Incident Response and Reporting

Target Audience: Any employee of Company X that has access to confidential information such as Personal Identifiable Information (PII), Sensitive Personal Identifiable Information (SPII), and Controlled Unclassified Information (CUII)

Duration: 30 Minutes

Objectives:

Identify the most common types of security incidents

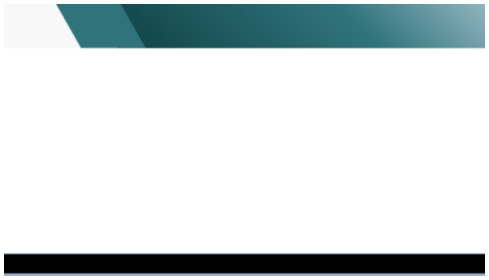
List in order the process of responding to security incidents

Outline:

1.1 Title Slide
1.2 Navigation
1.3 Course Objectives
1.4 What is an incident?
1.5 Four Types of Incidents
1.6 Knowledge Check 1
1.7 Knowledge Check 2
1.8 Incident Response Process
1.9 How to respond
1.10 Summary
1.11 Quiz Introduction
1.12 Quiz Question 1
1.13 Quiz Question 2
1.14 Quiz Question 3
1.15 Quiz Results
1.16 Thank You

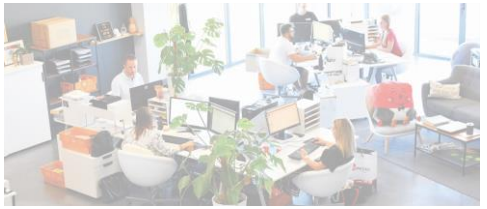
Notes for Reviewers:

- Please focus on the accuracy and completeness of the content during this review cycle.
- Questions or comments for the developer should be indicated in blue. All questions will need to be resolved before the developing the course can begin.
- Text in the Narration/ Voiceover column is narrated audio. This text will not appear on screen but will be heard.
    - Certain “connecting” words or phrases would not appear in written procedure. If you feel the wording needs changing, try reading the text aloud to see if it fits. Make changes if it still seems necessary.
- Capitalization is not important in the Audio column; however, it is very important in the column On-Screen Text.
- Information included in brackets [ ] or (italics) will not appear on screen or read. These labels are to show the order in which items will appear on screen or provide clarification to the developer.
- Timing for graphics/visuals/on screen text is tied to the narration/audio through a numbering system. For example, where you see a [1] in the narration/audio, you will likely see a [1] in the Visual/Display column telling you when an object is supposed to display on the screen.
- To provide feedback (edits, suggestions, etc.) You can edit directly in the document. To do this, please make sure track changes are on.
    - Click Review tab on the top of the document.
    - Select the Track Changes drop down and make sure “For Everyone” is selected.

Branding Hex Codes	
Fonts	Title: Articulate Bold Body: Open Sans
Sample Master Slide	
Image Attribution	Suggested images are free for commercial use.

Slide 1.1 Screen Title: Introduction			
Audio	On-Screen text	Functionality	On Screen Graphics
Welcome to the [1] Incident Response and Reporting eLearning course. Before we begin if you would like information on how to navigate the course, please select the [2] navigation tutorial button. If you are ready to jump right in, select [3] get started.	[1] **Introduction to Incident Response and Reporting** [2] Navigation Tutorial- button with shadow [3] Get Started- button with shadow	Text will appear to match narration. Introduction to Incident Response and Reporting- float in from top Participants will click “Get Started” to advance to slide 1.3 or “Navigation Tutorial” button to advance to slide 1.2	Buttons: rectangles with rounded corners. Light in color, with outer shadow.

Slide 1.2
Screen Title: Navigation

Audio	On-Screen text	Functionality	Description
To move backward and forward in the course, simply select the [1] previous and next buttons. Want to see something again select the [2]refresh button. Need to pause the course? Select the [3]play/pause button. Want to navigate to a different section in the course? Select the [4]menu button. When you are ready to begin, select the [5]next button.	Title Bar: Navigation No on-screen text	Arrows appear with narration and fade out as the next one appears so that only one arrow is visible at a time. Arrows are pointing to [1] previous and next button, [2] refresh, [3]play/pause button, [4]menu, and [5] next button (again).	Background image is a transparent office scene.  Arrows are dark teal with a shadow. 

Slide 1.3
Screen Title: Course Objectives

Audio	On-Screen text	Functionality	Description
When working with [1] Personal Identifiable Information, [2] Sensitive Personal Identifiable Information, [3] Controlled Unclassified Information it is your responsibility to report incidents as soon as you identify them. **In this lesson you will learn to:** • Identify the most common types of security incidents. • List in order the process of reporting and responding to security incidents.	Title Bar: Course Objectives • [1]Personal Identifiable Information (PII) • [2]Sensitive Personal Identifiable Information (SPII) • [3]Controlled Unclassified Information (CUI) [4] **In this lesson you will learn to:** • Identify the most common types of security incidents. • List in order the process of reporting and responding to security incidents. Click next to continue.	Fade in Personal Identifiable Information (PPI) to match narration. Remove to show Fade in Sensitive Personal Identifiable Information (SPII) timed to narration. Remove to show… Fade in Controlled Unclassified Information (CUI) Timed to narration. Remove to show… Float in from bottom of the screen: In this lesson you will learn to. Timed with narration. Remains on screen until timeline ends. Objectives appear one at a time to match narration. Remains on slide until timeline ends. Click next to continue appears after narration is complete. User clicks next to continue.	Master slide design Image of person 

Slide 1.4
Screen Title: What is an incident?

