Augusta University
Policy Library

Cybersecurity Charter Policy

Policy Manager: Chief Information Security Officer

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: Any individual or entity with access to enterprise information technology.

Section 1.0 Cybersecurity Charter

Introduction:

Augusta University (AU) recognizes the critical importance of cybersecurity in protecting its information and IT assets. As a member of the University System of Georgia (USG), AU aligns its cybersecurity efforts with the USG Cybersecurity program, which provides guidance, training, and coordination to ensure the development of robust cybersecurity processes and technologies across all USG institutions. This document outlines Augusta University's overarching cybersecurity philosophy to help improve shared understanding across the enterprise by emphasizing the motivation behind cybersecurity practices, defining cybersecurity goals, and establishing the scope of roles and responsibilities of different entities throughout the AU Community.

Authorization:

The cybersecurity initiatives at Augusta University are authorized by the Board of Regents (BOR) Policy Manual, Section 10.4. The USG Chief Information Security Officer (CISO) is responsible for developing and maintaining a cybersecurity organization and architecture that supports cybersecurity efforts across all USG institutions. As such, the USG CISO established cybersecurity implementation guidelines that AU, along with other USG institutions and the Georgia Public Library Service (GPLS), must follow when developing their individualized cybersecurity plans. Augusta University acknowledges and complies with this authorization, ensuring that its cybersecurity measures are in line with the USG's overarching cybersecurity framework.

Motivation:

Augusta University and USG recognize that information and IT assets are vital to their operations. It is the collective responsibility of all AU users to safeguard these assets. As such, AU maintains a comprehensive enterprise cybersecurity and compliance program, which includes the protection, monitoring, and maintenance of its information assets. Open communication and information sharing are highly valued, but it is crucial to protect USG information, whether it belongs to AU or is held in trust on behalf of clients and business partners. The misuse, unavailability, destruction, unauthorized disclosure, or modification of these assets can have severe consequences, potentially causing harm to the USG. To mitigate these risks, AU identifies, values, assesses, and protects its information assets according to their importance and the potential impact of their compromise. By prioritizing cybersecurity, AU ensures the continued confidentiality, integrity, and availability of its information resources, contributing to the overall resilience of the USG cybersecurity ecosystem.

Cybersecurity Goals:
Cybersecurity is a risk management discipline used to safeguard information confidentiality, integrity, and availability. It does so by implementing a hierarchical set of policies, standards, and procedures that help users and administrators define and mitigate risks, maintaining a trade-off between information value and cost of risk mitigation. AU's Cybersecurity goals are as follows:

- Establish a comprehensive cybersecurity framework.
  - Develop and implement policies, standards, and procedures that promote an enterprise-wide cybersecurity environment, aligning with best practices and industry standards.
  - Regularly review and update the framework to address emerging threats and technologies.
- Strengthen proactive threat detection and incident response capabilities.
  - Enhance the Security Operations Center's incident response capabilities through advanced technologies, training, and coordination with relevant stakeholders.
  - Establish processes for timely detection, analysis, and response to cybersecurity incidents, minimizing the impact on the university community.
- Foster a culture of cybersecurity awareness and education.
  - Develop and deliver comprehensive cybersecurity awareness and training programs for students, faculty, and staff, emphasizing their roles and responsibilities in safeguarding university resources.
  - Promote regular communication and engagement to keep the university community informed about cybersecurity risks, trends, and best practices.
- Ensure regulatory compliance and enhance audit readiness.
  - Regularly assess and align cybersecurity practices with relevant laws, regulations, and industry standards.
  - Implement robust audit and assessment processes to evaluate cybersecurity controls, identify vulnerabilities, and proactively address any compliance gaps.
- Foster collaboration and information sharing.
  - Establish mechanisms for sharing cybersecurity information, best practices, and lessons learned within the university community and with external partners.

- Collaborate with peer institutions, industry organizations, and government agencies to exchange threat intelligence and stay abreast of emerging cybersecurity trends.

Scope:
This charter, and subsequently referenced policies, generally apply to all members of the AU Community (as defined in Appendix B) that have access to AU resources. In the event a given policy applies only to a sub-set of the AU Community, the policy document will annotate the specific scope within its policy document. AU Community members collect data associated with the following categories while carrying out AU's academic, research, and clinical missions:

- Academic,
- Financial,
- Medical,
- Personal and Demographic,
- Faculty and Staff,
- Course and Curriculum,
- Research and Academic Publications,
- Alumni,
- Institutional Performance and Accreditation,
- Facilities and Infrastructure.

Federal and State laws and regulations, industry standards, and contractual obligations impose requirements on Augusta University regarding how it safeguards and protects the confidentiality, integrity, and availability of the data it collects. AU complies with all applicable requirements and all AU data are protected regardless of the media in which they are stored. This includes, but is not limited to, paper documents and electronic or digital formats regardless of whether the data is at rest or being handled, transmitted, or conveyed using AU's IT assets.

These guidelines and standards also play a pivotal role in governing how different data types are communicated or shared. By abiding by these established frameworks, the university ensures sensitive information is handled responsibly, access is restricted appropriately, and its data sharing practices align with the highest security measures.

Roles/Responsibilities:

Executive Leadership:
Executive Leaders (i.e., senior AU officials to include the Provost, Deans, Vice Presidents, Assistant Vice Presidents, Department Chairs, and Directors) are responsible for establishing strategic direction, defining risk appetite, and being accountable for cybersecurity. They ensure compliance with security policies, standards, procedures, and practices within their respective organization's areas of responsibility.

Chief Information Officer (CIO):
The Chief Information Officer (CIO) is a top-level executive responsible for overseeing AU's technology infrastructure and strategy. The CIO ensures that information and cybersecurity are top priorities for Augusta University and are integrated into all aspects of university operations. To that end, the CIO's cybersecurity responsibilities include:

- Executive Leader Collaboration: The CIO works closely with other university leaders to understand the University's mission, purpose, and intent and anticipate the organization's information security needs.

- Technology Initiative Advocate: Promoting cybersecurity initiatives and innovations that enhance the organization's security posture and align with AU's strategic goals while providing operational leadership, advice, and support to IT and Cyber Defense leadership.

- Risk Management and Compliance: The CIO provides insights and recommendations to executive leaders on managing cybersecurity risks, ensuring data privacy, complying with regulations, and implementing disaster recovery plans.

- Technology Roadmap Development: The CIO leverages knowledge of the evolving cybersecurity landscape and industry best practices to contribute to the technology development roadmap for the university. In doing so, the CIO ensures necessary cybersecurity measures and technologies are implemented in the AU enterprise to maintain a well-prepared and resilient cyber defense that is postured to meet emerging cyber threats.

- IT Impact and Value Communication: The CIO serves as the interface between the CISO and the Executive Leadership to effectively communicate the value of cybersecurity investments. During these interactions, the CIO emphasizes how these investments protect digital assets and support the organization's overall success.

- Vendor and Vendor Relationship Management: The CIO, or delegated representative, ensures third-party vendors providing cybersecurity services meet high standards, protecting the organization from potential vulnerabilities.

Chief Information Security Officer (CISO):
The Chief Information Security Officer (CISO) plays a pivotal role in providing solutions, guidance, and expertise in information technology (IT) security. The CISO is responsible for facilitating the effective implementation of the AU Information and Cyber Security Programs. The CISO's cybersecurity responsibilities include:

- University Leader and CIO Collaboration: The CISO continuously collaborates with University Leaders, the CIO, and organizational staff to ensure the information and cybersecurity programs effectively balance business needs, maintain a robust cybersecurity posture, and contribute to the overall success of the organization.

- System and Data Classification: The CISO ensures a comprehensive system and data classification process is developed, implemented, and maintained, ensuring that data is appropriately protected based on its sensitivity.

- Policy and Standard Development: The CISO reviews, approves, disseminates, and maintains information security policies, standards, guidelines, and procedures, ensuring that they are appropriate and current to safeguard AU's sensitive information and IT systems.

- IT Risk Management: The CISO oversees the development, implementation, and maintenance of a comprehensive IT risk management and assessment program, proactively identifying and addressing cybersecurity risks across AU's network enterprise.

- Security Status Monitoring: The CISO actively reviews security status reporting of all sensitive IT systems across the university environment. The CISO uses consolidated data to provide regular updates to the Compliance Team on the state of IT security.

- Incident Management: The CISO plays a crucial role in identifying developing a program to report all known or suspected security incidents to the USG. The CISO responsibility is to ensure that appropriate measures are taken to mitigate the impact of potential cybersecurity threats and prevent their recurrence.

- Awareness and Training: The CISO oversees the development, implementation, and maintenance of an information security awareness and training program for all users, enhancing the organization's overall cybersecurity posture.

- Vendor and Vendor Relationship Management: The CISO collaborates with the CIO, as a delegated representative, to ensure third-party vendors providing cybersecurity services meet high standards that reduce organizational risk resulting from external partnerships.

AU Resource Users:
Cybersecurity is everyone’s responsibility. Users are required to abide by this charter and subsequent policies, standards, and procedures. All have a responsibility to report suspected cybersecurity failures or policy violations as defined within the AU Policy and the USG IT Handbook.

Framework for Future:

The AU Cybersecurity Charter is designed to be a dynamic and adaptive framework. As such, it will be adjusted on an as needed basis, but not longer than every five years to ensure alignment with the latest guidelines and standards set forth by the USG IT Handbook. The charter will also be regularly updated to incorporate the most current best practices and protocols recommended by the U.S. government as technology and cyber threats evolve. Any and all changes will follow the standard policy review process with final approval by the Policy Advisory Group (PAG).

