The University of Arizona (University) is committed to preserving the confidentiality, integrity and availability of its information assets, while preserving and nurturing information-sharing requirements of its academic culture. An important step in protecting the University's information assets is ensuring that all UA personnel understand their roles and responsibilities in protecting University data.

I. **Scope**

All University Employees (including student employees) and Designated Campus Colleagues (DCCs) who have access to the University’s information assets are required to complete information security awareness training.

Security awareness training will include:

- General information security awareness
- Security best practices
- University policy and security resource information
- Employee roles and responsibilities
- University data classification and handling requirements
- Security threat and trend information
- Role-based training, as appropriate

II. **Definitions**

1. **AVAILABILITY**: assurance that authorized users have access to information assets when required
2. **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.
3. **CONFIDENTIALITY**: assurance that information assets are not disclosed without authorization
4. **DESIGNATED CAMPUS COLLEAGUES (DCC)**: Affiliates, associates, volunteers, and interns who contribute their time, services, and expertise to help the University accomplish its missions of teaching, research, and service.
5. **INFORMATION ASSET**: any data, system, computer, network device, document, or any other component of the University infrastructure which stores, processes, or transmits institutional data
6. **INTEGRITY**: assurance that information assets are not accidentally or maliciously altered or destroyed
7. **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.

8. **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.

## III. Authority, Responsibilities and Duties

1. All **University Employees** and **DCCs** are required to complete the All-Employee Security Awareness Training class within the first 30 days of hire or prior to receiving access to **University information assets**.

2. Additional security awareness training may be required for all **University Employees** and **DCCs** at other intervals when deemed necessary by the Chief Information Security Officer.

3. Additional role-based security awareness training will be required for employees whose job responsibilities require elevated privileges, including access to **regulated** or **confidential data** and **information assets**.

4. **University Employees** and **DCCs** who transmit, store, or handle **regulated data** must complete security and compliance training within the timeframe required under legal or contractual obligations.

5. Supervisors, Managers, Deans and Directors are required to ensure that each **University Employee** under his/her supervision has completed security awareness training.

6. Supervisors, Managers, Deans and Directors will ensure that all employees and **DCCs** under their supervision who require elevated privileges, including access to **regulated** or **confidential data** and **information assets**, receive additional role-based security awareness training, as deemed appropriate with their level of expertise, roles and responsibilities.

## IV. Recourse for Non-Compliance

**University Employees** and **DCCs** who have not completed all-employee security awareness training within a reasonable period (no longer than 60 days after onboarding) may lose access to **University information assets**.

**University Employees** and **DCCs** who fail to comply with this standard may be subject to disciplinary action, as described in the **University's Information Security Policy (IS-100)**.

## V. Revision History

1. Revision 001: November 16, 2016
2. Revision 001b: November 21, 2017