Project: Any project with total expenditures in the following categories that exceed \$1 million over five years:
 - 1. Capital Microcomputers Electronic Data Processing (EDP) Equipment/Computer Main Frame Electronic Data Processing – Other
 - 2. Maintenance
 - 3. EDP Equipment – R/M Telecommunications (telephone and internet access) Other Operations
 - 4. EDP Services
 - 5. EDP Supplies
 - 6. Equipment
 - 7. IT Personnel Expenses (including Employee Related Expenses [ERE] staff/administrative, service professional, student and graduate student expense in any of the identified job titles/classifications.

- G. IT Services: Third-party consultants and contractors, such as management, administration, project leaders, operations or technical support, and programmers.

- H. Licensing and Maintenance Fees: Licensing and maintenance fees for hardware, software and other products.

- I. Other IT Costs: Other IT costs not included above, such as manuals, travel, and training.

- J. Full Time equivalent (FTE) Positions:
 - 1. IT - The number of FTE IT positions assigned to the project, including college or unit and central IT positions.
 - 2. User - The number of non-IT college or unit FTE positions assigned to the project for design, development and implementation.

- K. FTE Cost:
 - 1. IT - The total personnel dollars expended for IT FTEs, including ERE (Employee Related Expenses) at its most current rate.
 - 2. User - The total personnel dollars expended for user FTEs, including ERE.

- L. Professional and Outside Consultant Positions: The number of consultants, contractors and personnel used on a project (does not include University employees).

- M. Software: All costs related to purchase of applications and systems related software for the project.

- N. Tri-University IT Architecture: The Tri-University IT Architecture (Tri-University ITA) is intended to provide a framework for information technology use at



GUIDELINES

Arizona's three state universities. The ITA facilitates the application of IT to University initiatives and projects. Its goal is to aid in the efficient and effective implementation of technology on campuses by describing a direction for current and future IT activities, supported by underlying principles, standards, and best practices. The six domains are: security, software, middleware, platforms (computers), networks, data/information. It facilitates Tri-University collaboration efforts by establishing a common vision for the future of IT on our campuses.

As approved, June 2008