Manager Information Security Standard

<table>
<thead>
<tr>
<th>Title</th>
<th>Manager Information Security Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>IS-S400, V002</td>
</tr>
<tr>
<td>Responsible Office</td>
<td>Information Security Office</td>
</tr>
<tr>
<td>Effective Date</td>
<td>18-December 2017</td>
</tr>
<tr>
<td>Last Updated</td>
<td>12/6/2017</td>
</tr>
</tbody>
</table>

I. BACKGROUND AND SCOPE

People play a fundamental role in protecting the University of Arizona’s (University) resources. Therefore, the management of human resource security and privacy risks is necessary during all phases of association with the university, including pre-hiring, during employment, at changes of employment within the University, and at the termination of employment.

The following checklist will assist unit supervisors in ensuring that they have done their due care in securing university resources related to personnel changes. This checklist should not be used to weaken procedures that may already exist.

This guideline applies to all University units.

II. DEFINITIONS

Authorization: The act of granting permission for someone or something to conduct an act. Even when identity and authentication have indicated who someone is, authorization is needed to establish what actions are permitted.

Confidential Data: Data protected as confidential by law, contracts, or third-party agreement, and by the University for confidential treatment. Unauthorized disclosure, alteration, or destruction of this data type could cause a significant level of risk to the University or its affiliates.

Designated Campus Colleagues (DCCs): Affiliates, associates, volunteers, and interns who contribute their time, services, and expertise to help the University accomplish its missions of teaching, research, and service.

Regulated Data: Data controlled by federal, state, local, and/or industry regulations. These data are affected by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information.

Unit: Any university college, department, school, program, research center, business service center or other operating unit.

University: The University of Arizona.

University Resource: Data in any form and recorded in any matter and computer-related resources operated, owned or leased by the university, including but not limited to:

- Networks and network appliances
• Computers (servers, workstations and laptops)
• Printers
• Software and applications
• Thumbdrives, paper, etc.
• Any other computer-related equipment, device or hardware used to access, store, transmit or interface with another university resource

**University Employee** – An individual who is employed by the university under classifications "faculty," "classified staff," or "academic professional," "administrative professional," “administrative personnel,” “administrator,” "service professional" or “student employee” as those terms are defined in Arizona Board of Regents' Policy Manual, the University Handbook for Appointed Personnel, Classified Staff Employee Handbook or Student Employee Manual.

**University-Related Persons** – University students and applicants for admission, university employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University, and third-party contractors engaged by the University and their agents and employees.

### III. REQUIREMENTS

#### A. PRE-HIRING

- When posting a job announcement, indicate whether the advertised position will have access to mission-critical university resources, and that the applicant will be required to have a criminal background check, including fingerprinting.
- Ensure reference check inquiries include questions about access to sensitive data, if appropriate.

#### B. POST-HIRING / ONBOARDING

- Prior to start date, conduct fingerprint criminal background checks in accordance with university policy. Check with Human Resources if employee will be engaged in activities that include access to Confidential or Regulated Data to see if more rigorous screening is required.
- Ensure that employee has agreed to the University's Acceptable Use Policy and Computer and Network Access Agreement Policy.
- Provide New Employee Checklist with links to all required new employee training, including All-Employee Security Awareness Training.
- If university employee or university-related person will have access to Confidential or Regulated Data or mission-critical university resources as part of job responsibilities, ensure that all required compliance training is completed within first month after start date.
C. **SUPERVISION**

- Inform university employees and university-related persons of changes in university or unit information security policies or protocols.
- Ensure that employees remain current on all security and compliance training, especially in roles where Regulated Data is in scope.
- Ensure that ongoing information security information (e.g., newsletters, policy updates) is shared with all unit employees.
- Review unit job announcements, promotions, change of job responsibilities, and employee transfers to ensure that access to university data and resources is appropriate to each position.
- Review access privileges at least annually. Employees should only have access to university resources and data for which they have a business need.
- Assess performance and competencies specifically related to proper handling of university resources and data annually.
- Ensure that supervisors are aware of their information security and privacy obligations.

D. **INTERNAL PROMOTION OR TRANSFER**

- Review and change access privileges based on job-related and need-to-know criteria.
- Ensure that newly hired or transferred employees receive appropriate security and compliance training appropriate for their new job.
- If new post requires it, conduct fingerprint criminal background check if this was not performed when employee was first on-boarded.

E. **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 reassigned or reformat it 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 university resources, Confidential or Regulated Data.

F. **IN VOLUNTARY SEPARATION (E.G., LAYOFFS, DISCHARGE/DISMISSAL, NON-RENEWALS)**

ALL GUIDELINES IN VOLUNTARY SEPARATION (SECTION E) 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.

IV. **REVISION HISTORY**

2. Revision 002: 12/6/2017