Augusta University
Policy Library

Cybersecurity Incident Response Plan Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

The purpose of this policy is to establish the requirement that all business units supported by the Cybersecurity Operations Team are to facilitate the Cybersecurity Incident Response Plan (IRP). This ensures that when the Cybersecurity Incident Response Team (CSIRT) is initiated, it has all the necessary information and cooperation to formulate a successful response should a specific security incident occur.

Scope

This policy applies to all employees and staff of Augusta University (AU), hereinafter referred to collectively as "AU". This policy applies to all duties of AU employees and staff performed within the scope of their employment at any site of the AU. AU is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), and/or other sensitive information (SEI) by implementing security standards within facilities and within areas of a facility that contain or provide access to SEI, PHI, PCI or ePHI.

This policy is in accordance with requirements of the University System of Georgia, USG IT Handbook

This policy addresses the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations (as well as changes made through the Health Information Technology of Economic and Clinical Health Act (HITECH)), Family Educational Rights and Privacy Act (FERPA) and other applicable federal, state, or local laws and regulations that may relate to the protection and security of SEI.

AFFECTED STAKEHOLDERS

Indicate all entities and persons within the Enterprise that are affected by this policy:

☐ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☒ Other: This policy applies to any established and defined business unit or entity within Augusta University

PROCESS & PROCEDURES

The development, implementation, and execution of a Cybersecurity IRP are the primary responsibility of Director of Cybersecurity Operations (DCO). Maintenance of the Cybersecurity IRP is the responsibility of the Chief Information Security Officer (CISO). Business units are expected to properly facilitate the Cybersecurity IRP applicable to the service they are held accountable. The CSIRT, IT Services Teams, and Business Units as applicable, are further expected to work with the DCO and the CISO in the development and maintenance of an Incident Response Plan at a minimum of every 2 years and as needed.

Office of Legal Affairs Use Only
Executive Sponsor: VP for Information Technology
Next Review: 6/2024

Reporting

All users of information technology owned or managed by AU must immediately report suspected information security incidents (including but not limited to virus infections and computers exhibiting behavior consistent with a compromised machine) to the CSIRT through:

- An email and/or phone call to the IT Help Desk or an IT staff member
- An email to the 72CYBER mailbox
- Identification and report by a system-specific Application Analyst
- System generated reports and alerts (SIEM, Antivirus, DLP, etc.)
- Manual reviews of system and device logs

NOTE: *The AU/AUHS Cybersecurity Operations team is responsible for identifying, categorizing, prioritizing, and triaging security events and potential security incidents. They will analyze the security event to determine if any indicators or precursors to a security incident exist or if it is a false positive. The incident's priority will be determined using the Security Incident Prioritization Guidelines.*

If the event is determined to be a security incident or it cannot be ruled out as one, the team member will work with the senior SOC analyst on duty and/or appropriate Subject Matter Expert for further analysis.

Upon confirmation of a security incident, the senior Security Operations Center (SOC) analyst on duty will submit an incident ticket into the AU ticketing system and submit a USG incident ticket into the USG ticketing system, as well as the initial USG cybersecurity incident report within the reporting guidelines.

The CISO will notify the CIO and Enterprise Privacy Officer with an executive summary of the incident following the procedures outlined in the Cybersecurity IRP.

Emergency Access to Devices or Information

In limited cases, authorized individuals may need immediate physical and/or logical access to areas and/or systems within Augusta University. All device users and administrators will facilitate the needs in the event access is requested during an emergency.

Contact Information

The Cybersecurity IRP includes contact information for dedicated team members to be available during non-business hours should an incident occur, and escalation be required. The availability of a CSIRT member is a 24/7 requirement. The Cybersecurity IRP document includes all phone numbers and email addresses for the dedicated team member(s).

Incident Handling

The Cybersecurity IRP defines cybersecurity incident handling strategy to be coordinated with the CSIRT in a cooperative manner with the intended goal of swift security incident mitigation. This step typically includes validating the reported vulnerability or compromise.

Identified Mitigations and Testing

The Cybersecurity IRP includes a defined process for identifying and testing mitigations prior to deployment. These details include both short-term mitigations as well as the remediation process.

Mitigation and Remediation Timelines

The Cybersecurity IRP includes levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported incident.

Policy Compliance

Compliance Measurement

Each business unit must be able to demonstrate they have received and understand the requirements of the Cybersecurity IRP in place.

Exceptions

Any exception to this policy must be approved by the CSIRT in advance and have a written record.

Non-Compliance

Any business unit found to have violated this policy may be subject to delays in service or product release until such a time as the CSIRT has reviewed and developed a response. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur due to deliberate negligence or unwillingness to accommodate the requirements of the CSIRT during an emergency.

Authority

The procedures used by the CSIRT members and other supporting staff with regard to security incidents are under the authority and control of the DCO.

The DCO has the authority to initiate changes in the way electronic traffic flows at AU when emergencies arise, based on approval from the Chief Information Security Officer (CISO).

REFERENCES & SUPPORTING DOCUMENTS

Cybersecurity Incident Response Plan

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/2/2021

President, Augusta University Date: 6/2/2021