Get Protected

Take Action Today!

Virus Protection

Encryption

Arizona State University
Information Technology
Physical (Environmental) Security
Audit Report

March 3, 2016

Mobile Devices

Security Training

ASU Top 5

Contact Us

REPORT A SECURITY EVENT

PHISHING INFORMATION

ALERTS ANNOUNCEMENTS

This page left blank intentionally.

Arizona State University
Information Technology Physical (Environmental) Security
Audit Report
March 3, 2016

Summary

The Information Technology Physical (Environmental) Security audit was included on the Arizona State University (ASU) FY 2016 annual audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and university senior leadership. This audit was conducted to review the adequacy of physical measures, policies and procedures protecting university electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

Background: ASU provides centrally managed information technology services and resources to employees, students, and other affiliates for activities related to its mission of teaching and learning, research, and service. The University limits access to only those individuals and entities that are actively involved in supporting the institution's mission and goals.

ASU’s University Technology Office (UTO) maintains facilities that contain critical servers, storage, and data backup systems supporting the data processing and internet connectivity needs of ASU. An important step in protecting electronic information is to implement appropriate physical safeguards for these facilities and related information systems and equipment. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of ASU, violate individual privacy rights, and possibly constitute a criminal act.

UTO has identified physical areas that must be protected from unauthorized physical access. Such areas include data centers and other locations on the campus where information assets that process and contain protected data necessary to support business operations are stored. These limited-access areas must be protected from unauthorized physical access while ensuring that authorized users have appropriate access.

Audit Objectives: The objectives of this audit were to review the adequacy of physical measures, policies, procedures and other controls protecting university electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

Scope: Using ISO (International Organization for Standardization) 27002 as a baseline for compliance, the audit focused on a review and evaluation of the administrative and operational controls over the campus data centers and information resources residing within, and equipment related to and supporting, the campus data centers.

Methodology: Our audit objectives were accomplished through:

- Conducting facility walkthroughs, observing operations, and reviewing documentation and equipment configurations
- Reviewing data center physical controls, doorways, card key locks and access systems, monitoring functions, and the physical layout of the main data centers
- Reviewing controls over environmental threats such as moisture and flooding, fire and heat, and power outages
- Discussing Information Technology Physical Security and related procedures and controls with representatives from UTO, including the Assistant Vice President and Chief Information Security Officer, Assistant Vice President of UTO Operations, Senior Director of UTO Operations, Director of Data Center Operations, Director of Policy and Compliance, Systems Support Specialist OPS Facilities, Telecommunication Engineer OPS Facilities and with data center representatives, including the Director of Global Security Operations
- Reviewing applicable ASU web-based policies and procedures
- UTO completing a written questionnaire prepared by University Audit
- Selecting a random sample of twelve individuals who had authorized access to the data centers during 2015. For each individual, the hiring records were checked for background screening requirements including:
    a. Fingerprint checks
    b. Resumes
    c. Character references
    d. Confirmation of claimed academic and professional qualifications.

Conclusion: Physical measures, policies, procedures and controls protecting university electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion are adequate. The main data centers are physically sound, of solid construction, unobtrusive, and give minimum indication of their purpose, with no obvious signs, outside or inside the buildings, identifying the presence of information processing activities. UTO personnel were responsive to University Audit inquiries and provided data and other requested information in a prompt and courteous manner. University Audit found UTO personnel to be knowledgeable and dedicated employees who are open to opportunities for improvement.

The main data center resides in the basement of a multi-story building, and in the concrete ceiling of the center there is a square opening approximately one–and-a-half feet long on each side. Also, there is a round hole in the concrete ceiling, approximately two inches in diameter. The potential exists that if a flood occurs above the basement, the center could receive severe water-related damage. To mitigate water-related threats from above the ceiling, ASU should investigate the best approach to seal these openings.

