Augusta University
Policy Library

Incident Response Policy

Policy Manager: Chief Information Security Officer

1.0 POLICY STATEMENT

It is the policy of Augusta University (AU) to respond to, mitigate, and recover from cybersecurity incidents as detailed in the Cybersecurity Incident Response Plan (CIRP). This policy ensures that when the Cybersecurity Incident Response Team (CSIRT) is initiated, it has all the necessary information and cooperation from AU entities to formulate a successful response to specific security incidents.

The purpose of this policy is to give AU a clear, predefined, and repeatable method to prepare for, detect, contain, and recover from cyber incidents, as defined in the CIRP. IT Services Teams and Business units are expected to properly assist during the response to an information security incident by the CSIRT, as defined in the CIRP. The CSIRT, IT Services Teams, and Business Units, as applicable, are expected to assist the Director of Cybersecurity Operations and the Chief Information Security Offer in developing and maintaining a CIRP annually, as required by the USG.

2.0 AFFECTED STAKEHOLDERS

This section identifies the groups and individuals who are expected to follow this policy*:*

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☒ Visitors
☐ Other:

3.0 DEFINITIONS

This section defines key terms used in this policy to support consistent understanding and application.

Refer to the *Cybersecurity Charter Policy, Appendix B* for all applicable definitions. This can be found online in the Augusta University Policy Library.

4.0 SCOPE

This section describes where this policy applies, including the types of data formats, systems, and environments covered.

Abstract: This policy applies to all information systems, networks, applications, data owned, operated, or managed by AU, including systems hosted by third-party service providers.

This policy governs the identification, reporting, analysis, containment, eradication, and recovery of information security incidents that may affect the confidentiality, integrity, or availability of AU systems and data.

5.0 ROLES AND RESPONSIBILITIES

This section defines the roles and responsibilities for executing and overseeing AU's cybersecurity incident response activities.

5.1 Chief Information Security Officer (CISO)

5.1.1 Is responsible for developing, implementing, executing and maintaining the CIRP.

5.1.2 The procedures used by the CSIRT members and other supporting staff regarding security incidents are under the authority and control of the Incident Response Leader.

5.2 Cybersecurity Incident Response Team (CSIRT)

5.2.1 is responsible for investigating cybersecurity incidents and for detecting, analyzing, containing, eradicating, and recovering from incidents.

6.0 REQUIREMENTS

This section defines the minimum requirements and expectations for establishing, maintaining, and executing AU's incident response capabilities.

Abstract: Immediate reporting of suspected security incidents is expected and enables rapid response. The CSIRT is authorized to obtain access to systems and devices as required, with users and administrators required to provide support response actions such as account controls and security updates, ensuring effective incident containment and recovery.

6.1 Reporting

6.1.1 All users of information technology owned or managed by AU must immediately, upon detection, report suspected information security incidents (including but not limited to providing AU login credentials to a phishing email, receiving and/or accepting multifactor authentication requests (DUO) that were not initiated by the employee, lost/stolen devices used for AU business, suspected malicious software (malware) on an AU device) to the CSIRT through:

6.1.1.1 A phone call to the 24/7 IT Help Desk (706-721-4000) or to 72Cyber (706-722 9237)

6.1.1.2 An email to the 72cyber@augusta.edu mailbox

6.1 Urgent Access to Devices or Information

6.2.1 In limited cases, CSIRT members may need immediate physical and/or logical access to areas and/or systems/data within AU.

6.2.2 All device users and administrators will facilitate the needs if access is requested during a cybersecurity incident.

6.2.3 Appropriate personnel may be requested by the CSIRT to conduct actions which fall under their purview, such as, but not limited to, emergency password resets, emergency account suspensions, or updating/setting security controls.

7.0 COMPLIANCE

This section explains how compliance with this policy is managed, including how to request documented exceptions and the potential consequences of non-compliance.

Abstract:

- If you cannot comply, you shall request a documented exception through the ETP process.
- Approved exceptions shall be time-limited and reviewed periodically.
- Non-compliance may result in disciplinary action and/or suspension or revocation of system and data access.

Exceptions: If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request approval for an exception through the AU Cyber Defense Governance, Risk and Compliance (GRC) Exception to Policy (ETP) process as referenced in Service Now in Knowledge Base Article KB2300201. All approved exceptions shall have a defined expiration date and shall be reviewed periodically for continued necessity.

Exception conditions: Failure to adhere to the approval conditions outlined in an approved exception to policy may result in revocation of the exception.

Non-compliance: Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment, as well as other administrative action as appropriate. Sanctions may also include suspension, limitation, or revocation of access to AU's computing environment, systems, applications, networks, and data.

8.0 REFERENCES & SUPPORTING DOCUMENTS

This section lists external regulations, frameworks, USG requirements, and AU supporting resources that inform or support this policy.

NIST Cybersecurity Framework (CSF)
NIST SP 800-61, Incident Response Recommendations and Considerations for Cybersecurity Risk Management

USG IT Handbook University System of Georgia (USG) Information Technology (IT) Handbook

Service Now Knowledge Base Article KB2300201
AU Incident Response Plan

9.0 RELATED POLICIES

This section lists internal policies, standards and resources that inform or support this policy.

Acceptable Use of Information Technology Policy
Cybersecurity Charter Policy
Risk Management Policy

All AU Policies can be found online at the Augusta University Policy Library

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/29/2026

President, Augusta University Date: 7/8/2026