Personnel changes are a cause for concern when it comes to protecting the university resources. Methods must be in place to insure the protection of these resources as changes occur. All units must meet the following minimum standards governing employee access to university resources.

The following standards will assist unit supervisors in developing procedures for maintaining and securing university resources related to personnel changes. These standards should not be used to weaken procedures that may already exist.

These standards apply to all units.

Personnel changes occur for various reasons. Each reason presents its own situations and therefore is covered separately below. There may be some overlap as circumstance requires.

1. **Hiring process**
   When posting a job announcement, indicate whether the advertised position will have access to confidential university data and other mission critical university resources and the applicant filling the position will be required to have a criminal background check.

   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 confidential university data, etc.

   Ensure reference check inquiries include questions about access to confidential university data, as well as related misconduct.

   Prior to hire, conduct criminal background checks in accordance with university policies as they relate to personnel with access to confidential university data and other mission critical university resources.

2. **Post Hiring**
   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 confidential university data with which they will have contact. Also include information about protecting confidential university data from unauthorized individuals, proper disposal of documents that contain confidential university data, and prompt reporting of suspected problems. Ensure that employees are aware of the consequences of not following information security policies and procedures.

   Ensure access controls to confidential university data and other mission critical university resources are in place that denies employee access until appropriate information security training is completed.
Ensure that periodic refresher training is conducted on access and responsibilities relating to *confidential university data* and other mission critical *university resources*.

Require employees to sign an appropriate statement acknowledging their responsibilities regarding access and protection of *confidential university data* and other mission critical *university resources*.

3. **Supervision**
Managers and supervisors are responsible for securing *university resources*. To that end, they are expected to:

- Promptly inform employees about changes in university or *unit* information security policies or protocols.
- Review job announcements, promotions, change of job responsibilities, and employee transfers to ensure that access to *confidential university data* is appropriate to each position.
- Review access privileges at least annually. Access should be revoked for all employees who do not have a business need for access to *confidential university data*.
- Review notices, policies, and procedures related to non-disclosure, security and privacy annually.
- Assess performance and competencies specifically related to proper handling of *confidential university data* annually.
- Ensure that supervisors are aware of their information security and privacy obligations.

4. **Internal Promotion or Transfer**
Consider the use of any or all guidelines listed under section D1, Hiring.

- Review and change access privileges based on job related and need-to-know criteria. This applies to *units* acquiring new employees and those whose employees are moving to other *units*.
- Train newly hired or transferred employees in accordance with information security policy, standards, procedures and guidelines and criteria appropriate for their new job as determined by their supervisor.
- Conduct background checks and/or finger print checks for internal promotion and transferred employees in accordance with university policy and procedures.

5. **Voluntary Separation (e.g., Resignation, Retirement)**
Upon receipt of notice that an employee intends to voluntarily separate from his/her university employment:

- 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.
- 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.
- Properly evaluate and cleanse individual’s computer workstation before it is re-assigned or reformatted before it is discarded.
- Inform appropriate staff of change in individual’s status.
- Determine a time for all resources to be returned and ensure that resources are returned.
Follow appropriate termination checklist to document procedures to revoke access and secure all equipment to include:

- The return of office and building access keys, cards, and ID badges
- Deactivation of all access IDs and passwords
- The return of all university data and documentation
- The return of all university resources provided to employee (e.g., laptop, PDAs, business credit cards, cell phones, etc.)
- The transfer of ownership of all online (active and archived) files or libraries
- Obtain signature of a non-disclosure agreement if appropriate to protect confidential university data.

6. **Involuntary Separation (e.g. Layoffs, Discharge/Dismissal)**
   All guidelines in previous section D5 should be followed along with the following (for cause):

- In consultation with Human Resources, take appropriate actions to protect and preserve university resources.
- As appropriate, notify university police.

**Related Guidance**
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline.

**Revision History**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>08/09/07</td>
</tr>
<tr>
<td>Effective Date</td>
<td>05/27/08</td>
</tr>
</tbody>
</table>