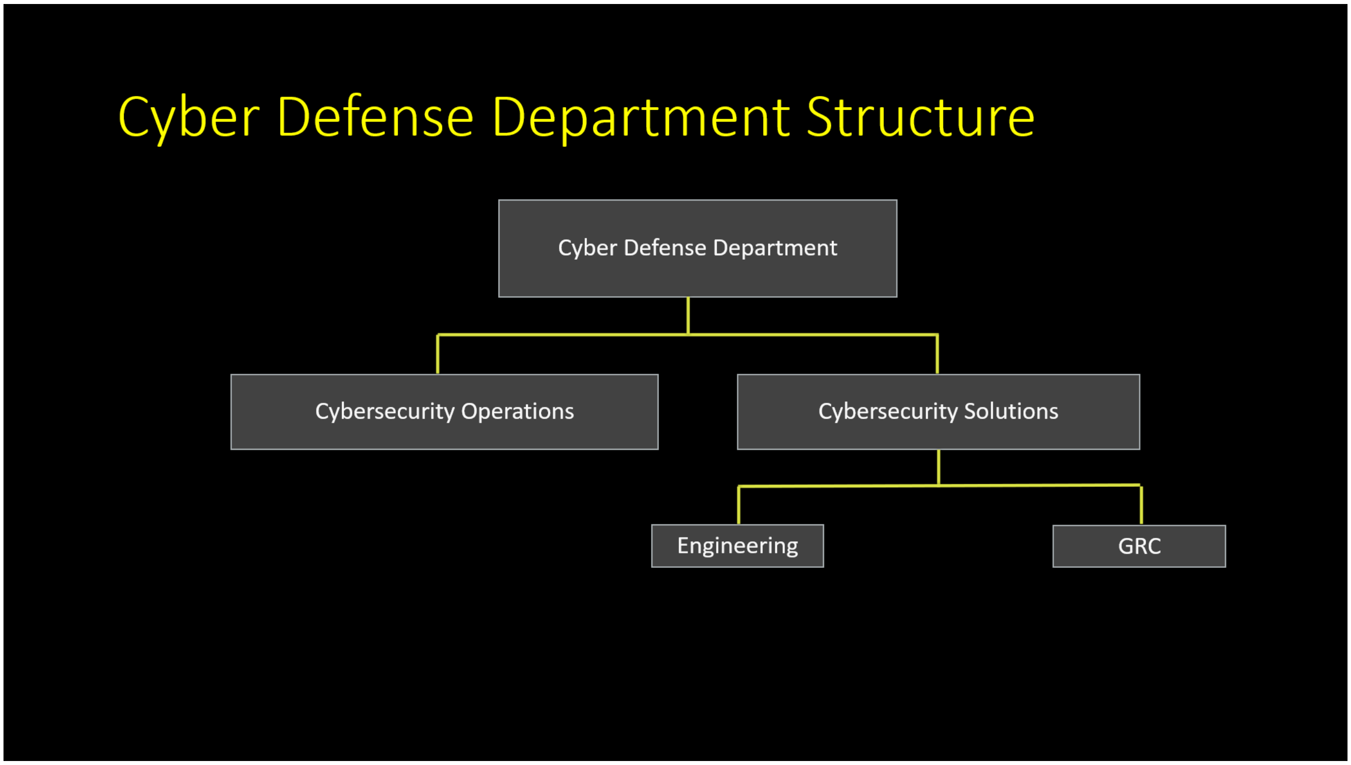
The AU Cybersecurity Charter acknowledges the university's unique IT infrastructure and operations and integrates university-specific policies (as needed) to address specific cybersecurity challenges and risks within its environment. This comprehensive and flexible approach ensures that AU remains at the forefront of cybersecurity preparedness and maintains a secure online environment while safeguarding its digital assets and sensitive data for all its stakeholders.

Section 1.1 Augusta University Cybersecurity Program

Augusta University developed a cybersecurity program that prioritizes understanding its mission, objectives, stakeholders, and activities in accordance with the Board of Regents' Policy Manual, Section 10.4 guidance. This program encompasses cybersecurity policies, standards, procedures, and guidelines, is aligned with the guidelines provided by USG Cybersecurity, and is subject to review by USG Cybersecurity upon request.

1.1.1 Organizational Responsibilities and Requirements:

AU has resourced and staffed a robust Cyber Defense Department, cohesively integrating its Cybersecurity Solutions and Cybersecurity Operations teams to effectively address its Information and Cybersecurity program responsibilities and requirements, as outlined in the USG IT Handbook (Reference USG IT Handbook v.2.9.7.1). Please see Figure 1 for the Department’s structure.



Cyber Defense Department Structure

Cyber Defense Department

Cybersecurity Operations

Cybersecurity Solutions

Engineering

GRC

Figure 1: Augusta University Cyber Defense Department Structure

The Cyber Defense Department has several key roles with specific responsibilities that allow it to accomplish its mission. Those roles are as follows:

Director, Cybersecurity Operations:

The Director of Cybersecurity Operations leads and oversees the Cybersecurity Operations Directorate within the Cyber Defense Department. This is a critical role that is responsible for ensuring the protection and security of the AU enterprise against cyber threats and data breaches through real-time monitoring, incident response, security policy enforcement, and collaboration with other cybersecurity teams. The Director of Cybersecurity Operations responsibilities include:

- Lead and provide strategic direction to the Cybersecurity Operations Directorate via input from the CISO.

- Ensure real-time monitoring, incident response, and security policy enforcement to protect Augusta University and its affiliated institutions.

- Oversee the Command Center for incident response and security monitoring activities.

- Foster a culture of collaboration and effective communication among cybersecurity teams.
- Evaluate team performance and allocate resources effectively.

- Identify, deploy, and implement effective cybersecurity tools and solutions.

Director, Cybersecurity Solutions:

The Director of Cybersecurity Solutions leads and manages a directorate composed of cybersecurity architects, analysts, and engineers who ensure AU's information technology systems are implemented securely in accordance with applicable rules, regulations, guidelines, and policies. the secure implementation of systems in accordance with regulations and information assurance/cybersecurity guidelines supporting Augusta University, including Augusta University Health and all related entities. The Director of Cybersecurity Solutions key responsibilities include:

- Cybersecurity Policy and Management: Collaborate with the Chief Information Security Officer on the development, documentation, implementation, and monitoring of policies, procedures, and practices that ensure confidentiality, integrity, and availability of Augusta University data and assets.

- Strategy Development and Prioritization: Plan project prioritization, strategy, execution, policies, procedures, coordination, and guiding practices throughout the procurement process and program life cycle.

- Governance, Risk Management, and Compliance (GRC) Integration: Manage the governance, risk management, and compliance (GRC) integration of compliance mechanisms, including HIPAA considerations, and capabilities to enable secure network operations.

- Stakeholder Communication and Briefings: Provides routine operational updates and briefings to senior executives, senior-level officials, and stakeholders within Augusta University staff and Augusta University Health System. Manages personnel, processes, technology, and development of concepts to effectively monitor and improve network security postures while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Manager, Governance – Risk – Compliance (GRC):

The GRC Manager at Augusta University supervises governance, risk, and compliance initiatives, with a focus on enhancing cyber risk processes, vendor management, and identity governance. They collaborate with cybersecurity teams, conduct security practice assessments, and develop technical standards. The manager also leads identity management efforts, guides security strategies, and oversees application onboarding and access control.

Key Responsibilities:

- Manage and maintain various cybersecurity tools, ensuring effective configuration, upgrades, and support issue resolution.

- Implement and enhance endpoint protection solutions, safeguarding AU/AUH endpoints with anti-malware and defense technologies.

- Support legal, compliance, and HR departments through data protection and eDiscovery tools for investigations and legal responses.

- Lead vulnerability management processes, identifying and prioritizing vulnerabilities across applications, systems, and infrastructure.

- Integrate cybersecurity solutions with IT systems, including data ingestion into SIEM, firewall/IPS security recommendations, and automated ticketing.

- Collaborate with IT teams and vendors to assess system configurations and optimize security measures.

- Deploy new protection solutions, such as data loss prevention, mobile device management, and Microsoft Defender, to ensure comprehensive security coverage.

1.1.2 Cybersecurity Governance

Cybersecurity Governance Committee: Provides advice and counsel on cybersecurity and information security matters to the AU President and IT Executive Governance Committee. The overall purpose of the committee is to ensure Augusta University leverages IT information security and risk management practices to protect the confidentiality of our students, patients, faculty, and staff, and to reduce adverse impacts to Augusta University.

Cybersecurity Advisory Committee: The Cybersecurity Advisory Committee's role is to create a cross-functional technical team for evaluating cybersecurity measures within the AU environment. It sets priorities for cybersecurity tasks, offers input on long-term architectural plans and immediate security needs, ensures compliance with relevant directives and recommendations, and serves as an expert group to determine optimal security approaches for the AU enterprise.

Section 1.2 Appropriate Usage Standard

1.2.1 Appropriate Usage Requirements:

Reference Augusta University Policy Library: Acceptable Use of Information Technology Policy
Reference Augusta University Policy Library: Acceptable Use of Electronic Mail & Electronic Messaging Policy

1.2.2 Mobile Workforce Requirements:

Reference Augusta University Policy Library: Remote Access Policy
Reference Augusta University Policy Library: Mobile Device Policy
Reference Augusta University Policy Library: International Travel Policy
Reference Augusta University Policy Library: Electronic Access Control Policy

1.2.3 Enforcement

It is the responsibility of all stakeholders to report any known vulnerabilities, suspected vulnerabilities, and Cybersecurity threats immediately by calling 72CYBER at (706) 722-9237 or emailing 72CYBER@augusta.edu. Furthermore, any user engaging in unethical and/or inappropriate practices that violate AU standards is subject to disciplinary proceedings that may include suspension of system privileges, expulsion, termination and/or legal action as appropriate. If a user is suspected of violating AU standards or policy, any right to privacy may be superseded by AU’s requirement to protect the integrity of IT resources, the rights of all users, and state assets. AU reserves the right to examine material stored on or transmitted through AU IT resources to maintain appropriate standards of conduct and duty of care.
Reference Augusta University Code of Conduct (Students)
Reference Augusta University Policy Library: Disciplinary Procedures for Employees (Faculty and Staff)

Section 1.3 Cybersecurity Incident Management

Reference Augusta University Policy Library: Cybersecurity Incident Response Plan Policy

Section 1.4 Information Asset Management and Protection

A "standard of due care" is required to prevent misuse or loss of AU information assets. Members of the AU Community must provide for the integrity and cybersecurity of its information assets.
Information assets are defined as:

1. All categories of automated information, including, but not limited to, records, files, and databases.

2. Information technology facilities, equipment (including endpoints, personal computer systems) and software owned or leased by AU.

