[Insert Company Name and Logo]	
Title: Information Security Risk Management	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy establishes the scope, objectives, and procedures of [Insert Company name] information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

Scope: The policy covers the administrative, physical, and technical processes that enable and govern sensitive and regulated data created, maintained, received, or transmitted by the organization.

Definitions:

1. Risk: The probability that the confidentiality, availability, and integrity of sensitive and regulated data, other proprietary electronic information, and other system assets will be affected by a threat or vulnerability. Per NIST SP 800-30 definitions of low, moderate, and high risk are:
    a. High risk- "means that a threat event could be expected to have a **severe or catastrophic** adverse effect on the organizational operations, organizational assets, individuals, other organizations, or the Nation."
    b. Moderate risk- "means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations or the Nation."
    c. Low risk- "means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation."
2. Risk Management Team: Individuals who are knowledgeable about [Insert Company name] cybersecurity policies, procedures, training programs, computer systems, and technical security controls are integral in informing the risk management process and procedures outlined below. This team is generally comprised of the Risk Manager, Privacy Officer, Security Officer, Systems Analyst(s), Compliance Officer, and Security/Technology subject matter experts. These roles may be filled by one or two people in a smaller organization.
3. Risk Assessment: A process which (according to the U.S. HIPAA Security Rule:
    a. Identifies the risks to confidentiality, availability, and integrity of sensitive and regulated data, determines the probability of occurrence, and the resulting impact for each threat/vulnerability pair identified given the security controls in place.
    b. Prioritizes risks.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

c. Results in recommended actions or controls that could offset or mitigate, the determined risk.

4. Risk Management: Within this policy, it refers to a process comprised of risk assessment and risk mitigation, which is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).
5. Risk Mitigation: A process that evaluates, prioritizes, and implements controls that will reduce or offset the risks determined in the risk assessment process to acceptable levels within an organization given its mission and available resources.
6. Threat: the potential for a particular threat-source to successfully exploit a particular vulnerability. Threats are commonly categorized as:
    a. Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
    b. Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
    c. Natural – fires, floods, electrical storms, tornados, etc.
    d. Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
    e. Other – explosions, medical emergencies, misuse of resources, etc.
7. Threat Source: Any circumstance or event with the potential to cause harm, whether intentional or unintentional, to an IT system. See above for common threat sources.
8. 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, possibly resulting in a security breach or violation of policy.

Policy:

1. It is the policy of [Insert Company name] to conduct thorough and timely risk assessments of potential threats to the confidentiality, integrity, and availability of Personally Identifiable Information (PII).
2. …to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's information security program.
3. Risk management is recognized as an important component of [Insert Company name] compliance program and Information Technology (IT) security program.
    a. [Insert Company name] 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 PHI.
4. [Insert Company name] implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
    a. Ensure the confidentiality, integrity, and availability of all sensitive and regulated data the organization creates, receives, maintains, and/or transmits.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of sensitive and regulated data.
c. Protect against any reasonably anticipated uses or disclosures of sensitive and regulated data that are not permitted or required.
d. Ensure compliance by workforce.

5. All documentation of risk management efforts, including decisions made on controls to implement as well as those to not implement, are documented and maintained for six years.

Procedure:

1. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of [Insert Company name] Security Officer or designee, and the identified Risk Management Team.
2. 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.
    a. Step 1. System Characterization
        i. Start by identifying where data is created, maintained, processed, received, or transmitted. Take into consideration policies, laws, the remote workforce and telecommuters, and removable media and portable computing devices.
    b. Step 2. Threat Identification
        i. Consider all potential threat-sources through the review of historical incidents and data from outside sources, such as intelligence agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its needs.
        ii. A threat statement containing a list of threat-sources that could exploit system vulnerabilities should be created.
    c. Step 3. Vulnerability Identification
        i. Next, develop a list of technical and non-technical system vulnerabilities which may be exploited or triggered by potential threat-sources. Vulnerabilities can include incomplete or conflicting policies that govern an organization's computer usage, insufficient safeguards to protect facilities that house computer equipment, or any number of software, hardware, or other deficiencies that comprise an organization's computer network.
        ii. The list of the system vulnerabilities that could be exercised by the potential threat-sources should be documented.
    d. Step 4. Control Analysis

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

i. Evaluate and document the effectiveness of technical and non-technical controls that have been or may be implemented by the organization to minimize or eliminate the likelihood or probability of a threat-source exploiting a vulnerability.
ii. A list of current or planned controls, such as policies, procedures, training, technical mechanisms, insurance, etc., used to mitigate the likelihood of a vulnerability being exploited and reduce the negative impact should be created.

