Teacher Summary: Security Policies

This document provides instructor guidelines for one of the ten integrated curriculum projects developed for the NSF-funded Necessary Skills Now (NSN) project (award #1501990). The NSN project partners consist of CORD and three national centers supported through the NSF's Advanced Technological Education (ATE) program: National Center for Systems Security and Information Assurance (CSSIA), Florida Advanced Technological Education Center (FLATE), and South Carolina Advanced Technological Education National Resource Center (SC ATE). The NSN project is designed to integrate employability skills into technical exercises, activities, and labs. The project partners created self-contained instructional modules vertically aligned to associate degree programs in **mechatronics/automation in manufacturing** and **cybersecurity in information technology**. (The activities described in this document support courses in cybersecurity.) Six categories of employability skills, repeatedly mentioned in workforce surveys and research reports, served as the focus of the integrated curriculum:

This project addresses the skills highlighted above. (Verbal communication is addressed in an optional procedure.)

Faculty Resources	
Section	**Content**
Project Overview	**Purpose:** To incorporate employability skills (teamwork, written communication skills, and problem-solving skills) into an exercise that focuses on creating information security policies to mitigate existing vulnerabilities exposed by a third-party audit. **Courses for Implementation:** Security+ **Key Terms:** Policies, Security Policies
Discussion	**The Problem:** ACME Healthcare is a healthcare company that runs over 25 medical facilities including patient care, diagnostics, outpatient care, and emergency care. The organization has experienced several data breaches over the last five years. These data breaches have cost the organization financially and damaged its reputation. The executive leadership team recently hired a new chief information security officer (CISO). The new CISO has brought in one of the top cybersecurity penetration teams to perform a full security audit on the entire organization. This independent contractor conducted the audit and found the following vulnerabilities: 1. Several accounts were identified for employees that are no longer employed by ACME. 2. Several user accounts allowed unauthorized and escalated privileges and accessed systems and information without formal authorization. 3. Several devices and systems allowed unsecure remote access. 4. Forty percent of all organization passwords audited were cracked within 6 hours. 5. Password expiration was not standardized. 6. Sensitive files were found unencrypted on user systems and laptops. 7. Several wireless hotspots used WEP for encryption and authentication. 8. Evidence indicates that sensitive e-mail was sent unencrypted to and from employee homes and mobile devices. 9. Intrusion detection logs were infrequently reviewed and analyzed. 10. Systems with sensitive company data were used by employees for private use. 11. Employee systems were left unattended and employees failed to log out of the company network and data systems. 12. Inconsistent system updates and configurations were performed. 13. Several firewall rules were set to permit all traffic unless specifically denied. 14. Company servers were not updated with the latest patches. 15. Intranet web server allowed users to change personal information about themselves, including contact information (address, phone number, etc.). The front line of protecting organizations from vulnerabilities are information security policies, standards, guidelines, and procedures. Organizations typically implement multiple security policies to protect their information and assets. Security policies include everything from acceptable use policies (AUP), which define the use of company assets, to policies for handling sensitive information. Review the SANS Security Policy Project. Students will read through the purposes of all the policy templates and select 5–6 policies that are relevant to mitigating items on the scenario list, download the template, and review the policy framework and elements that make up a policy. This information is critical in creating information security policy.

