

## Policy Contents

- [Purpose and Summary](#)
- [Scope](#)
- [Definitions](#)
- [Policy](#)
- [Compliance and Responsibilities](#)
- [Related Information\\*](#)
- [Revision History\\*](#)

## Policy Information

**Effective Date:**

May 7, 2019

**Last Revised Date:**

May, 2019

**Policy Number:**

ISO-1400

**Responsible Unit:**

Information Security Office

**Phone:**

(520) 621-6700

**Email:**[security@arizona.edu](mailto:security@arizona.edu) [1]

## Purpose and Summary

This document establishes the Secure Facility Access Control Policy for the University of Arizona. This policy defines information security requirements for physical security measures to safeguard against unauthorized physical intrusion to secure facilities.

## Scope

This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of the University. All University-Related Persons with access to University Information or computers and systems operated or maintained on behalf of the University are responsible for adhering to this policy.

# Definitions

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

**Information Owner:** The individual(s) or Unit with operational authority for specified University Information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This individual or Unit is responsible for making risk tolerance decisions related to such Information on behalf of the University and is organizationally responsible for any loss associated with a realized information security risk scenario.

**Information Resources:** University Information and related resources, such as equipment, devices, software, and other information technology.

**Information Security Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Information System or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**Information System:** A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

**Information System Owner:** The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

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

**Secure Facility:** Any University-owned facility (e.g., building, equipment, designated space within a building, infrastructure) that is not open to the public and has restricted access procedures established for purposes of maintaining the security or confidentiality of the information or other resources contained within it.

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

**University Information:** Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.

**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.

**User:** Individual or group that interacts with a system or benefits from a system during its

utilization.

## **Policy**

Information Owners and Information System Owners must ensure the protection of Secure Facilities containing University Information Resources in a manner proportional to the information security risk.

Information Owners and Information System Owners must develop or adopt physical access procedures for Secure Facilities covered by the preceding paragraph. These procedures must meet the following minimum requirements:

- Procedures must be documented and must provide ISO with the ability to monitor compliance.
- Physical access to Secure Facilities must be limited to authorized individuals who require access for the fulfillment of their job responsibilities and visitors who are always escorted by an authorized University-Related Person.
- Physical access and monitoring logs, where utilized, must be retained, stored, and disposed of in compliance with University retention requirements and applicable laws and regulations.
- Physical access authorizations must be reviewed during initiation, have documented approval, utilize change management when any aspect of authorized approval requires a change, undergo an annual review, and be revoked in a timely manner when access is no longer required.
- Physical access devices (e.g., keys, key cards, etc.) must be appropriately protected and only enable access to areas the device User is authorized to enter.
- When an issuer cannot revoke authorization for a physical device (e.g., keys, etc.), the device must be returned to the issuer when it is no longer needed. Lost, stolen, or unreturned devices must be reported to ISO immediately.
- Physical access breaches are Information Security Incidents and must be reported as such to ISO.

## **Compliance and Responsibilities**

### **Compliance**

#### **Tracking, Measuring, and Reporting**

ISO shall initiate mechanisms for tracking compliance with this policy and shall 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 information security policies (including this one) and related procedures. In cases where University resources are actively threatened, the CISO shall 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.

## **Exceptions**

Requests for exceptions to information security policies (including this one) may be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the CISO for review and approval pursuant to the exception procedures published by the CISO.

## **Frequency of Policy Review**

The CISO shall review information security policies and procedures annually, at minimum. This policy is subject to revision based upon findings of these reviews.

## **Responsibilities**

### **University-Related Persons**

All University-Related Persons are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.

### **Information Owners and Information System Owners**

Information Owners and Information System Owners are responsible for implementing processes and procedures designed to provide assurance of compliance with the minimum standards, as defined by ISO, and for enabling and participating in validation efforts, as appropriate.

### **Chief Information Security Officer**

ISO shall, at the direction of the CISO:

- identify solutions that enable consistency in compliance and aggregate and report on available compliance metrics;
- develop, establish, maintain, and enforce information security policy and relevant standards and processes;
- provide oversight of information security governance processes;
- educate the University community about individual and organizational information security responsibilities;
- measure and report on the effectiveness of University information security efforts; 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 shall take appropriate actions to comply with information technology and security policies. These individuals have ultimate responsibility for University resources, for the support and implementation of this policy 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](#) [2]

[University Retention Schedule Policy](#) [3]

[University Physical and Electronic Access Control Policy](#) [4]

[Information Security Incident Reporting and Response Policy](#) [5]

[Information Security Incident Response Plan](#) [6]

## **Revision History\***

Replaces Interim policy of 3/19/19

---

**Source URL:** <http://policy.arizona.edu/information-technology/secure-facility-access-control-policy>

### **Links**

[1] <mailto:security@arizona.edu>

[2] <https://security.arizona.edu/content/policy-and-guidance>

[3] <https://rmaa.arizona.edu/retention>

[4] <http://policy.arizona.edu/facilities-and-safety/physical-and-electronic-access-control-policy>

[5] <https://policy.arizona.edu/information-technology/information-security-incident-reporting-and-response-policy>

[6] [https://confluence.arizona.edu/download/attachments/39782340/Incident%20Response%20Plan\\_v4.pdf?api=v2](https://confluence.arizona.edu/download/attachments/39782340/Incident%20Response%20Plan_v4.pdf?api=v2)