e. Step 5. Likelihood Determination
   i. Determine the overall likelihood rating for the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
   ii. Create a document with different likelihood ratings of low (.1), moderate (.5), or high (1) for each vulnerability.

f. Step 6. Impact Analysis
   i. 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, costs associated, loss of confidentiality, integrity, and availability of systems and data.
   ii. Document the magnitude of impact ratings of low (10), moderate (50), or high (100) for each vulnerability.

g. Step 7. Risk Determination
   i. Multiply the ratings from the likelihood determination and the ratings from the impact analysis to obtain the risk level for each vulnerability. 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 provides a list that senior management can work from for each risk level.
   ii. Document the risk level of low (1-10), moderate (>10-50) or high (>50-100).

h. Step 8. Control Recommendations
   i. Work 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, legislation and regulation, organizational policy, operational impact, and safety and reliability. These control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

ii. Create a document that recommends controls and alternative solutions to mitigate risk.

i. Step 9. Results Documentation
   i. The results of the risk assessment should be 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.
   ii. Produce a risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

3. Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the above risk assessment process to ensure the confidentiality, integrity, and availability of sensitive and regulated data. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.
   a. Step 1. Prioritize Actions
      i. Using the results from Step 7 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 requiring the most immediate attention and top priority in allocating resources.
      ii. Create a document for actions ranked from high to low.
   b. Step 2. Evaluate Recommended Control Options
      i. Taking the possible controls for each threat and vulnerability pair in Step 8 of the Risk Assessment, review the recommended controls and alternative solutions for reasonableness and appropriateness. The feasibility and effectiveness of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.
      ii. Create a document with the list of feasible controls. This differs from the list of all possible controls in that the organization will likely implement these.
   c. Step 3. Conduct Cost-Benefit Analysis
      i. Determine the extent to which a control is cost-effective by comparing the benefit of applying a control with its cost of application. Controls that are considered not cost-effective are also identified and documented during this step. By prioritizing across all controls being considered, this step can greatly aid in the decision-making process.
      ii. Document the cost-benefit analysis of either implementing or not implementing each specific control. Remember, the potential cost for a

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

breach can be rather steep, so any controls used may be much more cost-effective over the whole scheme of things.

d. Step 4. Select Control(s)
    i. Considering the information and results from previous steps, the mission, and other important criteria, the Risk Management Team should determine the best controls to implement for reducing risks. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
    ii. Selected controls should be documented.
e. Step 5. Assign Responsibility
    i. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step and assign responsibilities. Also identify the equipment, training, and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, manpower, etc.
    ii. Create a list of resources, responsible persons, and their assignments.
f. Step 6. Develop a Safeguard Implementation Plan
    i. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
        1. Each risk or vulnerability/threat pair and risk level.
        2. Prioritized actions.
        3. The recommended feasible control(s) for each identified risk.
        4. Required resources for implementation of selected controls.
        5. Team member responsible for implementation of each control.
        6. Start date for implementation.
        7. Target date for completion of implementation.
        8. Maintenance requirements.
    ii. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements, 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 management team.
    iii. Individual project plans for the implementation of safeguards may be developed and contain detailed steps to meet timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope and requirements, a list of deliverables, key assumptions, objectives, and task completion.
    iv. Create a document for the Safeguard Implementation Plan.
g. Step 7. Implement Selected Controls

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

i. As controls are implemented, be sure to 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.
ii. Continually and consistently communicate expectations and results to the required people, such as management, throughout the risk mitigation process. Document when new risks are identified and when controls lower or offset risk rather than eliminate it.
iii. Continued monitoring is especially crucial during times of major changes.
iv. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

i. Create a document describing Residual Risk. This may be acceptable risk based on the determination of management that the controls are not reasonable, or it might be risk that has not been mitigated yet, but the plan is to implement controls within a specified timeframe.
    1. Any residual risk remaining after controls have been applied requires signoff by the Security and Privacy Officers or designees.

4. The risk assessment and risk mitigation will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement:
    a. Scheduled Basis – an overall risk assessment of [Insert Company name] infrastructure will be conducted annually (optionally, every two years, but no more than three years.). 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.
    b. 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.
    c. As Needed – the Security Officer or designee or Risk Management 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 [Insert Company name] information systems.

Violations:
Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Attachments: None

Related Policies: Network Security Continuous Monitoring

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.