Faculty Resources	
Section	**Content**
	Students will discuss their findings as a group. The group will determine and list the top five policies needed by ACME Healthcare. **Each group member will be responsible for creating one information security policy and a procedure to support that policy.** NOTE: All policies must have a common framework, format, and length. Students must address all existing elements in the template. Review the differences between policies, standards, and guidelines by showing the following YouTube video: Information Security Policy (4:35) The creation of information security policies has little impact on an organization without an effective dissemination and implementation plan. This plan identifies specific activities or events that require employees to review and become familiar with specific policies. For example, all new employees typically become familiar with the acceptable use policy and sign an agreement that states that they understand and will abide by the policy. Many other opportunities exist to proactively implement security policies. For example, a policy might need to be reviewed before administrators install a new server. The group will publish a dissemination and implementation plan that covers employees from date of hire to separation. This may also involve an evaluation to confirm that key employees fully understand an organization's information security policies. The plan should include other involved departments such as human resources, accounting, legal, and management. The plan document should be no more than one (1) page.
Objectives	Student Learning Objectives (Career and Technical, employability, etc.) a. ***Technical*** – Students will contribute to the process of analyzing current security vulnerabilities and will identify and create an information security policy designed to mitigate identified vulnerabilities and a procedure to support that policy. b. ***Teamwork*** – Students will demonstrate the ability to work constructively and respectfully in teams to contribute to the analysis of vulnerabilities and construction of security policies. c. ***Written Communication*** – Each participant will demonstrate the ability to communicate in writing the relevance and implementation of security policies and procedures, and document a plan for implementation and dissemination. d. ***Problem Solving*** – Participants must successfully analyze a list of security vulnerabilities and identify countermeasures in the form of security policies and operational procedures.
Teaching Strategies	Step 1 – Review the project and objectives with the class. (10 minutes) Show the video Information Security Policy (4:35). Students should take notes to differentiate the various levels and types of policies. Step 2 – Assign students to teams of three to five students. Distribute all student handouts, research materials and other resource materials to each team. Each team completes the group activity and creates a table that identifies the top five vulnerabilities from the list, the policy that will mitigate the vulnerability, and a short justification. (30 min)

Faculty Resources	
Section	**Content**
	Step 3 – Each participant completes the information security policy creation activity. Each student will create one policy that addresses one of the top five vulnerabilities identified. These items are graded on an individual basis. (20–30 min) Step 4 – Each student completes the security procedure activity. Each student will create a procedure that supports their new information security policy. (20 min) Step 5 – Each group will be responsible for developing an information implementation and dissemination plan of no more than one page. (20 min) Step 6 (optional) – Each student can be required to prepare and deliver a brief presentation (3–5 minutes) describing the new policy, as if to a panel of managers who must be convinced of the need and justification for such a new policy.
Student/Group Activity Steps	1. As part of the student activity handout, each student should read the results of the ACME Healthcare Audit. As a class, watch the video Information Security Policy, taking notes about the levels and type of policies. 2. After forming teams of 3–5 students, review the security audit findings. Working as a team, review and research each item using the websites below and then rank the significance of each vulnerability to the organization. Record the team's rankings in the vulnerability ranking table. • http://cwe.mitre.org/top25/index.html • http://www.networkworld.com/article/2193965/tech-primers/top-10-vulnerabilities-inside-the-network.html Groups should evaluate the stated vulnerabilities, determine a ranking, and come to a consensus on the top five policies that ACME Healthcare should implement. 3. Each member of each team will be responsible for developing a written document detailing the procedures to implement one of the security policies, based on the SANS templates. 4. As a team, discuss and document information required to create an information security policy **implementation and dissemination plan**. 5. Optional: Students will prepare and deliver a 3-to-5-minute presentation, as if to ACME Managers, describing and defending the need, cost, and consequences of the new policy.
Expected/Result and Solutions	An acceptable use policy (AUP) should be one of the five policies recommended by all groups.
Equipment/Materials	Computer system with Internet access
Faculty Resources	
Background Materials	1. Supplemental Materials: a. Information Security Policy – A Development Guide https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331 b. Technical Writing for IT Security Policies in Five Easy Steps

Faculty Resources	
Section	**Content**
	https://www.sans.org/reading-room/whitepapers/policyissues/technical-writing-security-policies-easy-steps-492 2. Suggested Website Links a. CWE Top 25 Most Dangerous Software Errors b. Top 10 vulnerabilities inside the network c. Information Security Policy Templates d. Information Security Policy
Student Handouts	**3_Student_SecurityPolicies**
Assessment	Assess student performance and abilities by referring to the compilation of rubrics in **4_Rubric_SecurityPolicies** • Teamwork Rubric • Problem Solving Rubric • Written Communication Rubric • Verbal Communications Rubric (Optional) • Technical Rubric