1.4.1 Information Asset Management

Augusta University (AU) employs a robust asset management approach utilizing several different tools to track its assets within the environment. This integrated solution ensures the continuous monitoring, assessment, and safeguarding of AU's information assets and allows AU to maintain an inventory of acquired hardware and software. AU's asset management program uses a continuous process to update its inventories as it strives to meet USG's standards for information asset protection and management.

1.4.2 Information Asset Protection

Reference Augusta University Policy Library: Acceptable Use of Information Technology
Reference Augusta University Policy Library: Data Management Classification Policy
Reference Augusta University Policy Library: Encryption Policy
Reference Augusta University Policy Library: Vulnerability and Patch Management Policy
Reference Augusta University Policy Library: Workstation Security Policy
Reference Augusta University Policy Library: Electronic Data Retention Policy
Reference Augusta University Policy Library: Electronic Data Storage Backup Policy

Section 1.6 Information System Categorization

1.6.1 General Overview

Data is a critical asset of Augusta University. Augusta University and its affiliates have a responsibility to protect the confidentiality, integrity and availability of the information and information systems assets utilized. However, to protect the data, there must be an understanding of what to protect, why protect it and how to protect it. The security objective is to maintain the confidentiality, integrity and availability of all information and information systems, products, or services. Security categorization is the characterization of information, or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organization operations, assets, or individuals and Augusta University itself, to include all AU contractors and suppliers that accesses, stores, processes and transmits data and information assets on behalf of AU. AU uses the USG definitions for confidentiality, integrity, and availability, which are defined as:

1) Confidentiality - “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.
2) Integrity - “Guarding against improper information modification or destruction and includes ensuring information non - repudiation and authenticity…” [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.
3) Availability - “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to, or use of, information or an information system.

1.6.2 Categorization Methodology

AU adheres to a comprehensive security categorization process aligned with FIPS Publication 199 standards. This process involves data owners inventorying and assigning security categories to information systems, products, or services based on potential impacts. Categories range from LOW to HIGH, reflecting the expected effects on organizational operations, assets, and individuals. The collaboration between information system owners, information owners/stewards, and organizational officials ensures accuracy. This organization-wide activity considers enterprise and cybersecurity architecture, as well as external suppliers interacting with AU data. The outcomes influence security control selection and assurance requirements, enhancing system protection. AU employs this process, designating mission-critical systems based on categorization outputs, safeguarding sensitive data and critical functions vital for achieving organizational goals.

Section 1.7 Classification of Information

Reference Augusta University Policy Library: Data Management Classification Policy

Section 1.8 Endpoint Management

Reference Augusta University Policy Library: Information Technology Configuration Standards Policy
Reference Augusta University Policy Library: Vulnerability and Patch Management Policy
Reference Augusta University Policy Library: Workstation Security Policy

Section 1.9 Cybersecurity Awareness, Training, and Education

Reference Augusta University Policy Library: Cybersecurity Training Policy

Section 1.10 Required Reporting

1.10.1 Required Reporting Activities

Augusta University adheres to a comprehensive cybersecurity reporting framework, ensuring compliance with USG's requirements and schedules. The reporting activities encompass various aspects of cybersecurity preparedness and incident response. When there are changes to the cybersecurity officer or their designee's contact information, they promptly update USG Cybersecurity. Additionally, the university must have a formal cybersecurity incident response plan documented and filed with USG Cybersecurity.

Augusta University promptly reports cybersecurity incidents and events affecting its information systems and/or services to USG Cybersecurity. High-priority incidents concerning critical systems require immediate reporting within one hour of identification. Additionally, Augusta University participates in an annual Cybersecurity Program Review (CPR), where it undergoes comprehensive assessments and provides updated reports through a survey. CPR includes various components such as personnel, policy and compliance, governance, awareness training, cybersecurity operations, data governance, risk management, incident management, and contingency planning. Compliance with these reporting requirements ensures a proactive approach to safeguarding sensitive information and maintaining robust cybersecurity measures.

1.10.2 Remediation and Mitigation Tracker

Augusta University maintains a Remediation and Mitigation Tracker in accordance with guidance outlined in the USG IT Handbook. This tool facilitates tracking and managing cybersecurity issues identified during audits or program reviews. It records issue details, assigns impact ratings, designates responsible parties, and estimates resources required for resolution. Specific milestones and completion dates are identified, with status and comments tracking the progress of issue remediation. This comprehensive approach ensures timely and effective mitigation of cybersecurity vulnerabilities and fosters a proactive response to potential threats.

Section 1.12 Password Management

Reference Augusta University Policy Library: Password Protection Policy

Section 1.13 Domain Name System Management

AU adheres to USG IT Handbook's Section 5.13 guidance for Domain Name System management. It follows USG specifications regarding internal DNS security (such as physical and logical securing of systems, resolution to internal servers, and adherence to static IP addresses) as well as external DNS security requirements (including placement within a demilitarized zone, firewall or intrusion prevention protection, and secured physical and logical systems).

Reference USG IT Handbook v. 2.9.7.1, Section 5.13 Domain Name System Management

Section 1.14 Information Protection Management

Augusta University complies with the guidelines noted in the USG IT Handbook, Section 5.14, in order to mitigate risks associated with identity theft and enhance information security. The principal aim of information protection management is the detection, prevention, and reduction of identity theft through the identification and remediation of potential vulnerabilities. The USG IT Handbook enumerates several indicators of potential fraud, including, but not limited to, suspicious activities or documentation, discrepancies in personal identifying information upon submission, and irregularities in account behavior. This section underscores the critical nature of recognizing such indicators and the necessity of timely intervention. Furthermore, it delineates precise strategies to safeguard and secure personal data.

Reference: USG IT Handbook v. 2.9.7.1, Section 5.14 Information Protection Management

Section 1.15 Email Use and Protection

Reference Augusta Policy Library: Acceptable Use of Electronic Mail & Electronic Messaging Policy

Appendix A: References

- Board of Regents, University System of Georgia - Policies https://www.usg.edu/policies
  - Policy Manual - Section 10
  - Business Procedures Manual
  - Data Privacy Policy and Legal Notice
  - Ethics & Compliance Program
  - Records Management and Archives - Records Retention Schedule
- Federal Regulation & Legislation https://www.govinfo.gov/ | https://www.cnss.gov/ | https://www.whitehouse.gov/omb/ | https://www.irs.gov/
  - Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, March 2014.
  - Committee on National Security Systems Instruction 4009, Committee on National Security Systems (CNSS) Glossary, April 2015.
  - Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017.
  - Federal Information Policy, 44 U.S.C, Sec 3502 (8)
  - Federal Information Security Modernization Act (P.L. 113-283), December 2014.
  - Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended by Public Law No. 104-231, 110 Stat. 3048
  - Electronic Freedom of Information Act Amendments of 1996.
  - Internal Revenue Service, IRS Publication 1075.
  - Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016.
  - Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016.
  - Office of Management and Budget Memorandum M-13-13, Open Data Policy-Managing Information as an Asset, May 2013.
  - Office of Management and Budget Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017.
  - Office of Management and Budget Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program, December 2018.
  - Privacy Act (P.L. 93-579), December 1974.
  - Title 21 Code of Federal Regulations, 21.
  - Title 32 Code of Federal Regulations, Sec. 2002.4, Definitions. 2018 Ed.
  - Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 Ed.
  - Title 44 U.S. Code, Sec. 3301, Definition of records. 2017 Ed.
  - Title 44 U.S. Code, Sec. 3502, Definitions. 2017 Ed.
  - Title 44 U.S. Code, Sec. 3552, Definitions. 2017 Ed.
  - Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities. 2017 Ed.

- Title 44 U.S. Code, Sec. 3601, Definitions. 2017 Ed.

- Industry Standards and Best Practices https://iso.org/ | https://technet.microsoft.com/ | https://www.archives.gov/cui | https://www.aicpa.org/

  - ISO 27005 Information Security Risk Management (ISRM)
  - Microsoft Securing DNS
  - National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry.
  - Generally Accepted Privacy Principles (GAPP)

- NIST Computer Security Resource Center - FIPS https://csrc.nist.gov/publications/fips

  - FIPS Publication 199, Standards for Security Categorization for Federal Information Systems, February 2004.
  - FIPS Publication 200, Minimum Security Requirements for Federal Information Systems, March 2016.

- NIST Computer Security Resource Center - Glossary https://csrc.nist.gov/glossary

- NIST Computer Security Resource Center - SP https://csrc.nist.gov/publications/sp

  - SP 800-16 IT Security Training Requirements, April 1998.
  - SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems, February 2006.
  - SP 800-28 Ver. 2 Guidelines on Active Content and Mobile Code, March 2008.
  - SP 800-30 Rev. 1 Guide for Conducting Risk Assessments, September 2012.
  - SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems
  - SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework
  - SP 800-50 Building an IT Security Awareness and Training Program, October 2003.
  - SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
  - SP 800-53A Assessing Security and Privacy Controls: Building Effective Security Assessment Plans, July 2008.
  - SP 800-55 Performance Measurement Guide for Information Security, December 2014.
  - SP 800-60 Vol 1&2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.
  - SP 800-61 Rev. 2 Computer Security Incident Handling Guide, August 2012.
  - SP 800-81-2 Secure Domain Name System (DNS) Deployment Guide, September 2013.
  - SP 800-83 Rev. 1 Guide to Malware Incident Prevention and Handling, July 2013.
  - SP 800-92 Guide to Computer Security Log Management, September 2006.
  - SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.
  - SP 800-181 Rev. 1 National Initiative for Cybersecurity Education (NICE).

