Augusta University
Policy Library

Cybersecurity Risk Management Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

It is the policy of Augusta University (AU) to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, availability of its electronic protected health information (ePHI), protected cardholder data, financial nonpublic personal information (NPI), and student education records (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's Cybersecurity program.

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:

DEFINITIONS

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Cybersecurity Governance, Risk Management, & Compliance (GRC) Team: Individuals who are knowledgeable about the organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, technical security controls, and who are responsible for the Cybersecurity risk management process and procedures outlined below. This team manages responsibilities for Cybersecurity risk management processes and procedures with the following offices: Cybersecurity, Public Safety, Enterprise Privacy, Legal, HR, Communications, Compliance and Enterprise Risk Management, Internal audit, Information Technology Services, and Security/Technology subject matter experts.

Cybersecurity Risk Management: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

NPI (nonpublic personal information): (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.

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

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.

RAARe – Triage: This form is to be completed by the department. Is a security questionnaire/ form used to collect information on technology in use or planned to be used in a department.

RAARe – Full: This form is to be completed by the vendor. The intention of this questionnaire/ form is to collect information about the security controls built into the technology in use or planned to be used by the department/ institution.

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: (Referred to as Risk Analysis in the HIPAA Security Rule); the
process:

> 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 possible actions/controls that could reduce or offset the determined risk.

Risk Mitigation: Referred to as Risk Management in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

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

- 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, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc.
- and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

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.

Threat Action – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

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.

RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Manage the Cybersecurity Risk Management program and coordinate the development and maintenance of Cybersecurity Risk Management policies, procedures, and standards.
- Ownership of risk register.

Executive Senior Leadership

- Participate in the Cybersecurity Risk Management program, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and implementation of risk treatment plan.
- Consider and jointly accept residual risk and Cybersecurity policy exceptions with AU Chief Information Officer where assessed risk level is medium or high.

Administrative and Faculty and Staff

- Collaborate with the CISO to complete Cybersecurity risk assessments.
- Develop and implement a risk treatment plan.
- Report updates on the risk treatment plan to the CISO or designate.
- Submit exceptions to the Cybersecurity Policy and work with University Cybersecurity through the exceptions process.

Cybersecurity Governance, Risk Management and Compliance (GRC) Team

- Schedule and prioritize Cybersecurity risk assessments.
- Request from administrative and collegiate faculty and staff information related to their collection and use of private data
- Conduct Cybersecurity risk assessments.
- Process and follow up on requested exceptions to the Cybersecurity policy.

PROCESS & PROCEDURES

This policy establishes the scope, objectives, and procedures of AU's information security risk management process. The Cybersecurity risk management process is intended to support and protect the organization and its ability to fulfill its mission. Cybersecurity risk analysis and risk management are recognized as important components of AU's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the

HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8), the Privacy Rule (16 C.F.R. Part 313) and are in compliance with the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) as well as PCI Data Security Standard version 3.2.1 (PCI DSS).

Risk assessments are done throughout IT system life cycles:

- Before the purchase or integration of new technologies and changes are made to physical safeguards;
- While integrating technology and making physical security changes; and
- While sustaining and monitoring of appropriate security controls.

AU performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI, financial NPI, protected cardholder data, and student education records.

AU implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

- Ensure the confidentiality, integrity, and availability of all ePHI, financial NPI, protected cardholder data, and student education records the organization creates, receives, maintains, and/or transmits,
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, financial NPI, protected cardholder data, and student education records,
- Protect against any reasonably anticipated uses or disclosures of ePHI, financial NPI, protected cardholder data, and student education records that are not permitted or required, and
- Ensure compliance by workforce.

Any risk remaining (residual) after other risk controls have been applied requires approval by Executive Senior Leadership and will be recorded by the organization’s Cybersecurity GRC Team. Clinical and Information Technology Services Management will be designated as additional approvers of residual risk that is associated with their respective areas.

All Cybersecurity risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for seven years.

