Course Final - NIST Cybersecurity Policies and Standards

Austin Rocks

DeVry University

SEC 310: Principles and Theory of Security Management

Professor Ronald Baugh

04/20/24

**Security Awareness and Training Policy**

The Security Awareness and Training Policy in the NIST functions to Identify and Protect and the sub-categories Asset Management and Awareness and Training.

The University of Arizona (UA), part of the education sector, implemented this policy to raise awareness about information security among its faculty, staff, and students. It is crucial that UA operates within the CIA Triad, which ensures confidentiality, integrity, and availability of information. Based on its policy, UA is committed to creating a culture of security awareness and responsible information-handling practices tailored to meet their unique needs. All individuals are held accountable when accessing the university's sensitive information, computers, and systems. To ensure the policy is understood, annual training is provided to the university personnel. The training ensures all personnel are trained and knowledgeable within their roles and responsibilities concerning information security. All personnel must take the Employee and DCC Security Awareness Training and Role-Based Security Awareness Training, which teaches employees cybersecurity best practices, data protection, and common cyber threats. According to UA, the policy must be evaluated annually to remain current. However, I recommended conducting the review quarterly or bi-quarterly. The cyber landscape is changing rapidly, and threat actors are evolving; it is crucial for organizations to consistently review these policies to ensure that they stay ahead of potential risks.

**Contingency Planning Policy**

The Contingency Planning Policy is implemented for the NIST function Recover and the

sub-categories Recovery Planning and Improvements.

UA uses a Contingency Planning Policy to safeguard the university's information systems; the policy creates a structured approach to contingency planning. Having a detailed framework when responding to security incidents helps reduce the attack's severity while keeping operations running. Information owners and system owners are held accountable for implementing the policy. The personnel are responsible for ensuring their systems meet the requirements discussed in the policy. By following this policy, UA can maintain its operational effectiveness and ensure the security of its information systems. According to the contingency plan page, the Information Security Officer (ISO) must develop, test, maintain, and communicate the university's information security posture to leadership. According to NIST control 4, the plans must maintain their business functions regardless of system disruption, compromise, or failure. On UA’s contingency plan, the Chief Information Security Officer (CISO) is allowed exceptions for disconnecting affected individuals or units from their network, which allows the vulnerability to be isolated from the rest of their systems.

**Risk Assessment Policy**

The Risk Assessment policy is implemented for the NIST function Identify and the sub-category Risk Management Strategy.

Fordham University, part of the education sector, implemented a Risk Assessment Policy to proactively mitigate potential vulnerabilities by conducting periodic assessments. Based on the policy they implemented, the University can leverage its structured assessment framework and continue to preserve its reputation by protecting the students, employees, and information assets. The policy is designed to ensure compliance with federal and state laws that safeguard and keep the University's resources confidential. This policy also makes decision-making regarding risk management more manageable by providing staff training and knowledge of potential risks in the cyber landscape. The policy at Fordham University is customized to focus on the University's IT resources. The policy discusses the importance of keeping information confidential and ensuring data integrity, and the University's policy differs from that of large corporations. The University focuses on legal and operational requirements that protect students, staff, and information and remain a significant focus in their day-to-day activities. Another customization the University made is the disclaimer statement, which includes the details the school covered to fit the overall structure of the University. They focus on working hand in hand with information security and assurance to ensure proper risk analysis, the findings are well documented, and they may even require presentations to authorized personnel.

The senior director of IT security and assurance is responsible for conducting periodic risk assessments to ensure no risks and compliance with the policy. Fordham requires formal Information Security Risk Management (ISRM) programs to identify and mitigate potential risks by having security professionals periodically conduct evaluations, which allows potential risks to be found and mitigated and ensures that the ISRM has adequate management and the policies are followed and maintained. Another example I read about was the Risk assessment process; they conduct the assessment to estimate the likelihood and potential impacts of the risks. Periodic assessments enable the University to identify and address high-risk vulnerabilities, which mitigates the possibility of unauthorized access and ensures compliance by conducting assessments using specific processes. The findings of the assessments are well-documented and may be presented to authorized personnel to ensure transparency and accountability.