- NIST Frameworks
    - Cybersecurity Framework https://www.nist.gov/cyberframework
    - Privacy Framework https://www.nist.gov/privacy-framework
- NIST Interagency/Internal Report - IR https://csrc.nist.gov/publications/nistir
    - NISTIR 8259 Baseline for Securable IoT Devices, May 2020.
- Official Code of Georgia Annotated - http://www.lexisnexis.com/hottopics/gacode/default.asp
    - O.C.G.A. § 10-1-910 – Identity Theft
    - O.C.G.A § 16-9-90, et seq. – Georgia Computer Systems Protection Act
    - O.C.G.A. § 16-9-150 – Georgia Computer Security Act of 2005
    - O.C.G.A § 50-18-72 – Georgia Open Records Act
    - O.C.G.A. § 38-3-22 (2021 Cyber incident reporting responsibilities.)

Appendix B: Glossary

Abuse

Activity that violates an organization's Acceptable Use Policy (AUP).

Academic Classroom

Space officially categorized and reported as a "classroom" in Archibus; these include 110 – Classroom, 212 – Computer Classroom, 213 – Distance Learning Classroom,

Academic Laboratory

Space officially categorized and reported as a "lab" in Archibus; these include 211 – Class Lab, 221 – Discipline Open Laboratory, 222 – Testing/Services Laboratory, 411 – Open Computing Lab, 412 – Learning Support Lab

Access Control

The process of permitting or restricting access to applications at a granular level, such as per-user, per-group and per-resources. (Source: SP 800-113)

Advanced Encryption Standard (AES)

Reference "Encryption."

Adversarial Threats

Any circumstance or event with the potential to adversely impact organizational operations (including mission, function, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Affiliates

Individuals or Business Entities with contractual or other relationships with the University and are not employees, faculty, or students.

Architecture

A set of related physical and logical representations (i.e., views) of a system or a solution. The architecture conveys information about system/solution elements, interconnections, relationships and behavior at various levels of abstractions and with different scopes. Refer to security architecture. (Source: SP 800-160)

Assurance

Measure of confidence that the security features, practices, procedures and architecture of an information system accurately mediates and enforces the security policy. (Source: SP 800-39)

Attack

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality (Source: SP 800-82 Rev. 2). The following includes examples of common attack methods observed targeting enterprise networks:

- Brute Force Attack: Repeatedly attempting different password combinations to gain unauthorized access to a system or account.

- Distributed Denial of Service (DDoS): Overwhelming a system or network with a massive volume of requests, causing it to become unavailable to legitimate users.

- Malware Infection: Introducing malicious software, such as viruses, worms, or Trojans, to compromise the integrity of a system, steal data, or gain control over the affected device.

- Phishing Attack: Sending deceptive emails or messages to trick users into revealing sensitive information or clicking on malicious links, potentially compromising confidentiality.

- SQL Injection: Exploiting vulnerabilities in web applications to manipulate or inject malicious SQL queries, potentially compromising the integrity and confidentiality of a database.

- Ransomware: Encrypting a user's data and demanding a ransom for its decryption, impacting both availability and confidentiality.

- Man-in-the-Middle (MitM) Attack: Intercepting and potentially modifying communications between two parties, compromising both confidentiality and integrity.

- Insider Threat: A malicious or negligent employee exploiting their access to compromise system integrity, availability, or confidentiality.
- Zero-Day Exploit: Taking advantage of a vulnerability that is unknown to the vendor or not yet patched, potentially compromising system integrity or confidentiality.

Augusta University (AU) Community

Full-time or part-time employees, trainees, vendors, contractors, students, alumni, non-paid affiliates, faculty, emeritus faculty or any other individuals who may create, use, disclose, access, or transmit any AU information.

Augusta University (AU) Cyber Defense Department

Reference Section 1.1 Augusta University Cybersecurity Program

Augusta University (AU) Data

Reference Institutional Data

Authentication

A process of attempting to verify the digital identity of a system user or processes. (Source: SP 800-47)

Authorization

In this context means to grant permission to an identified individual to use a computer or data resource. Acceptance of authorization to use AU computer and data resources establishes an obligation on the part of the individual to use those resources responsibly.

Authorized User

Any employee, contractor or individual who has been granted authority or access to use AU information technology resources to carry out their job responsibilities and/or to support enterprise business, clinical and/or academic endeavors. This definition includes students who may be using information technology resources as part of their academic pursuits or in their capacity as part-time, temporary employees. Sensitive Data is institutional data that is not legally protected but should not be made public and should only be disclosed under limited circumstances. Users must be granted specific authorization to access since the data's unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution.

Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]. A loss of availability is the disruption of access to, or use of, information or an information system. (Source: SP 800-137)

Awareness

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate job performance. (Source: SP 800-50)

Awareness, Training and Education Controls

Includes (1) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure, (2) training which teaches people the skills that will enable them to perform their jobs more effectively and (3) education which is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities. (Source: SP 800-16)

Baseline

Formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle. Note: The engineering process generates many artifacts that are maintained as a baseline over the course of the engineering effort and after its completion. The configuration control processes of the engineering effort manage baselined artifacts. Examples include stakeholder requirements baseline, system requirements baseline, architecture/design baseline and configuration baseline. (Source: SP 800-160)

Benign Policy Violation

Activity that violates organizational Acceptable Use Policy (AUP) but is not a threat and requires no action.

Bring Your Own Device (BYOD)

Reference Personally Owned Device (POD).

Brute Force Attack

In cryptography, an attack involves trying all combinations to find a match. A method of accessing an obstructed device through attempting multiple combinations of numeric/alphanumeric passwords. (Source: SP 800-72)
Reference Attack

Business Associate

A person or entity that creates, receives, maintains, or transmits protected health information to perform certain functions or activities on behalf of a covered entity.

Three categories of service providers are specifically identified as business associates under the final rule:

- Health information organizations, e-prescribing gateways, and other people or entities that provide data transmission services to a covered entity with respect to protected health information and that require access on a routine basis to such protected health information;
- People or entities that offer personal health records to one or more individuals on behalf of a covered entity; and
- Subcontractors that create, receive, maintain or transmit protected health information on behalf of business associates.

Business Case

A description of a requested project or initiative that explains the goals, benefits and cost of the request.

Business Continuity Plan

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. (Source: SP 800-34 Rev.1)

Business Impact Analysis

An analysis of an information system's requirements, functions and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (Source: SP 800-34 Rev. 1)

Certificate

A data structure that contains an entity's identifier(s), the entity's public key (including an indication of the associated set of domain parameters) and other information, along with a signature on that data set that is generated by a trusted party, i.e., a certificate authority, thereby binding the public key to the included identifier(s). (Source: SP 800-56A Rev. 2)

Certificate Authority

A trusted entity that issues and revokes public key certificates. (Source: SP 800-63-2)

Chain of Custody

A process that tracks the movement of evidence through its collection, safeguarding and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred and the purpose for the transfer. (Source: 800-72)

Chief Information Officer (CIO)

Organization official responsible for: 1) providing advice and other assistance to organization senior leadership to ensure that information systems are acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations and priorities established by the organization presidents, chancellor, or the Board of Regents; 2) developing, maintaining and facilitating the implementation of a sound and integrated information system architecture; and 3) promoting the effective and efficient design and operation of all major information resources management processes, including improvements to work processes. (Source: SP 800-53)

Chief Information Security Officer (CISO)

Organization official responsible for: 1) developing and maintaining a cybersecurity organization and architecture in support of cybersecurity across the USG and between USG institutions; and 2) maintaining cybersecurity implementation guidelines that the USO, all USG institutions and the GPLS follow in the development of their individualized cybersecurity plans. (Source: BOR Policy Manual)

Classified Information

Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD). (Source: SP 800-53 Rev. 4)

Cloud Computing

A computing infrastructure refers to the delivery of computing services, such as storage, processing power, databases, networking, software, and more, over the internet. Instead of owning and maintaining physical hardware and software infrastructure, users can access and use these resources on-demand through remote servers provided by cloud service providers. Cloud computing offers scalability, flexibility, and cost-efficiency, as users can adjust their usage according to their needs. It encompasses different service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), allowing organizations and individuals to leverage advanced technology resources without the burden of managing and maintaining them on-premises.

Common Control

A security control that is inherited by one or more organizational information systems. See Security Control Inheritance. (Source: SP 800-137)

Common Meeting Space

Space officially categorized and reported as a “common meeting space” in Archibus; this includes 612 – General Assembly

Compensating Controls

The cybersecurity or privacy controls or safeguards implemented in lieu of the baseline controls that provide equivalent or comparable protection for a system or organization.

Compliance Date

The date by which the USG organization is expected to comply with the policy or standard.

Compromise

The unauthorized disclosure, modification, or use of sensitive data (e.g., keying material and other security-related information). (Source: SP 800-133)

Computer Data

Computer Data is raw and structured information processed, stored, and manipulated by computer systems. It encompasses all types of digital content, such as text, images, videos, numbers, and more. Computer data can be represented in various formats, including binary code, text files, databases, spreadsheets, and multimedia files. It forms the foundation for computer operations, software applications, and digital communication, enabling computers to perform tasks, make calculations, store information, and generate meaningful output based on input and algorithms.

Confidential / Regulated / Restricted Data

Confidential Data (also referred to as Restricted and/or Regulated data) encompasses information subject to limitations on accessibility and distribution, as dictated by legal and contractual obligations. This category includes data whose inappropriate use or disclosure could detrimentally affect the institution's mission accomplishment. It includes records concerning individuals seeking protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), alongside data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act. Additionally, it encompasses data governed by federal, state, and local regulations or policies. This incorporates categories like protected health information, personally identifiable details about students or research participants, and information conducive to identity theft. Moreover, it involves data categorized as business-sensitive, where unauthorized disclosure might harm Augusta University's operational, financial, or reputational relationships.