Responsibility: The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of AU’s Information Security Officer (or other designated employee), and the Cybersecurity GRC Team.

For software and hardware security risk assessments, the entity or department who owns the technology in use are responsible for collecting and submitting information for security review.

The RAARe – Triage must be submitted by the requesting department to cybersecurity GRC to begin the vendor security review process. *Security Review of the Triage will determine any additional information that will be required.*

Risk Assessment: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

1. **System Characterization**
    - The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI, financial NPI, protected cardholder data, and student education records are created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).
    - *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries. Endpoints and data is discovered and inventoried.

2. **Threat Identification**
    - In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
    - *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

3. **Vulnerability Identification**
    - The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
    - *Output* – A list of the vulnerabilities (observations) that could be exercised by the potential threat-sources.

4. **Control Analysis**
    - The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat source exploiting a system vulnerability.

- Output – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

5. **Likelihood Determination**
   - The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
   - *Output* – Quantitative ranking of likelihood.

6. **Impact Analysis**
   - The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
   - *Output* –Documented description of impact.

7. **Risk Determination**
   - This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
   - *Output* – Quantitative ranking of Risk.

8. **Control Recommendations**
   - The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
   - *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

9. **Results Documentation**
   - Results of the risk assessment are documented in an official report or briefing and provided to senior management to make decisions on policy, procedure, budget, and system operational and management changes.
   - Output – The risk register is the source of record for risk management activities at AU.

Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI, financial NPI, protected cardholder data, and student education records. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

1. **Prioritize Actions**
   - Using results from Risk Determination of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.
   - *Output* – Actions ranked from high to low

2. **Evaluate Recommended Control Options**
   - Although possible controls for each threat and vulnerability pair are arrived at in Control Recommendations of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
   - *Output* – list of feasible controls

3. **Conduct Cost-Benefit Analysis**
   - Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
   - *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific control

4. **Select Control(s)**
   - Taking into account the information and results from previous steps, AU’s mission, and other important criteria, the Cybersecurity GRC Team, in cooperation with senior leadership to included but not limited to the Chief Information Officer, determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI, financial NPI, protected cardholder data, and student education records. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
   - *Output* – Selected control(s)

5. **Assign Responsibility**
   - Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step and assign their responsibilities. Also, identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

- *Output* – List of resources, responsible persons and their assignments

6. **Develop Plan of Action and Milestone (POA&M)**
   - Develop an overall implementation program and individual project plans needed to implement the safeguards and controls identified. The POA&M should contain the following information as appropriate:
     - Each risk or vulnerability/threat pair and risk level
     - Prioritized actions
     - The recommended feasible control(s) for each identified risk
     - Required resources for implementation of selected controls
     - Team member responsible for implementation of each control
     - Start date for implementation
     - Target date for completion of implementation
     - Requirements.

     The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).

     Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.
   - *Output* – Project Plans for selected safeguards

7. **Implement Selected Controls**
   - As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk. Continually and consistently, communicate expectations to Cybersecurity GRC Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

     Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes. If risk reduction expectations are not met, then repeat all or a part of the Cybersecurity risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

- *Output* – Residual Risk

8. **Cybersecurity Risk Management Schedule:** The two principle components of the Cybersecurity risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of AU's Cybersecurity program:

   Scheduled Basis – an overall risk assessment of AU's information system infrastructure will be conducted at least annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process. The Cybersecurity GRC Team must communicate and collaborate with USG's Enterprise Risk Management coordinator at least annually.

   Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.

   As Needed – the Security Officer (or other designated employee) or Cybersecurity GRC Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect AU's information systems.

REFERENCES & SUPPORTING DOCUMENTS

Cybersecurity Risk Management Procedure
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
Privacy and Security regulations
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended (including the Breach Notification Rule)
PCI Data Security Standard version 3.2.1 (PCI DSS)
Privacy Rule (16 C.F.R. Part 313)
USG IT Handbook

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

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

President, Augusta University Date: 6/2/2021