**CIT 485 ADVANCED CYBERSECURITY-**

**Lab6: ﻿Building an Incident Response Program**

The purpose of this lab is:

**Lab6-1: Importance of Incident Response**

After completing this lab, you will be able to:

* View a Sample Incident Response Plan

**Lab6-2: Host Related Incident Compromise Indicators**

After completing this lab, you will be able to:

* Create a Sample Batch File
* Create a Local Software Restriction Policy

Lab Instructions:

We assume you have completed lab0 and have created and activated your practice labs account. If you have not done that yet, please refer to lab0 instructions in Canvas, Week1, Lab0 section.

## **1) Lab6-1: Importance of Incident Response (20-points)**

Lab **Submission**

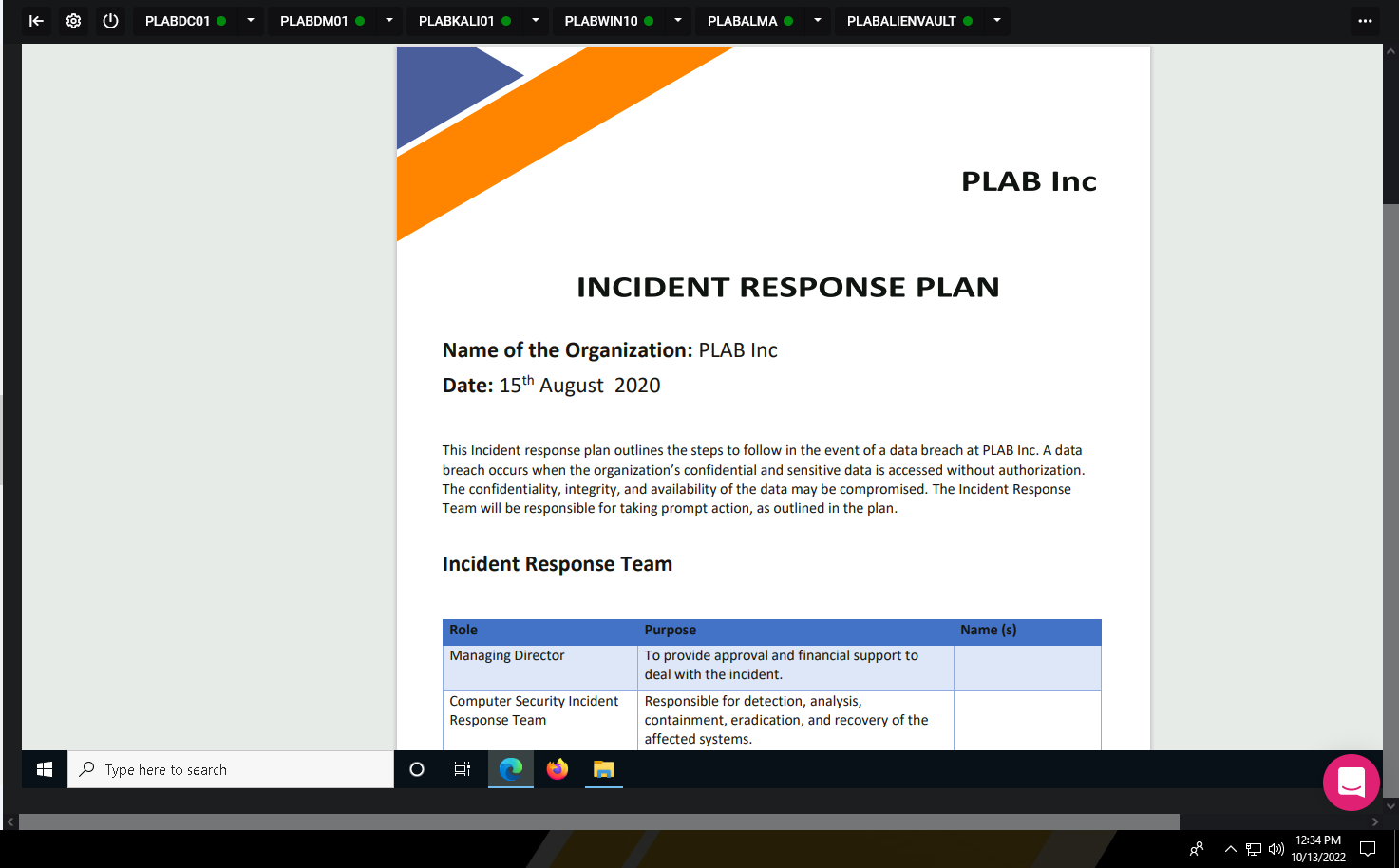
Please make sure to do all the exercises.

**Exercise 1 – Communication Plan**

**Task 1 - View a Sample Incident Response Plan**

#### **Perform the Step 1 - Step 4 View a Sample Incident Response Plan and copy and paste the screenshots here. In step 4, summarize what you learned from the report.**

**Incident Response Plan**



Summary:

After reading over the document we can see that each team is given a specific purpose when an attack does happen. We can also see that it is important to have a step by step procedure to allow for a simple smooth fix with whomever is working on the response to the attack. As we can see this is a very important document to demonstrate what and how to properly deal with cyber attacks on Plab Inc. This document reminded me of a risk management report I did last semester.

## **Exercise 2 – Factors Contributing to Data Criticality**

**Task 1:**

#### **IN your words, summarize the Factors Contributing to Data Criticality.**

Overall data criticality is that all data has a different level of criticality depending on what the data may hold. There is data that everyone is able to handle and have access to in comparison there is private data that may hold medical records, credit card info, etc, that you don’t want everyone to have access and control over. Some of the factors that define the data criticality are personally identifiable information (PII) , intellectual property (IP), financial information, special protected info (SPI), high valued assets, and personal health information (PHI). These are all examples of certain levels of criticality which all depend on what data type they hold. For example PII is going to be your address, full name, credit card information. IP is going to be anything that has value that you created from your mind such as music, logo, slogan. Financial information is pretty self explanatory but this is essentially your banking records and information. High value assets to a company are going to be your servers, employee records, etc. SPI is going to be your information you may want to keep confidential such as religious beliefs, genetic data, biometric data. Lastly PHI is your personal health information such as medications, diagnosis, family history, hospital visits.

· Save the report as a docx file (first name and last name: ex. Awad\_Mussa1.docx)

· Keep this file as you will upload it when you take the lab5’s quiz.