Specific examples of restricted data encompass non-directory information identifiable to an individual, such as dates of birth, driver’s license numbers, employee and student ID numbers, license plate numbers, and compensation information. Additionally, the institution's proprietary information, including intellectual research findings, intellectual property, financial data, and donor and funding sources, falls within this category.

Access to restricted data necessitates specific authorization due to the potential for unauthorized disclosure, alteration, or destruction causing perceivable damage to the institution. This safeguards the institution's mission, operational integrity, financial well-being, and overall reputation.

Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information. (Source SP 800-137)

Configuration Standard

A document or collection of documents that describe how a device should be configured. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy.

Context of Use

The purpose for which PII is collected, stored, used, processed, described, or disseminated.

Continuity of Operations Plan

A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days because of a disaster event before returning to normal operations. (Source: SP 800-34 Rev. 1)

Controlled Unclassified Information (CUI)

A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (Source: SP 800-53 Rev. 4)

Controls

Controls, also known as safeguards, are proactive measures prescribed to meet the security requirements specified for an information system.

1. Administrative Controls
2. Technical Controls
3. Physical Controls

Course

A course scheduled in Banner.

Covered Individual

Any individual who is an AU employee (faculty or staff), AU students, an unpaid AU adjunct faculty member, any unpaid person (including a postdoc or fellow) who has an AU email account and access to AU systems or AU institutional data, or any individual who is engaged in any activity on AU campus or in AU facilities pursuant to a visa sponsored by AU.

Covered International Travel

Any international travel outside the United States (A) by Covered Individuals who are traveling for AU business, teaching, conference attendance, research purposes, or who have receive offers of sponsored international travel for research or professional purposes; or (B) by Covered Individuals for which the traveler proposes to (i) access AU information systems while traveling, and/or (ii) travel with an AU device (i.e. laptop), and/or (iii) travel with sensitive AU data. Covered International Travel does not include personal travel by a Covered Individual.

Critical System

Reference “Mission-Critical System.”

Critical System/Infrastructure

System and/or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: SP 800-30 Rev. 1)

Cybersecurity

The practice of protecting computer systems, networks, programs, and data from unauthorized access, use, disclosure, disruption, or destruction. It involves implementing measures and safeguards to prevent and detect potential threats, vulnerabilities, and attacks targeting information technology infrastructure and assets.

Cybersecurity Incident

Cybersecurity Incident is a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. This includes attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Cybersecurity Official

Organization official responsible for
1) maintaining the cybersecurity of different types of information within the organization that typically involves maintaining computer networks to ensure that sensitive financial or private information is kept secure and cannot be accessed by someone not authorized to do so;
2) that usually reports to a chief information security officer or other member of upper management, such as a vice president in charge of information technology (IT) or cybersecurity.

Data Access

The process of being granted authorization to interact with data at a level that includes, but is not limited to, read, write and modify.

Data Actions

A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission and disposal. (NIST IR 8062)

Data at Rest

Computer files that are used as reference, but are not often, if at all, updated. They may reside on servers, in backup storage or on the user’s own hard disk.

Data Custodian

AU employees who have administrative and/or operational responsibility over institutional data.

Data Element:

The smallest named item of data that conveys meaningful information. (NIST PF)

Data in Transit

Data on the move from origin or source to destination.

Data Integrity

A loss of integrity is the unauthorized modification or destruction of information. “Guarding against improper information modification or destruction and includes ensuring information non - repudiation and authenticity…” [44 U.S.C., Sec. 3542]
A property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored. In this Recommendation, the statement that a cryptographic algorithm "provides data integrity" means that the algorithm is used to detect unauthorized alterations. (Source: SP 800-56B Rev.1)

Data Leak/Leakage

The unauthorized or unintended transmission of data from within an organization to an external destination or recipient.

Data Loss

The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. (Source: SP 800-137)

Data Loss Prevention

A systems ability to identify, monitor and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions) and data at rest (e.g., data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of protected/classified/CUI information. (Source: CNSSI 4009-2015)

Data Manager

Personnel with day-to-day responsibility for managing administrative processes and establishing business rules for the transactional systems. They have operational responsibility for the data management activities related to the collection, maintenance, protection, and dissemination of data in their functional areas

Data Owners

The heads of Augusta University, the president, chief executive officer, Chancellor, or other identified head of AU are identified as the data owners.

Data Privacy

The practices which ensure that the data shared by customers is only used for its intended purpose.

Data Processing

The collective set of data actions (NIST IR 8062)

Data Processing Ecosystem

The interconnected relationships among entities involved in creating or deploying systems, products or services or any components that process data. (NIST PF)

Data Spillage

An accidental or deliberate cybersecurity incident that results in the transfer of classified information onto an information system not authorized to store or process that information. (Source CNSSI 4009-2015)

Data Steward

Data Steward is defined in section 9.2 of the USG Information Technology Handbook. They are responsible for recommending policies, and establishing procedures and guidelines concerning the accuracy, privacy, and integrity of the data subsets for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas.Examples are the registrar and director of human resources (HR).

Data Subject

Any person whose personal data is being collected, held, or processed.

Data Subject Request (DSR)

A DSR is a petition to an organization by a data subject looking to confirm whether or not the organization is holding personal data about the data subject petitioning and if so, the data subject has the right to access that data, amend that data, or were permitted by law request for that his/her data be erased.

Data Trustee

Executives who have overall responsibility for all the data sets maintained by the units reporting to them. The data trustees are responsible for ensuring that campus institutional data resources are used in ways consistent with the mission of Augusta University. Data trustees are responsibility for the appointing and maintaining accountability of data stewards.

De-Identified Information

Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

Denial of Service

Activity involving an attempt to make a resource unavailable to your network. (Source: SP 800-33)

Departmental Security Authority

Roles that include requesting access and permissions for various Augusta University clinical and administrative systems, assisting in Cybersecurity awareness training and cooperating with the Enterprise Privacy Officer, Chief Information Security Officer, Cybersecurity Office, Chief Compliance Officer, Human Resources, and Public Safety with incident investigations.

Device

Any media, material, or type of equipment that records, stores, transmits, distributes, or uses electronic information. This includes, but is not limited to, computers (hard drives), any removable/transferrable digital memory, disks, memory cards, cloud storage, internet, extranet or any other device which involves the access, storage, or creation of sensitive information.

Device Manager

Person, Entity, or Unit owning responsibility for maintaining or managing information assets and devices as assigned by the respective Cybersecurity Officer, CISO or CIO.

Disassociated Processing

Processing of data or events without association to individuals or devices beyond the operational requirements of the system (NIST IR 8062)

DNS Spoofing

DNS Spoofing refers to confusing a DNS server into giving out bad information.

Domain

Domain is most often used to refer to a domain zone; it is also used to describe a zone or a domain name.

Domain Name Service (DNS)

DNS refers to the domain name system, which represents a powerful Internet technology for converting domain names to their corresponding IP addresses. It is a protocol within the set of standards for the exchange of AU Data on the Internet or on a private Network. The DNS translates a user-friendly domain name such as https://www.augusta.edu/ into an IP address such as “158.93.6.11” that is used to identify computers on a Network.

Dwell Time

The time calculated as the number of days an adversary is present on a victim network, from first evidence of compromise to detection.

Dynamic Host Configuration Protocol (DHCP)

A Network protocol that enables a Server to automatically assign an IP address to a Network enabled device from a defined range of numbers (i.e., a scope) configured for a given Network.

Electronic Message

Any message created, sent, forwarded, replied to, transmitted, stored, copied, downloaded, displayed, viewed, or read by means of telecommunications networks or computer systems. This definition applies equally to the contents of such messages; transactional information associated with such messages, such as headers, summaries, addresses, and addressees; and attachments (text, audio, video).

Electronic Messaging System

Any messaging system that depends on electronic facilities to create, send, forward, reply to, transmit, store, copy, download, display, view, or read Electronic Messages, including services such as email, text messaging, instant messaging, social networking, blogging, electronic bulletin boards, listservs, and newsgroups.

Electronic Protected Health Information (ePHI)

See Protected Health Information (PHI)

Email System

A System that transmits, stores, and receives emails.

Encryption

Encryption is the process of converting plaintext data into unreadable ciphertext through cryptographic techniques, ensuring data confidentiality and security during transmission or storage. It relies on encryption algorithms and keys. There are two main types:

Symmetric Encryption: It employs a single secret key for both encryption and decryption. AES (Advanced Encryption Standard) is a prominent symmetric algorithm, with variations of 128, 192, or 256 bits, securing data efficiently.

Asymmetric Encryption: Also known as public-key encryption, it uses key pairs: public (shared openly) and private (kept secret). RSA and ECC (Elliptic Curve Cryptography) are examples. RSA handles secure communication, digital signatures, and key exchange. ECC offers strong security with shorter key lengths, useful for resource-constrained systems.

These encryption methods underpin secure communication, data protection, and privacy across various digital platforms and applications.

Endpoint Security / Protection

Endpoint Security is an approach to network protection that requires each computing or mobile device on a corporate network to comply with certain standards before network access is granted. Simple forms of endpoint security include personal firewalls or anti-virus software that is distributed and then monitored and updated from a server. (Source: SP 800-128)

Endpoint Security Management

Endpoint Security Management is a policy-based approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources.

Endpoint Security Management Systems

Endpoint Security Management Systems, which can be purchased as software or as a dedicated appliance to discover, manage and control computing devices that request access to the corporate network. Endpoints that do not comply with policy can be controlled by the system to varying degrees. For example, the system may remove local administrative rights or restrict Internet browsing capabilities.

