**Student Name: Andrew Newhart**

**Date: 10/22/22**

**Part 1: Cyber Incident Response Standard**

Locate and read the **Cyber Incident Response Standard** in the NIST Cybersecurity Framework Policy Template Guide. Research online for a real-world implementation example of the standard/policy and compare it with the NIST policy template side by side.

Answer the following questions clearly and systemically in this Word document. Make sure to include a References section toward the end of the document.

1. *The* ***Cyber Incident Response Standard*** *is implemented for which NIST functions and sub-categories? [5 points]*

Answer: The ***Cyber Incident Response Standard*** is used for the NIST functions of cybersecurity, security management, privacy, and information quality. The Standard is also used in the NIST subcategories of Cybersecurity Policy, Security Governance, Risk Management, Security Operations, and Threat Intelligence.

1. *Which organization is the implementation example you identified for? Which industry sector (e.g., education, government, etc.) is the organization in? [5 points]*

Answer: Oklahoma Office of Management & Enterprises Services - Government

What is the purpose of the example standard/policy? Which party (parties) does the standard/policy apply to? Who is/are responsible for implementing this standard/policy? [5 points]

Answer: This document establishes the requirements for reporting a security incident. Oklahoma Cyber Command

As compared to the NIST policy template, how is the example standard/policy customized to fit the needs of the organization? Describe two occurrences of the customization (e.g., incident triggering sources or incident types) in detail. [10 points]

Answer: A summary of the events surrounding the cybersecurity incident including

affected assets, systems, and services. The types of data compromised by the

cybersecurity incident.

**Part 2: Personnel Security Policy**

Locate and read the **Personnel Security Policy** in the NIST Cybersecurity Framework Policy Template Guide. Research online for a real-world implementation example of the standard/policy and compare it with the NIST policy template side by side.

Answer the following questions clearly and systemically in this Word document. Make sure to include a References section toward the end of the document.

1. *The* ***Personnel Security Policy*** *is implemented for which NIST functions and sub-categories? [5 points]*

Answer: its part of the Protect function and sub-category Awareness and Training.

1. *Which organization is the implementation example you identified for? Which industry sector (e.g., education, government, etc.) is the organization in? [5 points]*

Answer: Oklahoma Office of Management & Enterprise Services – Government

1. *What is the purpose of the example policy? Which party (parties) does the policy apply to? Who is/are responsible for implementing this policy? [5 points]*

Answer: To ensure that personnel security safeguards are applied to the access and use of

information technology resources and data. This policy is applicable to all departments

and users of IT resources and assets

1. *As compared to the NIST policy template, how is the example policy customized to fit the needs of the organization? Describe two occurrences of the customization in detail*

**Answer:** It gives a section defining the rationale of the standard - To coordinate and require central approval of state agency information technology purchases
and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

1. *If specified in the example policy, what criteria are defined to verify the organization’s compliance to the policy? If not specified in the example policy, what are your recommendations? [5 points]*

Answer: This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

**REF:**

National Incident Management System (NIMS).
Oklahoma Cyber Command Cybersecurity Breaches.
Oklahoma State Government Security Breach Transparency Initiative.