**Access Control Policy**

The Access Control Policy is implemented for the NIST functions Identify and Protect and the sub-categories Asset Management, Identify Management and Access Control, Data Security, Information Protection Processes and Procedures, and Protective Technology.

The Access Control Policy and Procedures of the State of Maine are measures designed to ensure access controls are implemented and maintained to safeguard Executive branch assets, locations, and other state governments. The policy has been put in place to protect the state's information assets, and its implementation is the responsibility of various individuals and organizations. Among these are the CISO, who owns and enforces the policy, and the Department of Administration and Financial Services Bureau of Human Resources, which oversees the review of requests from state employees for out-of-state remote access. In addition to state employees, contractors must abide by all federal and state regulations and guidelines put out by the Office of IT. Failure to comply with the policy can result in disciplinary actions, including termination of employment. Non-state employees and contractors who fail to adhere to the policy may be denied access to Maine's data or systems. The Access Control Policy of the State of Maine was last updated on July 6, 2023, and is reviewed annually. Given the increasing number of internal security attacks and cyber threats targeting government agencies and organizations, it is recommended that the policy be reviewed and modified more frequently than once annually. There were around 2,000 internal security attacks daily by May 2023; this number of cyberattacks continues to rise daily. Reviewing the policy frequently could mitigate the risks associated with such attacks and protect Maine's information assets.

**Vulnerability Scanning Standard**

The Vulnerability Scanning Standard is implemented for the NIST function Detect, and the sub-categories are Anomalies and Events and Security Continuous Monitoring.

The University of Wisconsin has established a Vulnerability Scanning policy, which explains the minimum requirements for vulnerability management and scanning of the systems owned by the University. The Associate Vice President of Information Security oversees the policy, and system administrators are responsible for performing remedial action for detected vulnerabilities. The National Institute of Standards and Technology (NIST) provides a template that offers guidance on how often scans should be conducted. The University of Wisconsin has customized this template to fit their risk profile. This customization aligns with the organization’s risk management strategy and ensures that proper resources are available for assets with higher exposure risks. The remediation timeline specifies different timelines based on the severity ratings of the organization. This customization allows UW to prioritize its patching efforts based on the severity of the vulnerabilities. To ensure compliance with this policy, roles are clearly defined and assigned to different roles within the organization. UW conducts regular audits, assessments, and documentation to review the findings. This makes UW aware of risks and ensures compliance with its policy.

**Encryption Standard**

The Encryption Standard is implemented for the NIST function Protect and Detect, and the sub-categories are Data Security, Information Protection Processes and Procedures, Protective Technology, and Security Continuous Monitoring.

The University of Texas at Austin’s encryption standard policy, which belongs to the education sector, ensures that sensitive information relating to the university is handled securely. It provides clear responsibilities for those assigned different roles and explains how to comply with this policy. The policy emphasized combining encryption with access control, authentication, and authorization. This reflects an understanding of the universities’ needs and aligns their strategy with a larger security framework. Responsible users are responsible for following the encryption guidelines, Key managers are accountable for following encryption guidelines and storing data securely, and ISO is responsible for developing and maintaining the university encryption guidelines. To ensure compliance with the encryption policies, UT could conduct quarterly audits, provide annual employee training, and establish incident response protocols for encryption key compromises. These measures would ensure that incidents are reported and addressed according to the policies and procedures.

**Physical and Environmental Protection Policy**

The Physical and Environmental Protection Policy is implemented for the NIST function Protect and the sub-category Awareness and Training.