Endpoints

Endpoints can include, but are not limited to, PCs, laptops, smart phones, tablets and specialized equipment such as bar code readers or point of sale (POS) terminals used to connect to the AU wireless or wired Network, access AU email from any local or remote location or access any institutional (AU, departmental or individual) Information System either owned by AU or by an individual and used for AU purposes.

Enterprise

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, fiscal management (e.g., budgets), human resources, security and information systems, information and mission management. For Augusta University, the enterprise consists of the University, Medical Center, and Medical Associates. See Organization. (Source: SP 800-30)

Event

A questionable or suspicious activity that could threaten the security objectives for critical or sensitive data or infrastructure. They may or may not have criminal implications. (Source: SP 800-160)

Exploit Attempt

Activity involving an attempt to manipulate or abuse a specific flaw (vulnerability.)

False Positive

Activity that matches the specified criteria but is not an actual threat or vulnerability. (Source: SP 800-115)

Family Educational Rights and Privacy Act of 1974 (FERPA)

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that affords parents the right to have access to their children’s education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student (“eligible student”). The statute applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Federal Information Processing Standards (FIPS)

Standards and guidelines for federal computer systems that are developed by National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular government requirement. Although FIPS are developed for use by the federal government, many in the private sector voluntarily use these standards.

General Support System (GSS)

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications and people. (Source: SP 800-18 Rev. 1)

Georgia Open Records Act (GORA)

The Georgia Open Records Act (GORA) (OCGA 50-18-70), also known as the Georgia Open Meetings and Open Records Acts or the Georgia Sunshine Laws, is a series of Georgia state laws guaranteeing any citizen of Georgia, as well as non-residents, can request access to public records held by government agencies and departments. These records include documents, papers, letters, maps, books, tapes, photographs, electronic data, and other materials generated or received by public officials and agencies in the course of their official duties.

Georgia Personal Identity Protection Act (GPIPA)

The Georgia Personal Identity Protection Act safeguards personal information by prohibiting public posting or display of Social Security Numbers (SSNs), unsecured transfer of SSNs, and use of SSNs to access websites without additional PIN or password. The law's breach notification aspect was extended in 2007 to encompass state agencies and public universities. Protected data includes names combined with unencrypted SSNs, driver's license numbers, account details, and access codes. Excluding publicly available data, GPIPA addresses identity theft risks by regulating sensitive information handling in Georgia, under O.C.G.A. 10-1-910, 10-1-911, and 10-1-912.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), enacted in 1999, is a U.S. federal law that enhances consumer privacy by regulating how financial institutions handle personal information. It provides limited privacy protections for private financial information and codifies safeguards against pretexting – the fraudulent acquisition of personal data. GLBA requires financial institutions to furnish privacy notices, enabling customers to understand data handling. Furthermore, it establishes rules for financial privacy notices and enforces measures for the administrative, technical, and physical protection of personal information. The GLBA ensures transparency, empowers consumer choice, and mandates robust security practices within the financial sector.

Guideline

A guideline is a set of recommendations, instructions, or principles that provide guidance and direction for achieving a specific goal, desired outcome, and/or policy compliance. It serves as a reference point to assist individuals or groups in making informed decisions, taking appropriate actions, and adhering to established standards or best practices. Guidelines are designed to offer clarity, consistency, and a framework for addressing various situations or tasks effectively.

Family Educational Rights and Privacy Act of 1974 (FERPA)

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The statute applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Harm

Any adverse effects that would be experienced by an individual or an organization if the confidentiality, integrity, or availability of its data were breached.

Health Information

Any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. (Source: SP 800-66 Rev. 1)

Health Information Technology for Economic and Clinical Health (HITECH)

The Health Information Technology for Economic and Clinical Health (HITECH) Act is a U.S. federal law passed in 2009 as part of the American Recovery and Reinvestment Act. It complements HIPAA by addressing the adoption and meaningful use of electronic health records (EHRs) and health information technology (HIT) in healthcare. The HITECH Act promotes the use of EHRs to improve the quality of patient care and increase the efficiency of healthcare delivery. It also strengthens the enforcement of HIPAA regulations and introduces provisions for breach notifications, electronic exchange of health information, and penalties for non-compliance. HITECH aims to accelerate the adoption of digital health technologies while maintaining the privacy and security of patients' health information.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law enacted in 1996 to safeguard the privacy, security, and confidentiality of individuals' protected health information (PHI). It establishes rules and standards for healthcare providers, health plans, and healthcare clearinghouses, collectively known as covered entities, as well as their business associates, who handle PHI. HIPAA's Privacy Rule governs the use and disclosure of PHI, ensuring patients' rights to control their health information. The Security Rule mandates measures to safeguard electronic PHI (ePHI) against unauthorized access and breaches. HIPAA aims to promote the seamless exchange of healthcare data while upholding patient privacy and data security. See https://www.augusta.edu/compliance/privacy/hipaa.php.

Human Resource Management

Human Resource Management (HRM) is the area of administrative focus pertaining to an organization's employees. HRM is sometimes referred to simply as HR.

Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (Source: SP 800-34 Rev. 1)

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. (Source: SP 800-53 Rev. 4)

Incident Response Management

Process of detecting, mitigating and analyzing threats or violations of cybersecurity policies and limiting their effect.

Incidental Storage

The unintentional or secondary retention of data that occurs as a byproduct of using a system, service, or application for its primary purpose. This data is not deliberately collected or stored but rather accumulates over time due to the nature of interactions or transactions. Incidental storage often involves temporary or transient data that is not essential to the main function but is retained temporarily for operational purposes, such as logging, error tracking, or system performance analysis.

Information Leakage

Intentional or unintentional activity that could result in the transmission of data to unauthorized parties. (Source: SP 800-53 Rev. 4)

Information Resources

Information Resources are the collective digital assets, data, and information that the organization possesses and utilizes to support its operations, decision-making processes, and overall objectives. These resources encompass a wide range of digital content, including documents, databases, software applications, intellectual property, research findings, financial records, and communication archives. Effective management of enterprise information resources involves organizing, securing, and optimizing these assets to enhance collaboration, streamline workflows, and ensure compliance with relevant regulations and data protection measures.

Information Security Officer (ISO)

Organization official responsible for: 1) maintaining the cybersecurity of different types of information within the organization that typically involves maintaining computer networks to ensure that sensitive financial or private information is kept secure and cannot be accessed by someone not authorized to do so; 2) that usually reports to a chief information security officer or other member of upper management, such as a vice president in charge of information technology (IT) or cybersecurity.

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: SP 800-137)

Examples of Information Systems (IS) found within the Augusta University Enterprise include the following:

1. Health Information Management Systems (HIMS): These systems are used to store, manage, and retrieve health-related data and records. They play a critical role in healthcare facilities for maintaining patient records, scheduling appointments, billing, and supporting clinical decision-making.
2. Student Information Systems (SIS): SIS are used by educational institutions to manage student data, including enrollment, attendance, grades, course registration, and academic performance. They help schools and colleges streamline administrative processes and enhance communication with students and parents.
3. Enterprise Resource Planning (ERP) Systems: These integrated software solutions help organizations manage various business processes such as finance, supply chain, human resources, and customer relationship management.
4. Customer Relationship Management (CRM) Systems: CRM systems help businesses track and manage interactions with customers and prospects, enabling them to improve customer service, sales, and marketing efforts.
5. Database Management Systems (DBMS): DBMS software is used to create, manage, and manipulate databases, allowing organizations to store and retrieve data efficiently.
6. Content Management Systems (CMS): CMS platforms are used to create, manage, and publish digital content, such as websites and blogs.
7. Business Intelligence (BI) Systems: BI systems gather, analyze, and present data to help organizations make informed business decisions.
8. Supply Chain Management (SCM) Systems: These systems assist in managing the flow of goods, services, and information across the supply chain, optimizing processes and reducing costs.

Information System Owner

See System Owner

Information technology (IT)

Hardware, software, licenses and services used to create, collect, record, process, store, retrieve, display and transmit information in any electronic format.

Information Technology Device

Any institutionally or personally owned device to include, desktops, laptops, servers, network/telecommunications equipment, mobile devices, and storage systems that store, process, or transmit Augusta University data.

Institutional data

Information may be considered institutional data if it satisfies on or more of the following criteria:

o Data used for planning, managing, reporting, or auditing a major administrative function;

o Data reference or used by a participant organization to conduct organization business;

o Data included in an official participant organization administrative report; or,

o Data used to derive an element that meets any of the criteria above.

Institutional Investigation

Activity reported by an institution in accordance with their incident response plans.

Institutional Online Resources

Web pages and documents published or developed by the institution on the internet that provide useful information.

Integrity

Reference Data Integrity.

Isolated Event

Activity that is isolated or the context is undetermined.

Linkable Information

Information about or related to an individual for which there is a possibility of logical association (linkability) with other information about the individual.

Loaner Device

Any AU-owned computer, laptop, or similar electronic device provided for temporary use to a Covered Individual for use only during international travel. These devices will have a limited set of user applications.

Media Access Controller (MAC)

A unique identifier assigned to network interface hardware, such as network adapters or wireless cards. It is a 12-character alphanumeric code that serves as a hardware address for devices within a network. MAC addresses are used to uniquely identify devices on a local network, allowing them to communicate with each other. They play a crucial role in the Ethernet protocol by determining how data packets are sent and received on a network segment, helping to regulate access to the network media and prevent data collisions.

Metric

Metric is a numeric indicator(s) used to monitor and measure accomplishment of goals by quantifying the level of implementation and effectiveness. (Source: SP 800-137)

Misconfiguration

An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities. (Source: SP 800-128)

Mission-Critical System

A Mission-Critical System is a system, product, or service whose failure or malfunction will result in not achieving organizational goals and objectives. Criteria are a) contains confidential or sensitive data (i.e., personally identifiable information (PII) and other regulated information), or b) serves a critical and necessary function for daily operations, or c) a combination of both protected data and critical function.

