# PROCEDURE MANUAL

| | | | | |
|---|---|---|---|---|
| ARIZONA WESTERN COLLEGE | | | **PROCEDURE 223.017** | |
| | | | **Page 1 of 3** | |
| | | | **Last Revision Date:** | 04/13/2026 |
| | | | **Effective Date:** | 05/06-2025 |
| | | | **Last Review Date**: | 04/13/2026 |
| **Section:** | Technology | **Subject:** | Cyber Security Incident Reporting | |

**** Notify the IT Service Desk immediately of any real or suspected cyber security incident by calling our support line at (928) 317-5892. ****

## PURPOSE

The purpose is to define the process Arizona Western College's (AWC) Information Technology Services & Support (ITSS) uses to report and escalate cyber security incidents that threaten the confidentiality, integrity, and availability of college information assets, information systems, and the networks that deliver the information. This procedure outlines the cyber security incident reporting procedures required to assist in the deployment of trained information technology staff, and/or emergency response teams, formed with the purpose of managing the cyber security incidents at the College. This effort is to improve the response time to cyber incidents, to provide consistent responses, and to improve cyber security incident reporting. The handling of these cyber security incidents is covered in the Information Security Incident Management Plan 999.012 (found on MyAWC).

## SCOPE

This procedure applies to all users of AWC technology assets including employees, students, volunteers, and contractors.

## PROCEDURE

ITSS is responsible for implementing a cyber security incident response related to all systems and services for which it is responsible. Nothing in this Cyber Security Incident Response procedure should be taken to conflict with college policies and procedures which include but are not limited to the following:

- College Security
- Acceptable Technology Use procedure 223.001
- Federal or State of Arizona mandates/Laws

These procedures specifically exclude the following:

- Non-electronic information including paper mail.
- Physical security or emergency response.

| ARIZONA WESTERN COLLEGE | | | PROCEDURE 223.017 | |
|---|---|---|---|---|
| | | | Page 2 of 3 | |
| | | | **Last Revision Date:** | 04/13/2026 |
| | | | **Effective Date:** | 05/06-2025 |
| | | | **Last Review Date**: | 04/13/2026 |
| **Section:** | Technology | **Subject:** | Cyber Security Incident Reporting | |

Contingency planning, business continuity and disaster recovery are handled by different procedures. An event may initially be declared a "Critical Incident" and subsequently declared to be a "Disaster." In this case, a critical incident response team would implement the Disaster Recovery process outlined in 999. 011.Notification **(How and When)**

Please notify the IT Service Desk immediately of any real or suspected cyber security incident by calling our support line at (928) 317-5892.

- The IT Service Desk will immediately notify the Chief Information Officer (CIO).
- The Chief Information Officer will activate the Information Security Incident Management Plan outlined in Procedure 999.012.
- Individuals (faculty, staff or student), who report a breach of cyber security incident will receive appropriate feedback and updates regarding the incident from one or more of the following areas: college's senior administration; human resources department; campus security department; department / division manager; IT Leadership.
- Individuals reporting a breach of security incident will be assured of confidentiality, and if necessary, appropriate protection.
- Criminal activity or immediate risks to the safety of individuals should be reported to the College Public Safety Office or 911 immediately.

When faced with a potential IT-related security situation, faculty, staff, and students should do the following:

- If the cyber security incident involves a compromised computer system, do not alter the state of the computer system. The computer system should remain powered on, and all currently running computer programs should be left as is. Do not power down the computer or restart the computer.
- Immediately disconnect the computer/laptop or other IT connected device from the campus network by removing the patch cable from the back of the computer. If the computer, laptop or device is utilizing wireless network connectivity, the system's wireless network hardware should be disabled via the Network Settings in the Control Panel or via the appropriate system configuration tool.

## HISTORY

| IT Reviewer Name | Update Date | AWC Reviewer | Approval Date |
|---|---|---|---|
| Scott Estes, Tyler Vodehnal, Mercedes Soto | 2/5/2025 | Dr. Daniel Corr | 05/06/2025 |
| Scott Estes, Tyler Vodehnal | 02/04/2026 | Dr. Reetika Dhawan | 04/13/2026 |