Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
January, 2020
Policy Number:
ISO-1700
Responsible Unit:
Information Security Office
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Electronic Privacy Policy for the University of Arizona. The University provides information and services to students, employees, and the public through its Information Technologies to supplement services provided on campus.

This policy sets forth the obligations of the University with respect to informing these constituencies about the University privacy practices and the collection, use, and dissemination of information through electronic means.

Scope

This policy applies to all personal data and information collected, transferred, or maintained by or on behalf of the University in an electronic format. All University-Related Persons with responsibility for the collection, processing, maintenance, or transfer of any such personal data or information are responsible for adhering to this policy.

Definitions

CISO: The senior-level University employee with the title of Chief Information Security Officer.

ISO: The University Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

Unit: A college, department, school, program, research center, business service center, or other operating Unit of the University.

Unit Privacy Notice has the meaning given in the policy, below.

University Information Technologies: all electronic information systems, devices, networks, and other technologies owned or controlled by or on behalf of the University that collect, transmit, display, process, store, or otherwise handle personal information of individuals.

University Privacy Statement has the meaning given in the policy, below.

University-Related Persons: University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), retirees, alumni, 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.

Policy

A. All Classifications of University Information

1. **University Privacy Statement**.

    a. The University must publish a privacy statement (the "**University Privacy Statement** [2]") that is generally applicable to the collection and submission of personal information and data through the University Information Technologies. University Information Technologies is defined above and includes, but is not limited to, websites owned or controlled by the University (e.g., domains ending in arizona.edu), applications (including mobile applications) published by the University, email and messaging systems maintained by the University, electronic payment processing performed by the University, and other electronic services offered by the University.
    b. The University Privacy Statement [3] must contain the information required by Arizona law (A.R.S. § 18-202 [4]) about privacy, confidentiality, and related policies for individuals who use University official websites and other aspects of its Information Technologies.
    c. ISO (or other unit subsequently designated by the Senior Vice President for Academic Affairs and Provost) is responsible for publishing and updating the University Privacy Statement [3]. ISO should consult with relevant stakeholders on a periodic basis to ensure that the University Privacy Statement [3] is an accurate reflection of the University privacy practices and policies, as well as contains all information required by applicable laws and regulations. Where appropriate or necessary to comply with law, the University Privacy Statement [3] may be supplemented by additional provisions that apply in a more limited manner.
    d. Each responsible Unit will provide a visible and accessible link to the University Privacy

Statement [3] on any electronic or digital user interface that collects user information, including but not limited to all websites, intranet sites, and mobile applications. This includes websites with a top-level domain ending in “arizona.edu,” as well as all other websites owned and/or controlled by the University.

e. In addition to the public display of the University Privacy Statement [3], each student, employee, designated campus colleague, and other individual who accesses University Information Technologies through a University-provided NetID is required to read and acknowledge the University Privacy Statement [3] both as a condition of obtaining a NetID and again annually, at a minimum.

2. **College-, Department-, and Unit-Level Privacy Notices**.

   a. Units that maintain their own webpages, applications, or other electronic services that collect, use, or disseminate personal information are encouraged to provide additional information on their privacy practices and policies through unit-specific privacy notices (“**Unit Privacy Notices**”). Unit Privacy Notices should be posted on the relevant webpages and other electronic or digital user interfaces (such as mobile applications) of the Unit and include a link to the University Privacy Statement [3] alongside the Unit Privacy Notice.
   b. Unit Privacy Notices should contain information that is additional to, and that does not conflict with, the University Privacy Statement. Where a Unit’s privacy practices will conflict with the University Privacy Statement, the Unit must seek advance approval of an exception for its Unit Privacy Notice from the Chief Information Security Officer in accordance with the exception procedures issued by ISO.

3. **External Connections and Links**.

   a. University websites may contain links to external websites. Through the existence of these links, the University does not intend to, and does not, endorse or take any responsibility for the privacy practices or policies of external websites.

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

ISO must initiate mechanisms for tracking compliance with this policy and must produce reports representing these measures to support University decision making.

Recourse for Noncompliance

ISO is authorized to limit network access for individuals or Units not in compliance with this policy, the University Privacy Statement, or any supplemental provisions. In cases where University resources are actively threatened, the CISO should act in the best interest of the University by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the CISO is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, the University may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

In cases where employees, DCCs, or other University-Related Persons violate this policy, the University Privacy Statement, or any supplemental provisions, the University may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

Exceptions

Any requests for exceptions must be submitted to the CISO for review and approval pursuant to the exception procedures published by ISO (or other unit subsequently designated by the Senior Vice President for Academic Affairs and Provost).

Frequency of Policy Review

The CISO must review this policy and the University Privacy Statement annually, at minimum. This policy is subject to revision based upon findings of these reviews.

Responsibilities

University-Related Persons

All University-Related Persons who collect, process, maintain, or transfer personal data or information collected or maintained by or on behalf of the University are responsible for being familiar with, and treating all such information and data in compliance with, the University Privacy Statement and any related Unit Privacy Notices that may apply.

University Compliance Personnel

Compliance personnel with designated responsibility for interpreting the University Privacy Statement (e.g., the HIPAA Privacy Office, the University Registrar, the CISO, the ISO, and the University Compliance Office) are authorized to make determinations regarding violations of this policy. Information regarding designated compliance personnel and reporting avenues is available at privacy.arizona.edu [5].

Information Security Office

ISO (or other unit subsequently designated by the Senior Vice President for Academic Affairs and Provost) must:

- publish and update the University Privacy Statement, in consultation with relevant University stakeholders; and
- delegate individual responsibilities and authorities specified in this policy or associated standards and procedures, as necessary.

Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers

All Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers must take appropriate actions to comply with information technology and security policies, including the University Privacy Statement and any Unit Privacy Notices. These individuals have ultimate responsibility for University resources, for the support and implementation of this policy and related privacy practices within their respective units, and, when requested, for reporting on policy compliance to ISO. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Related Information*

- ISO Website [6]
- Arizona Board of Regents Policy 6-912. Access to or Disclosure of Personnel Records or Information [7]
- Arizona Revised Statutes § 18-202 [4]
- University of Arizona Privacy website [5]
- University of Arizona Privacy Statement [2]
- University of Arizona Privacy Statement - GDPR Supplement [8]
- HIPAA Privacy Program [9]
- FERPA Information from the Office of the Registrar [10]
- Additional information is available on the UA Information Security Office website [11]

Revision History*

03/16/2023: Grammatical revisions.

01/24/2020: Non-substantive revisions.

03/19/2019: Replaces Interim policy.

Links
[1] mailto:security@arizona.edu [2] https://privacy.arizona.edu/privacy-statement [3] http://privacy.arizona.edu/privacy-statement [4] https://www.azleg.gov/ars/18/00202.htm [5] https://privacy.arizona.edu [6] https://security.arizona.edu/content/policy-and-guidance [7] https://public.powerdms.com/ABOR/documents/1499363 [8] https://privacy.arizona.edu/privacy-statement-supplement [9] https://rgw.arizona.edu/compliance/hipaa-privacy-program [10] https://www.registrar.arizona.edu/personal-information/family-educational-rights-and-privacy-act-1974-ferpa [11] http://security.arizona.edu/