Underground systems of tunnels across the ASU campuses contain network cabling infrastructure that provides computing services across the campuses. These tunnels also contain pipes (including water piping for the chiller system) and ducts that heat, cool, and provide electricity and telephone services. If this network equipment or cabling is damaged, especially in critical tunnels, by malicious intent or otherwise, certain ASU computer systems would be non-operational during the time repair work is performed. For example, there are chilled water lines that run along the top of the tunnels. If these chilled water lines are damaged, there could be major flooding in the tunnels. Repair work in the tunnels takes lengthy periods of time because asbestos issues in the tunnels require significant time to address. To help prevent unauthorized access to the tunnels, ASU could lock down the tunnel system with all the entry points to the tunnels alarmed and monitored.

The main data center serving ASU has two entrances. When an authorized cardholder inserts his card in the reader at an entrance, the system does not restrict access into the main data center to only the authorized person. A device, or “mantrap,” allowing access to only one individual at each entrance would permit only the authorized ISAAC (Integrated System for ASU Access Control) cardholder to enter the main data center. UTO is investigating installing these devices in the main data center, and working to improve other procedures to ensure that data centers are protected by appropriate entry controls to ensure only authorized personnel are allowed access.

UTO is currently in the process of relocating servers that are in various ASU departments to the data centers. Servers located in ASU departments require cooling through a chilled water system on a twenty-four hour, seven day a week basis. UTO efforts to move the servers to the Data Centers is reducing power consumption, and therefore reducing the cost to ASU for utilities, because utilities can now be provided on an 8AM to 6PM workday schedule in affected departments.

The control standards we considered during this audit and the status of the related control environment are provided in the following table.

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	**Control Environment**	**Finding No.**	**Page No.**
Reliability and Integrity of Financial and Operational Information	Not Applicable	NA	NA
Effectiveness and Efficiency of Operations			
• Delivery and loading areas are controlled and isolated from information processing facilities.	Reasonable to Strong Controls in Place	NA	NA
• Equipment is correctly maintained to ensure its continued availability and integrity.	Reasonable to Strong Controls in Place	NA	NA
• Equipment, information or software is not taken off-site without prior authorization.	Reasonable to Strong Controls in Place	NA	NA
• All items of equipment containing storage media are verified to ensure that any sensitive data is removed prior to disposal or re-use.	Reasonable to Strong Controls in Place	NA	NA
Safeguarding of Assets			
• Security perimeters are defined and used to protect facilities that contain sensitive or critical information.	Reasonable to Strong Controls in Place	NA	NA
• Secure areas are protected by appropriate entry controls to ensure only authorized personnel are allowed access.	Opportunity for Improvement	1	6
• Physical security for offices, rooms and facilities is designed and applied.	Reasonable to Strong Controls in Place	NA	NA
• Physical protection against natural disasters, malicious attack or accidents is designed and applied.	Opportunity for Improvement	2	8
• Equipment is sited and protected to reduce risks from environmental threats and opportunities for unauthorized access.	Reasonable to Strong Controls in Place	NA	NA
• Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	Reasonable to Strong Controls in Place	NA	NA
• Power and telecommunications cabling carrying data is protected from interception, interference or damage.	Reasonable to Strong Controls in Place	NA	NA
• Security is applied to off-site assets.	Reasonable to Strong Controls in Place	NA	NA

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	**Control Environment**	**Finding No.**	**Page No.**
Compliance with Laws and Regulations			
• ASU Information Technology Physical Security practices are being administered in compliance with University policies and procedures.	Reasonable to Strong Controls in Place	NA	NA

We appreciate the assistance of UTO representatives during the audit.

Gordon Murphy

Gordon Murphy, CPA, CFE, MAEd
Internal Auditor Senior

Audit Results, Recommendations, and Responses

1. Certain control procedures over access into Data Centers should be reviewed, updated, and implemented by UTO.

Condition: University Audit noted there are opportunities to improve procedures for access and termination of access into the data centers.

Criteria: ISO 27002 Article 11.1.2 states that “Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.”

Cause: UTO can work to update their practices that ensure only authorized employees, vendors and contractors are allowed access into the data centers, and update procedures for prompt termination of access.

Effect: Streamlining control procedures over access into data centers can help prevent unauthorized access, damage, interruption, modification, deletion, or disclosure of ASU’s information assets, while ensuring that authorized users have appropriate access.

