Teacher Summary: Incident Response

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.

Incident Response Faculty Resources	
Section	**Content**
Project Overview	**Purpose:** To incorporate employability skills (teamwork, written communication, and problem-solving) into an exercise that focuses on preparing students to gain the knowledge and skills necessary to participate in an incident response process **Courses for Implementation:** Security+ **Key Terms:** incident response, CIRT, policies, incident response policies, incident response procedure, data breach
Discussion	As an information security professional at XYZ College, you are responsible for protecting the college's digital assets. You must follow cybersecurity standards and monitor incoming and outgoing traffic in order to detect malicious activity impacting the college's network. All IT security personnel must read and sign off on the college's policies. One of these policies is the *Incident Response Policy*. **The Problem:** The XYZ College Chief Information Office (CISO) just received notice of a potential data breach from the Research and Education Networking Information Sharing and Analysis Center (REN/ISAC). The report specifically identifies credentials of XYZ College students that appear in a credential dump on a well-known black hat public website. Below is the notification received from REN-ISAC: Greetings. It has been brought to the attention of REN-ISAC that credentials from your institution have appeared in a credential dump. Most of these credential dumps are discovered on publicly accessible sources. The credentials in question may be those used to access your institution's information resources. Even if that is not the case, the matter should be investigated as credentials are sometimes captured via password stealers. We have no way of determining when or how the credentials were acquired or whether the accounts to which they pertain are active. We only know that the credentials were disclosed within the last few days. Two days before the notification from REN/ISAC, a student reported that he received erroneous charges from the college on his account. A major responsibility of today's cybersecurity professional is to understand and participate in implementing an organization's *incident response process*. Security professionals are required to identify incidents, question system administrators and system owners, and take appropriate actions to mitigate potential threats. Assign students to **two-person incident response teams**. Each team will review the organization's incident response policies, procedures, framework, and roles and responsibilities. Each team will analyze the data to develop an incident response questionnaire and complete an investigation form as part of the incident response process. Review the Incident Handlers Checklist on page 10 of the Incident Handler's Handbook and explain the concept of *system quarantines* and *critical incident response*.

Incident Response Faculty Resources	
Section	**Content**
	The Incident Handler's Handbook In the procedures document, review both of the workflow process diagrams and the roles and responsibilities of individuals involved in an incident response investigation. Each team will develop interview questions for the affected system's owner and administrator to determine if the incident should trigger a CIR-level investigation. The questions should align to the Incident Response Workflow Process Diagram contained in the Incident Response Procedure document.
Objectives	Student Learning Objectives (career and technical, employability, etc.) a. ***Technical*** – Each team will analyze the incident response policy, procedure, and workflow process to develop an incident response questionnaire. b. ***Teamwork*** – Each team will develop interview questions that determine if the incident should trigger a CIR-level investigation. c. ***Written Communication*** – Each participant is required to demonstrate the ability to write questions designed to gather relevant qualitative data associated with the incident. d. ***Problem Solving*** – Participants must demonstrate the ability to analyze the incident response policy, procedures, and workflow processes to identify questions that can be used to differentiate a CIR-level investigation from a noncritical investigation.
Teaching Strategies	Instructors can add this project to NDG Security+ Lab 4, Incident Response Procedures. Step 1 – Review the project and objectives with the class. (10 min) Step 2 – Introduce the concept of a data breach and the impact that these events have on organizations. Emphasize current cybersecurity-related legislation and the obligations that organizations have when their systems are breached. Step 3 – Discuss the financial impact, operational impact, legal liability, and impact on an organization's goodwill. Step 4 – As a class, discuss each team's results and complete the incident response investigation form. Discuss the impact of a CIR-level incident on an organization's operations, liabilities, and reputation. (20 min)
Student/Group Activity Steps	1. Review the project and objectives with the class. (10 min) 2. Assign students to two-person teams. Distribute handouts, research materials, and other resource materials to each team. Each team will complete the incident response workflow process based on the scenario, policy, procedures, and memo received from the system owner. (30 min) 3. Step 3 – Each team will develop ten (10) questions to gather data for determining whether the incident will trigger the CIR process. (20–30 min)

Incident Response Faculty Resources	
Section	**Content**
Expected Result and Solutions	Following are sample questions. 1. How did the system owner become aware of the incident? 2. Did the affected system contain personal or private information? 3. Is the data on the system encrypted to ensure confidentiality? 4. Is the affected system mission-critical to the organization's operations? 5. Is the affected system on the organization's whitelist? 6. Is the system accessible from both inside and outside the organization? 7. Was the data backed up regularly? 8. Are countermeasures implemented to protect the affected system? 9. Can the system be easily replicated or restored? 10. What type of data is stored on the system? 11. How many users have access to the system? 12. What users have access to the system? 13. Do time, location, or credentials control access to the system? 14. Is the system still functioning? 15. Has operation of the system been affected? 16. Does the system reside on more than one physical host? 17. Does the system reside in more than one physical location? 18. How many people have administrator privileges? 19. Does the system have logs that track access and incidents? 20. Can the system be isolated from external access? Note: Many of these questions are found on the incident response investigation form.
Equipment/Materials	Computer system with Internet access
Background Materials	1. Handouts and Supplemental Materials: a. Student procedure for this activity (see *3_Student* in list below) b. Student handouts 1-4 (see list below): questionnaire/investigation form, incident response policy document, sample memo announcing an incident, incident response procedures document 2. Website resources a. The Incident Handler's Handbook (SANS) b. PCI ComplianceGuide.org c. NDG Netlab+ Security+: ***Lab 6 – Incident Response Procedures*** (always use latest version)
Student Handouts	• 3_Student_IncidentResponse • 5_Handout1_Questionnaire_IncidentResponse • 6_Handout2_Data_Breach_Policy_IncidentResponse • 7_Handout3_Memo_XYZCollege_IncidentResponse • 8_Handout4_Procedure_for_Breach_IncidentResponse

Incident Response Faculty Resources	
Section	**Content**
Assessment	Assess student performance and abilities by referring to the compilation of rubrics in **4_Rubric_Incident Response** for • Incident Response Teamwork Rubric • Incident Response Problem Solving Rubric • Incident Response Written Communication Rubric • Incident Response Technical Rubric