The state of Maine implemented a policy for physical and environmental protection, which belongs to the government sector; this policy aims to establish Maine’s information technology protection. This policy applies to multiple parties; a few are the Office of Information Technology, Server Support Staff, and uniformed security, which oversee compliance with different areas. A wide range of responsibilities ensures compliance in all sectors interacting with the physical and Environmental Information technology. The policy scope focuses on specific locations related to the state Maines Office of Information Technology. The NIST template applies this in a broader focus; meanwhile, Maines policy applies to only two OIT data centers and the OIT headquarters, which covers these locations’ physical and environmental protection needs. To ensure compliance and accountability, the policy outlines specific roles and responsibilities for various parties, such as OIT Information Security, Server Support Staff, and Uniformed Security. These roles are designed to ensure that compliance is maintained and that all parties are held accountable. The policy’s detailed roles and responsibilities and its legal compliance demonstrate its commitment to ensuring compliance with regulatory obligations and state laws.

**Secure System Development Life Cycle Standard**

The Secure System Development Life Cycle Standard is implemented for the NIST function Protect and the sub-categories Data Security, Identity Management and Access Control, Data Security, Information Protection Processes and Procedures, and Protective Technology.

The University of Kansas’ (KU) Secure System Development Life Cycle Stand, which is in the education sector of the industry, aims to explain the minimum required phases and considerations when new software and systems are being developed or implemented at the university. This policy applies to many parties at the university, including the students attending the college, university employees, vendors, and contractors who work with software and systems development. The Chief Information Officer oversees the policy, the information technology department is responsible for assessing requests and ensuring compliance with the system development life cycle standards, and each department that works with the software and systems is responsible for following industry standards and best practices. KU tailored the policy to ensure it addresses the unique needs, stakeholders, and potential risks the university may face. Universities differ from other industry sectors, such as the government, and they must form policies that fit their specific needs. It allows them to ensure the members that the policy applies to understand and adhere to the policy. The policy also specifies circumstances for exemptions related to the policy. The university has a committee to assess exemption requests; this allows the university to maintain compliance with the main principles. KU acknowledges the diverse nature of projects and provides flexibility in certain circumstances. It may not be possible for a project to be done correctly due to the strict standards, but allowing a committee to review the request will enable them to collectively review the request and make an exception while ensuring the fundamental principles are maintained. The policy explained that it is reviewed annually and as needed. This means the CIO will review the policy at least once yearly but may review it additional times throughout the year. Certain circumstances may require the university to review the policy or make modifications multiple times in a year. The cyber landscape is ever-changing, and I highly advise the workers responsible for adherence to stay current on new standards and practices. Reviewing the policy frequently and making necessary modifications can ensure alignment with the evolving standards and best practices. One way to review it more regularly is to have a committee or team oversee the reviews. Stakeholders involved in the software or system development projects could provide additional feedback on areas they can improve; this will ensure the policy is being adhered to and that the policy always fits the needs and goals of the university.

**Cyber Incident Response Standard**

The Cyber Incident Response Standard is implemented for the NIST functions Identify, Protect, Detect, Respond, and Recover and the sub-categories Supply Chain Risk Management, Data Security, Information Protection Processes and Procedures, Detection Processes, Response Planning, Communications, Analysis, Improvements, Recovery Planning, Improvements, and Communications.

The U.S. Department of Education (ED), which belongs to the government sector, aims to adhere to the Federal Information Security Modernization Act and implement its regulations. The Office of Management and Budget A-130 ensures that all federal agencies develop, document, and implement programs for information security. There are minimum security requirements when working with federal information and systems. The overall focus of this policy is to establish IT incident response controls for the department. The aim is to enhance operations and improve the security of the information systems. ED tailored its focus to align closely with the needs and obligations of federal agency requirements. The policy covers its own information and information systems, contractors, and other external sources. The scope is broadened beyond internal systems, which aligns with the requirements to ensure security across all information systems, regardless of ownership. ED integrates specific regulations required to adhere to federal laws and regulations. By referencing these, the organization demonstrates its commitment to meeting the legal and regulatory requirements. IR-4 outlines the requirements for implementing incident handling capabilities with the incident response plan. It mandates lessons learned from incident handling into procedures, training, and testing. IR-4(2) emphasizes correlating incident information and individual responses to achieve an organization-wide perspective and response. The organization strives to integrate incident data to understand the threat landscape better and enhance its effectiveness.

**Personnel Security Policy**

The Personnel Security Policy is implemented for the NIST function Protect and the subcategory Awareness and Training.