Recommendation: Regarding ASU employees currently authorized to enter the data centers, UTO can reduce the number of these employees by restricting access to a primary and secondary ISAAC cardholder for each ASU department that needs access to the data centers. If other individuals within a department want access, the department would have to obtain additional approval from UTO. Decreasing the number of personnel accessing the data centers reduces the risk of damage, interruption, modification, deletion, or disclosure of ASU’s information assets. Also, it would allow UTO to perform more efficiently its reviews of verifying authorization for employees who have access to the data centers, as the reviews would be done for fewer individuals. Also, it would help UTO be more effective in obtaining all hiring records, including fingerprint checks and character references, for all employees requesting access authorization.

Regarding the times when access authorization into the data centers for any ASU employee is required to be terminated, UTO can work with ASU Human Resources and University Business Services to create and implement procedures for immediate termination of access. Related procedures also would be implemented for representatives of outside contractors and vendors.

For contractors and vendors who enter the data centers, ASU could require each contractor/ vendor to provide ASU a written certification that all representatives of the contractor/ vendor with access rights have completed appropriate background checks, including fingerprinting, to certify that their representatives are cleared to enter the data centers. The certification would list the names of the individuals who have been cleared to enter the data centers.

Management Response:

UTO concurs with this recommendation and will take the following steps to improve data center controls:

1. UTO has reduced the number of persons with datacenter access, restricting access to primary or essential staff requiring access in order to fulfill support responsibilities. Status: Complete.
2. UTO will investigate solutions for removing access from ISAAC system in a more automated fashion upon changes to affiliate active status and propose solution. Status: To be completed by 09/30/2016.
3. UTO has confirmed vendor datacenter access is appropriate. A follow-up is in progress to confirm the vendor representatives with datacenter access have satisfactorily completed the fingerprinting with background check. Status: To be completed by 06/30/2016.

2. There are openings in the roof of the main data center that should be sealed, and the tunnel systems containing network cabling infrastructure should be locked down.

Condition: University Audit noted that in the concrete ceiling of the main data center there is a square opening approximately one and a half feet long on each side, and a round hole approximately two inches in diameter. For the underground system of tunnels across ASU campuses, not all the tunnel system access points are alarmed or monitored for unauthorized access events.

Criteria: ISO 27002 Article 11.1.4 states that "Physical protection against natural disasters, malicious attack or accidents should be designed and applied."

Cause: UTO can collaborate on the best methods to seal the openings in the concrete ceiling of the main data center, and alarm necessary locations within the tunnels and all tunnel access points.

Effect: Sealing the openings in the concrete ceiling helps prevent both deliberate and accidental threats, such as unauthorized entry and flooding, to ASU information assets. Alarming and monitoring the tunnels, including all tunnel access points, to prevent unauthorized access into the tunnels helps stop the multitude of ways in which threats could take advantage of vulnerabilities to harm ASU.

Recommendation: The openings in the concrete ceilings should be appropriately sealed. The tunnel system should be locked down with all the entry points to the tunnels alarmed and monitored for effective access control.

Management Response:

UTO concurs with this recommendation and will take the following steps:

1. Investigation is underway to implement an appropriate solution to seal openings in the data center ceiling that could pose an environmental risk to the data center, i.e. water damage due to flooding on upper floors. Status: Investigation to be completed by 12/31/2016.
2. Assess the risks associated with tunnel systems facilitating critical network equipment and cabling that tie into the datacenter and provide recommendations to executive leadership for improvement. Status: To be completed by 12/31/2016.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Mark S. Searle, Executive Vice President and University Provost
José A. Cárdenas, Senior Vice President and General Counsel
Joanne Wamsley, Vice President of Finance
Nichol Luoma, Interim Associate Vice President
Gordon Wishon, Chief Information Officer, University Technology Office
Tina Thorstenson, Assistant Vice President and Chief Information Security Officer
Jay Steed, Assistant Vice President, University Technology Office Operations
Shawn Bryan, Senior Director, University Technology Office Operations
Terry Hinton, Director, Data Center Operations, University Technology Office
Susan Moore, Director of Policy and Compliance, University Technology Office