Mobile Device

Portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, cellular telephones, digital cameras and audio recording devices)." Additionally, all the device form-factors listed above can create data (written, photographed and audio) that are governed by USG Data Retention Standards and may be open records accessible. (NIST SP 800-53)

Monitoring

Monitoring is observing and checking for a set standard or configuration. Continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected. (Source: SP 800-160)

Multifactor Authentication (i.e., Duo)

Multi-factor authentication (MFA) is a security method that requires users to provide multiple forms of identification to access a system or account. It enhances security beyond a single password by combining different authentication factors: something the user knows (like a password), something the user has (like a smartphone or token), and something the user is (like a fingerprint or facial recognition). By demanding two or more of these factors, MFA adds an extra layer of protection against unauthorized access, reducing the risk of breaches even if one factor is compromised.

Network

The network (or Enterprise Network) refers to a complex and interconnected system of computers, devices, and resources within a large organization or company. This network infrastructure is designed to facilitate communication, data sharing, and resource utilization among various departments, locations, and functions of the enterprise. It includes both physical and virtual components, such as servers, routers, switches, wireless access points, and security appliances. Enterprise networks often span multiple geographic locations and can incorporate various technologies like local area networks (LANs), wide area networks (WANs), and cloud services, all managed and maintained to ensure seamless connectivity, data integrity, and operational efficiency across the organization

Non-Public Information (NPI)

Non-Public Information (NPI) is any information that:
(1) provided by a consumer to a financial institution;
(2) resulting from any transaction with the consumer or any service performed for the consumer, or;
(3) otherwise obtained by the financial institution.

Obscured Data/Information

Data/information that has been distorted by cryptographic or other means to hide information (aka masked, obfuscated).

Operations Security

Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling and protecting unclassified evidence of planning and execution of sensitive activities.

Payment Card

Any payment card/device that bears the logo of the founding members of PCI Security Standards Council (PCI SSC), which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc.

Payment Card Industry Data Security Standard (PCI DSS)

Data collected by organizations that accept, store, transmit, or process cardholder data must comply with the PCI DSS and is administered by the PCI SSC (Payment Card Industry Security Standards Council) to decrease payment card fraud across the internet and increase payment card data security. This includes sensitive data that is presented on a card or stored on a card - and personal identification numbers entered by the cardholder. A set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

Peer

a network participant that makes a portion of its resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by Servers or stable hosts.

Peer-to-Peer File Sharing Program

a program that allows any computer operating the program to share and make available files stored on the computer to any machine with similar software and protocol. Examples include BitTorrent, Shareaza and uTorrent.

Performance Goals

Performance Goal is the desired result(s) of implementing the security objective or technique that are measured by the metric.

Performance Measures

Performance Measures are the actions required to accomplish the performance goal validated through the completion and analysis of the institution report.

Personal Travel

Travel by a Covered Individual that is travelling for personal reasons and who (i) is not receiving any support for their travel from any person or organization, (ii) is not receiving any compensation from AU or any other person or organization during their travel, (iii) is not traveling with an AU device, and (iv) is not traveling with AU sensitive data.

Personally Identifiable Information (PII)

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. (Source: OMB Memorandum M-07-1616)
Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's family name, etc.). (Source: SP 800-53 Rev. 4)
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (Source: OMB Circular A-130)

The term personally identifiable does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Personally Owned Device (POD)

Refers to employees taking their own personal device to work to interface to the USG organization's network resources.

Phishing:

Phishing is a cyberattack technique in which malicious actors use deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal identification. These deceptive communications often appear to be from legitimate sources, such as banks, social media platforms, or trusted organizations, but are designed to steal valuable data or deliver malware. Phishing attacks commonly involve tactics such as creating fake login pages to capture credentials, urging recipients to click on malicious links, or enticing them to download infected attachments. Phishing exploits human psychology by relying on urgency, fear, curiosity, or offers that seem too good to be true to manipulate recipients into taking actions that compromise their security.

Policy

Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component. (Source: SP 800-95)

Port scanning

Port scanning is the practice of systematically scanning a computer system, network, or device to identify open ports and services available for communication. Ports are numbered endpoints on a computer's networked devices where specific services or applications listen for incoming connections.

Port scanning tools are used by security professionals, administrators, and hackers to assess the security posture of a system. By identifying open ports, an attacker can determine potential entry points for unauthorized access or vulnerabilities that might be exploited. Conversely, administrators use port scanning to identify and address security weaknesses, ensure compliance, and maintain a secure network environment.

Principle of Least Function

The principle of least function or functionality provides that information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that information system.

Principle of Least Privilege

The Principle of Least Privilege (PoLP) describes minimal user profile or access privileges to information resources based on allowing access to only what is necessary for the users to successfully perform their job requirements. (Source: SP 800-179)

Privacy Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other-than authorized purpose. (OMB M-17-12)

Privacy Risk

The likelihood that individuals will experience problems resulting from data processing and the impact should they occur. (NIST PF)

Privacy Risk Assessment

A risk management sub-process specifically for identifying and evaluating privacy risk concerns.

Problematic Data Actions

A data action that could cause an adverse effect for individuals.

Program

A group of related projects (and services) managed in a coordinated way to obtain benefits and control not available from managing them individually.

Project

A temporary endeavor undertaken to create a unique product, service, or result.

Project Risk

An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.

Protected Health Information (PHI) / Electronic Protected Health Information (ePHI)

PHI / ePHI means individually identifiable health information that is:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:
(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
(iii) In employment records held by a covered entity in its role as employer; and
(iv) Regarding a person who has been deceased for more than 50 years.

See the Health Insurance Portability and Accountability Act of 1996 privacy regulations, ("HIPAA"), as amended.

Provisioning

The process of preparing systems/products/services to permit and provide for new services to its end-users.

Public Data/Information

Data elements that have no access restrictions and are available to the public. Also, can be designated as unrestricted data.

RAARe – Full

A form submitted to a vendor designed to collect information about the security controls built into the technology in use or planned to be used by the department/ institution.

RAARe – Triage

A form submitted to a department designed to collect information about the security controls built into the technology in use or planned to be used in a department.

Reconnaissance

Activity that attempts to gather information about information systems and network architecture and activity.

Remote Access

Using any device, regardless of ownership, to access Augusta University information or information systems from outside the enterprise network. Examples would include virtual private network (VPN), email access offsite, Citrix web access offsite, etc.

Remote Wipe

Remote wipe, as per the National Institute of Standards and Technology (NIST), refers to the process of remotely erasing data stored on a mobile device or computer. This action is typically initiated by an authorized administrator or owner in response to specific circumstances, such as the loss, theft, or unauthorized access to the device. Remote wipe functionality helps protect sensitive information by swiftly and effectively removing data from the device, reducing the risk of data breaches or unauthorized access. This action can be particularly crucial in maintaining data confidentiality and preventing potential exposure of sensitive data when devices are compromised or no longer in the owner's control.

Removable Media

CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices, and copiers.

Research Health Information (RHI)

Research health information" refers to data, records, and knowledge collected and analyzed for the purpose of advancing medical knowledge, healthcare practices, and scientific understanding. This type of information is often gathered through systematic investigations, studies, experiments, and observations in the field of health and medicine that are not involve a Covered Transaction. Research health information encompasses a wide range of topics, including disease mechanisms, treatment effectiveness, patient outcomes, medical technologies, and public health trends. It plays a vital role in shaping evidence-based medical practices, developing new therapies, and improving healthcare delivery for the benefit of individuals and society as a whole.

Individual health information that (1) is created or received in connection with research that does not involve a Covered Transaction or (2) although previously consider PHI, has been received in connection with research pursuant to a valid HIPAA authorization or IRB waiver of authorization.

Risk

The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, financial NPI, protected cardholder data, and student education records (and other confidential or proprietary electronic information, and other system assets).

Risk Assessment / Risk Analysis

Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place; Prioritizes risks; and Results in recommended actions/controls that could reduce or offset the determined risk.

Risk Management

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (FIPS 200)

Risk Mitigation

Risk mitigation" refers to the strategic process of identifying, assessing, and implementing measures to reduce or minimize the potential negative impact of risks on an organization's objectives, assets, projects, or operations. It involves taking proactive steps to manage identified risks, enhancing their visibility and controllability. Risk mitigation strategies can vary and might involve implementing safeguards, controls, best practices, policies, and procedures to lessen the likelihood or severity of adverse events. The goal of risk mitigation is to enhance an organization's resilience by effectively managing and limiting the impact of potential threats and vulnerabilities. Risk Mitigation is referred to as Risk Management in the HIPAA Security Rule.

Risk Monitoring

Risk monitoring involves the systematic and continuous process of observing, evaluating, and tracking potential risks and uncertainties within an organization's operational environment. This ongoing practice includes collecting and analyzing data, assessing risk levels, and identifying any shifts or changes that might impact the organization's objectives, projects, assets, or operations. Risk monitoring enables timely detection of emerging threats, assessment of risk factors' evolution, and the identification of patterns or trends that could affect the organization's overall risk profile. This process aids in informed decision-making, allowing proactive adjustments to risk mitigation strategies and the implementation of necessary measures to address changing risk scenarios.

Risk Remediation

See Risk Mitigation

Risk Tolerance

The level of risk or degree of uncertainty that is acceptable to organizations. (NIST SP 800-39)

Role-Based Access (Need to Know)

Workforce members, contractors, vendors and/or agents' access to information must be based on their job duties/assigned roles.

Rooting or Jailbreaking

"Rooting" (for Android devices) and "jailbreaking" (for iOS devices) refer to the process of removing or bypassing the restrictions imposed by the operating system, allowing users to gain privileged access and control over their devices beyond what is typically permitted.

Rooting Android devices involves obtaining "root" access, which is the highest level of administrative control, enabling users to modify system files, install custom software, and make changes that are otherwise restricted by the manufacturer or carrier.

Jailbreaking iOS devices involves removing the limitations imposed by Apple's operating system, granting users the ability to install unauthorized apps, customize the device's appearance, and access system files that are normally hidden.

RSA

See Encryption

Safeguards

The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security and security of physical structures, areas and devices. Synonymous with security controls and countermeasures. (Source: FIPS 200)

Schedule

The planned dates for performing schedule activities and the planned dates for meeting the schedule milestones.

Scope

The work that needs to be accomplished to deliver a product, service, or result with the specified features and functions.

Security Authority (SA)

A Security Authority is a designated person within each department who is responsible for submitting requests on behalf of AU Community members within their department to access AU information systems.

Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration or destruction will cause perceivable damage to the USG organization. Example: personally identifiable information, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA) data, or data exempt from the Georgia Open Records Act. (Source: SP 800-53 Rev. 4)

Sensitive Electronic Information / Sensitive Data

Sensitive information refers to data that pertains to an identified or identifiable individual or entity, and possesses a confidential, proprietary, or sensitive nature, such that its unauthorized access, use, disclosure, alteration, or loss, whether internal or external to the respective organization (such as AU or AU Health), may result in harm to the individual or entity. This category encompasses a range of data, including but not limited to Confidential Information, Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry (PCI) data, undisclosed financial statements, audit reports, and any other data subject to applicable federal, state, and local laws, regulations, industry standards (like HIPAA, HITECH, PCI-DSS), as well as specific legal exceptions (e.g., Exception 25 of the Georgia Sunshine Act) or provisions (such as the Georgia Open Records Act O.C.G.A. § 50-18-70 et seq). This information requires specific authorization for access due to the potential harm resulting from its unauthorized disclosure, alteration, or destruction, and is safeguarded to prevent perceivable damage to the organization to which it belongs.

Server

A server is a specialized computer or software application that provides services, resources, or data to other computers, devices, or clients over a network. Servers are designed to respond to requests from clients, which can include other computers, applications, or users, by delivering the requested information or performing specific tasks.

Service Account

A service account is a special type of user account used by software applications, processes, or services to interact with other resources, systems, or networks. Service accounts are distinct from regular user accounts and are created specifically to facilitate the execution of tasks, services, or applications without requiring human interaction.

Simple Mail Transfer Protocol (SMTP)

SMTP is a widely used network protocol for sending and routing email messages between servers and email clients. It's a crucial component of the email communication process, responsible for delivering outgoing emails from the sender's email client to the recipient's email server. It operates on a client-server model. When an email is sent, the sender's email client communicates with their outgoing mail server using SMTP. The server then relays the email to the recipient's mail server using the same protocol. The recipient's email client later retrieves the email from the server using protocols like POP3 or IMAP. Furthermore, it defines the rules and procedures for formatting and transmitting email messages, including addressing, message headers, and attachment handling.

Smart Phone

A mobile communication device that combines the functionalities of a traditional cellular phone with advanced computing capabilities, such as internet access, email, messaging, multimedia playback, photography, and application support. They typically feature touchscreens for intuitive user interaction and run operating systems that allow users to install and run various applications and provide connectivity through cellular networks, Wi-Fi, and Bluetooth wireless communications.

Spam

Irrelevant, unsolicited, undesired, or inappropriate messages sent on the Internet to many recipients. The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (Source: SP 800-53 Rev. 4)

Spillage

Cybersecurity incident that resulted in the transfer of protected information (classified or CUI) onto an information system or directly to a person not authorized as the recipient. (Source: CNSSI-4009)

Split Domain Name Service (DNS)

Split DNS is a network architectural design configuration where a single domain's DNS information is configured to resolve to different IP addresses based on the location or network segment of the requesting device. This is achieved by maintaining separate DNS records for the same domain within different DNS servers or zones. For example, a split DNS arrangement might supply private network answers to private users while providing different answers to public users. Internal hosts are directed to an internal domain name server for name resolution, while external hosts are directed to an external domain name server for name resolution

Split-tunneling

A network configuration technique allows a device or user to divide its traffic into two categories such that some of their internet traffic goes through an encrypted Virtual Private Network (VPN) tunnel while sending other traffic directly to the regular internet connection without passing through the VPN. This can offer benefits such as improved performance for non-sensitive activities, reduced load on the VPN server, and access to local resources while connected to the VPN.

Standard

A standard is a requirement that: 1) supports a policy; and 2) provides for common and repeatable use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in each context. (Source: NISTIR 8074 Vol. 2)

Student Education Records

Student Education Records, as defined by the Family Educational Rights and Privacy Act (FERPA), are any records that are directly related to a student and maintained by an educational institution or an educational agency. These records can be in any format, including paper, electronic, or digital, and encompass information that is personally identifiable to the student. Examples of student education records covered by FERPA include academic transcripts, grades, class schedules, enrollment information, disciplinary records, and any other records used for educational purposes. FERPA grants eligible students certain rights regarding their education records, including the right to review, request corrections, and control the release of their records.

Suspicious Activity

Anomalous activity that requires further investigation.

System Administrator

A System Administrator is an IT professional responsible for managing, configuring, and maintaining computer systems, networks, servers, and software within an organization. Their role involves tasks such as installing and upgrading software, managing user accounts and permissions, monitoring system performance, troubleshooting technical issues, ensuring data backup and recovery, and implementing security measures to safeguard against unauthorized access and cyber threats.

System or Application Event

Activity that occurs in the operation system or in a software application, which may or may not require action.

System Owner

A person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. (Source: SP 800-161)

The National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness. NIST's activities are organized into physical science laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

Threat

The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as the following:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.

- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, power outages, hazardous material spills, etc.

- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc.

- Other – explosions, medical emergencies, misuse or resources, etc.

Reference Adversarial Threat.

Threat Action

Reference Attack

Threat Agents

Persons, methods, operations, techniques, systems, or entities that act – or may have the potential to act – to initiate, transport, carry-out, or in any way support a particular threat exploit.

Threat Source

Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental, which can impact the organization’s ability to protect ePHI, financial NPI, protected cardholder data, and student education records.

Traceable

Information that is sufficient to decide about a specific aspect of an individual’s activities or status.

Training

Activity involving learning or accessing knowledgebases or resources to improve a skill or behavior.

Transition Period

A period whereby an object moves from one state or level to another.

Transport Layer Security (TLS)

TLS, or Transport Layer Security, is a cryptographic protocol used to establish a secure and encrypted communication channel between two computer systems over a network. It ensures the privacy, integrity, and authenticity of data exchanged between these systems, typically in applications such as web browsing, email, and messaging.

TLS operates by using a combination of encryption algorithms and digital certificates to protect the data during transmission. It prevents unauthorized parties from intercepting and reading the information being exchanged, thereby enhancing the security of online communications and transactions. TLS is commonly used to secure sensitive information like login credentials, credit card details, and personal data, providing a crucial layer of protection in modern internet communication.

Truncated Alert

A truncated alert is an alert or notification that has been shortened or cut off, often due to limitations in the display area or communication medium.

Uninterruptible Power Supply (UPS)

An Uninterruptible Power Supply (UPS) is an electrical device designed to provide temporary power during electrical outages or fluctuations in the main power supply. UPS systems include a battery that stores energy, allowing connected devices to continue operating for a limited time when the main power source is interrupted. This provides critical time for proper shutdown procedures, preventing data loss and potential damage to electronic equipment. UPS units are commonly used to protect sensitive devices such as computers, servers, networking equipment, and other electronics from power-related disruptions and ensuring uninterrupted operation in scenarios like power failures, surges, sags, or voltage fluctuations.

User / End Users

Users are individuals who use the information processed by an information system. (Source: FIPS 200). Also See Authorized User

User Identifier (ID)

A unique alphanumeric identifier assigned to an individual user or account within a computer system, application, or network. It serves as a way to distinguish and authenticate users, granting them access to specific resources or functionalities based on their assigned permissions and privileges. User IDs are commonly used in various contexts, such as logging into operating systems, applications, websites, or databases, helping to ensure secure and controlled access while maintaining accountability for user actions.

Vulnerability

A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Web publisher:

Someone who uploads, creates, or edits content on web pages; one who maintains or manages a website.

Workforce

Workforce means employees, students, volunteers, contracted personnel, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the covered entity or business associate.

Workstation

See Endpoint

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network and may consume computer resources destructively. (Source: SP 800-82 Rev. 2)

Section Control

Table 1: Revision History

Date	Description of Change
7/14/2023	Initial Redesign – Referenced in a new structure and format. PDF, structure and format
9/28/2023	Compiled document supersedes previously published Information Security Program Policy

Table 2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Review Date
1.0	Cybersecurity Charter	8/29/2023	11/1/2023	11/1/2028
1.1	Cybersecurity Program	8/29/2023	11/1/2023	11/1/2028
1.2	Appropriate Usage Standard	5/20/2022	5/20/2022	5/20/2027
1.3	Cybersecurity Incident Management	6/2/2021	6/2/2021	6/2/2024
1.4	Information Asset Management and Protection	TBD	TBD	TBD
1.5	Risk Management	TBD	TBD	TBD
1.6	Information System Categorization	TBD	TBD	TBD
1.7	Classification of Information	TBD	TBD	TBD
1.8	Endpoint Management	TBD	TBD	TBD
1.9	Cybersecurity Awareness, Training, and Education	TBD	TBD	TBD
1.10	Required Reporting	TBD	TBD	TBD
1.11	Open	N/A	N/A	N/A
1.12	Password Management	TBD	TBD	TBD
1.13	Domain Name System Management	TBD	TBD	TBD
1.14	Information Protection Management	TBD	TBD	TBD
1.15	Email Use and Protection	5/20/2022	5/20/2022	5/20/2027

Table 2: Appendices

Appendix Reference	Section Name	Compilation Date	Published Date	Review Date
A	References	8/29/2023	11/1/2023	11/1/2028
B	Glossary	8/29/2023	11/1/2023	11/1/2028

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/14/2024

President, Augusta University Date: 5/14/2024