St. John's University (SJU), which belongs to the education sector, policy aims to ensure appropriate guidelines are in place to secure information assets and protect customers, personnel, and business partners. SJU discussed how the Human Resources Department significantly ensures successful operations and effective IT services. SJU customized its policy to align with its needs, structure, scope, security measurements, and requirements. St John’s policy defines the scope of application to the university community. This includes a broad range of individuals associated with the institution; the terminology reflects the unique environment of a university, which goes beyond its employees. The policy emphasizes that the guidelines help safeguard information assets and the interests of their customers, business partners, and personnel. The security measures and Responsibilities are focused on recruiting and retaining staff members. This is crucial for ensuring a secure work environment within the institution. During staff hiring and termination processes, they provide security awareness training, user management, and security mechanisms. The policy also defines key terms to clarify the university’s operational framework. The university conducts periodic audits and reports and investigates breaches and disciplinary actions to ensure users adhere to their policies. St. John’s discloses that it reserves the right to conduct audits of their networks and systems periodically. Periodic audits imply they regularly review its systems and processes to assess adherence to security standards. According to their policy, there hasn’t been a revision since 6/11/2020; I highly recommend reviewing and revising this policy more often. The cyber landscape is ever-changing, and revising their policies can ensure they stay ahead of security risks. All information security breaches must be reported and investigated by the Chief Information Officer and the Director of Security to ensure the incidents are promptly identified and resolved. The policy establishes a framework for compliance, incident response, and enforcing accountability within the university.

**References**

*Contingency Planning Policy | Policies and Procedures*. (n.d.). <https://policy.arizona.edu/information-technology/contingency-planning-policy>

*Data Encryption Guidelines | UT Austin Information Security Office*. (n.d.). UT Drupal Kit Version 3. <https://security.utexas.edu/policies/encryption>

Fordham University. (n.d.). *Risk Assessment Policy | Fordham*. <https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/risk-assessment-policy/>

Hernandez, S. & U.S. Department of Education (ED) Office of the Chief Information Officer (OCIO) Information Assurance Services (IAS). (2022). *Information Technology (IT) Incident Response (IR) Standard*. <https://www2.ed.gov/fund/contract/about/acs/2022-ir-incident-response-standard-signed.pdf>

*Information Security: Threat and Vulnerability Management Standard*. (2022, September 21). UW Policies. <https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-threat-and-vulnerability-management/information-security-threat-and-vulnerability-management-standard/>

Laborde, S. (2023, July 3). 31 Insider threat statistics you need to know in 2023. *The Tech Report*. <https://techreport.com/statistics/insider-threat-statistics/#:~:text=As%20of%20May%202023%2C%20Businesses%20in%20the%20United,States%20Encounter%20Around%202%2C200%20Internal%20Security%20Attacks%20Daily>.

*NIST’s 7-Step Contingency Planning Process*. (n.d.). GovInfoSecurity. <https://www.govinfosecurity.com/nists-7-step-contingency-planning-process-a-2615>

*Policy 908 - Personnel Security Policy*. (n.d.). St. John’s University. <https://www.stjohns.edu/my-st-johns/human-resources/policy-908-personnel-security-policy>

State of Maine Department of Administrative and Financial Services Office of Information Technology. (n.d.). *Access Control Policy and Procedures (AC-1)* (pp. 2–12). <https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf>

State of Maine Department of Administrative and Financial Services Office of Information Technology (OIT). (n.d.). Physical and Environmental Protection Policy and Procedures (PE-1). In *Physical and Environmental Protection Policy and Procedures (PE-1)* (pp. 3–14). <https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/PhysicalandEnvironmentalProtection.pdf>

*Systems Development Life Cycle (SDLC) Standard | Policy Library*. (n.d.). <https://policy.ku.edu/IT/systems-development-life-cycle-standard>

Wilson, M., Hash, J., & National Institute of Standards and Technology. (2003). Building an information technology security awareness and training program. In *NIST Special Publication 800-50*. U.S. Government Printing Office. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf>