BOARD OF Regents ARIZONA'S PUBLIC UNIVERSITIES

EDUCATE · DISCOVER · IMPACT

GUIDELINES

Tri-University Personnel Guidelines on Protecting University Information and Systems

Arizona universities should incorporate the following personnel guidelines into their business practices and procedures relating to any employee who has access to sensitive university information, research, and systems.

1. HIRING:

   A. When posting a job vacancy, indicate if the advertised position will have access to sensitive information and systems and whether the applicant will be subject to a criminal background check.

   B. When screening candidates, consider position requirements concerning information security factors in the search process, i.e. security questions during interviews, reference check requirements, past job responsibilities and experience relating to sensitive information, etc. Ensure reference check inquiries include questions about access to sensitive information and data, as well as related misconduct.

   C. Prior to hire, conduct criminal background checks in accordance with university policies as they relate to personnel with access to sensitive information and systems.

   D. Provide training for new employees on information security procedures, to include: confidentiality of student records, personnel information, financial information, medical information, research, and other types of sensitive data and information with which they will have contact. Also include information about protecting confidential information from unauthorized individuals, proper disposal of documents that contain sensitive data and information, and prompt reporting of suspected problems. Ensure that employees are aware of the consequences of not following information security policies and procedures.

   E. Ensure access controls to sensitive data and systems are in place that deny employees' access until appropriate information security training is completed.

   F. Ensure that periodic refresher training is conducted on access and responsibilities relating to sensitive data and information.

   G. Require employees to sign an appropriate statement acknowledging their responsibilities regarding access and protection of sensitive data and systems.

Tri-University Personnel Guidelines on Protecting University Information and Systems

2. INTERNAL PROMOTION or TRANSFER:

   A. Consider the use of any or all guidelines listed under section 1, Hiring.

   B. Review and change access privileges based on job related and need-to-know criteria. This applies to departments acquiring new employees and those whose employees are moving to other departments.

   C. Train newly hired or transferred employee in accordance with information security guidelines and criteria appropriate for their new job as determined by their supervisor.

   D. Conduct background checks and/or finger print checks for internal promotion and transferred employees in accordance with university policy.

3. SUPERVISION:

   A. Review with employee annually:

      1) Access privileges. Access should be revoked for all employees who do not have a business need to sensitive data and information.

      2) Notices, policies, and procedures related to non-disclosure, security and privacy.

      3) Performance and competencies specifically related to proper handling of sensitive data and information.

   B. Review job announcements, promotion, change of job responsibilities, and transfers of employees to ensure that access to sensitive data and information is appropriate to position.

   C. Immediately inform employees of any institutional or departmental changes to policies or procedures related to sensitive data and information.

   D. Review with subordinate supervisors of employees who have access to sensitive information and systems that they have fulfilled their responsibilities set forth in these guidelines and university information security policies and procedures.

Tri-University Personnel Guidelines on Protecting University Information and Systems

4. VOLUNTARY SEPARATION (e.g., RESIGNATION, RETIREMENT):

Upon receipt of notice that an employee intends to voluntarily separate from his/her university employment:

A. Determine a date to revoke all types of access rights to include building access, individual's computer systems, information access privileges, and computer system accounts.

B. Change computer/network systems shared account passwords to which the individual has access, especially those with access to privileged accounts, e.g. root, administrator, etc.

C. Properly cleanse individual's computer workstation before it is re-assigned or discarded.

D. Inform appropriate staff of change in individual's status.

E. Determine a time for all resources to be returned and ensure that resources are returned.

F. Develop appropriate termination checklist to document procedures to revoke access and secure all equipment to include:

1) The return of office and building access keys, cards, and ID badges

2) Deactivation of all access IDs and passwords

3) The return of all university data and documentation

4) The inventory and return of all resources provided to employee (e.g. laptop, PDAs, business credit cards, cell phones, etc.)

5) The transfer of ownership of all online (active and archived) files or libraries

6) Signature of a non-disclosure agreement if appropriate to protect sensitive research or other important university data.

5. INVOLUNTARY SEPARATION

Tri-University Personnel Guidelines on Protecting University Information and Systems

All guidelines in section 4, Voluntary Separation, should be followed along with the following:

A. FOR CAUSE:

1) Escort individuals while they pack their belongings and leave facilities.

2) As appropriate, notify university police.

B. RESULT OF FUNDING CUTS OR RESTRUCTURING

1) Following guidelines for voluntary separation will generally be adequate. When in doubt, follow guidelines for involuntary separation (for cause).