Southern New Hampshire University

CYB 420 Project Two Milestone One Project Charter Template

Project Charter

Complete this template by replacing the bracketed text with the relevant information.

Project Name
ACME Company Network Security Enhancement Plan

Project Description
Create a **mission statement** to explain the project goal of addressing one vulnerability for each of the three risk domains (people, process, and technology).
This project aims to enhance ACME Company's network security by addressing vulnerabilities in three key risk domains: people, processes, and technology. The project will implement security awareness training in the people domain to reduce the risk of social engineering and phishing attacks. Formal security policies and an incident response plan will be established in the process domain to ensure the consistent handling of security threats. Network segmentation and hardware updates will be implemented in the technology domain to limit the lateral movement of threats and improve infrastructure resilience. The organization will strengthen its security posture and minimize risks by mitigating these vulnerabilities. Additionally, this initiative will foster a culture of cybersecurity awareness within the company, ensuring that all employees actively contribute to safeguarding organizational assets. The project will also improve the organization's ability to respond to emerging threats by continuously assessing and refining security measures. Implementing these changes will position ACME Company as a security-conscious enterprise, ready to adapt to evolving cyber threats and industry standards.

Organization

Southern New Hampshire University

Prompt	Answer
Discuss the **business needs** you will meet by completing this project.	This project will meet ACME Company's business needs by reducing cybersecurity risks, ensuring regulatory compliance, and enhancing operational efficiency. Security awareness training will equip employees to recognize and respond to cyber threats, reducing human error-related breaches. Establishing formalized security policies and an incident response plan will create a structured approach to threat management, minimizing downtime and data loss. Implementing network segmentation and upgrading outdated hardware will fortify the organization's technological defenses, ensuring a robust and secure network infrastructure. The company will enhance data protection, maintain customer trust, and safeguard critical assets by addressing these needs.
Explain your project's methods of **scalability**.	ACME Company can scale this project to strengthen security as it grows. Regular updates and integration into employee onboarding will expand security awareness training. The company can continuously refine security policies and the incident response plan to address emerging threats and evolving business processes. As new departments and systems are added, IT teams can adjust network segmentation to maintain strong protection. Routine hardware assessments will help phase out outdated equipment and introduce advanced security solutions. By implementing these scalable strategies, ACME ensures its security measures remain effective.

Southern New Hampshire University

Project Completion

Prompt	Answer
Explain the **scope** of what will be delivered at the end of the project.	After this project, ACME Company will have a comprehensive security awareness training program, ensuring employees understand and follow cybersecurity best practices. The organization will also have a structured security policy framework and a well-documented incident response plan to guide employees in handling security threats. We will implement network segmentation in the technology domain to isolate critical systems and replace outdated hardware with updated equipment to enhance security. These deliverables will collectively improve the company's security posture and resilience against cyber threats.
Assess the potential **business impacts** of the project.	The successful implementation of this project will yield significant positive business impacts. Employees will be better equipped to recognize and mitigate security threats, reducing the likelihood of breaches caused by human error. The formalized security policies and incident response plan will enhance regulatory compliance, preventing legal and financial penalties. Improved network segmentation and hardware updates will enhance system performance and reduce downtime caused by cyber incidents. The company will experience increased data protection, improved business continuity, and strengthened stakeholder confidence in its cybersecurity measures.