Audio	On-Screen text	Functionality	On- Screen Graphics
An incident refers to any violation that can compromise your information or the information systems you use. This can include: • [1] Violation of acceptable use policies • [2] Violation of standard security practices • [3] Violation of computer security policies	Title Bar: What is an incident? • [1] Violation of acceptable use policies • [2] Violation of standard security practices • [3] Violation of computer security policies	Text will float in from the bottom of the screen on dark teal rectangles one at a time as timed to narration. Click next to continue appears after narration is complete. User will click next to continue.	Picture of computer system on left side of the screen.  Dark Teal rectangles on right side.

Slide 1.5
Screen Title: What are the types of incidents?

Audio	On-Screen text	Functionality	On- Screen Graphics
[1] When working with confidential personal information, sensitive personal identifiable information, and controlled unclassified information there are four common incidents that may occur. [2] Click each picture to learn more. [3]Loss, damage, or theft of equipment, media, or documents containing PII, SPII, and other CUI. [4] Situations where unauthorized persons use your computer or credentials to access CUI.	Title Bar: What are the types of incidents? [2]Click each picture to learn more. Appears as a flashcard when images are selected: [3] Image 1 Selected State: Loss, damage, or theft of equipment, media, or documents containing PII, SPII, and other CUI. [4] Image 2 Selected State: Situations where unauthorized persons use your computer or credentials to access CUI.	[1] 4 images float in from the bottom of the screen during narration. [2] Click each picture to learn more appears after narration. User will click each image and selected state for each image turns into a flashcard with text and narration plays. Images 2-4 will be disabled until the previous audio is complete. Only one audio should play at a time. Cards should not be clickable after the first time.	   

[5] Sending a report containing confidential information to someone not authorized to view it or sending the report unencrypted. [6] Any security situations such as viruses, phishing emails, and social engineering attacks that could compromise information systems.	[5] Image 3 Selected State: Sending a report containing confidential information to someone not authorized to view it or sending the report unencrypted. [6] Image 4 Selected State: Any security situations such as viruses, phishing emails, and social engineering attacks that could compromise information systems. Click next to continue.	After viewing all four cards, the user will click next to continue. All cards should be visited before next appears.	

Slide 1.6
Screen Title: Knowledge Check

Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Knowledge Check A coworker uses your computer while you are gone to lunch. A report with controlled unclassified information (CUI) was open. The coworker seems nice so there is no need to report it. True False	Question is not graded and users may have two attempts. User will choose their answer True False (correct) User will click submit Incorrect answers will be prompted to try again. Correct answers will give a popup box with the reason confirming they are correct. User will click continue to move to the next slide	

1.6a Feedback Layers On-Screen Text

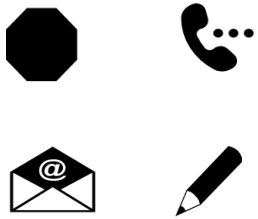
Correct- That's right! You selected the correct response. You should report when any unauthorized person has viewed CUI.

Incorrect- You did not select the correct response. You should report any unauthorized person has reviewed CUI.

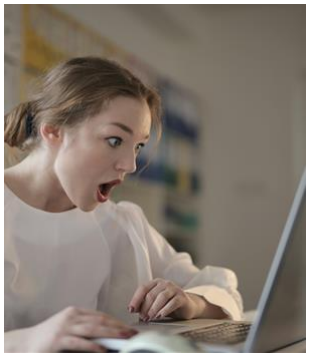
Try Again- That is incorrect. Please try again.

Slide 1.7 Screen Title: Knowledge Check			
Audio	**On-Screen text**	**Functionality**	**On- Screen Graphics**
No Audio	Title Bar: Knowledge Check You accidentally send a confidential PII to the wrong person. The recipient is not authorized to view the file. You should report this immediately. True False	Question is not graded and users may have two attempts. User will choose their answer True(correct) False User will click submit Incorrect answers will be prompted to try again. Correct answers will give a popup box with the reason confirming they are correct. User will click continue to move to the next slide.	
1.7a Feedback Layers On-Screen Text Correct- That's right! You selected the correct response. You should report when any unauthorized person has received access to PII. Incorrect- You did not select the correct response. You should report any unauthorized person has received access to PII. Try Again- That is incorrect. Please try again.			

Slide 1.8
Screen Title: Incident Response

Audio	On-Screen text	Functionality	On- Screen Graphics
[1] If you suspect a security incident has occurred, you must react quickly. Every second counts when dealing with security breaches. [2] [3]Failing to respond allows hackers more time to operate unnoticed. Here are the four actions you should take to report and respond. • [4] Stop • [5] Call • [6] Email • [7] Write	Title Bar: How should I respond? [3] 1 2 3 4 [4] Stop [5] Call [6] Email [7] Write Click each icon to learn more. (appears after narration is finished)	[1] Image of computer system will fade in during narration and [2]fade out. [3] Numbered Infographic fades in Icons and text fade together on infographic as timed with narration. [4]Text: Stop Icon: stop sign [5]Text: Call Icon: telephone [6] Text: Email Icon: computer [7] Text: Write Icon: pencil Icons should be clickable in order. Next button is hidden until all layers have been visited.	Picture of computer system with distressed person.  Infographic with four places  Icons: stop sign, telephone, computer, pencil 

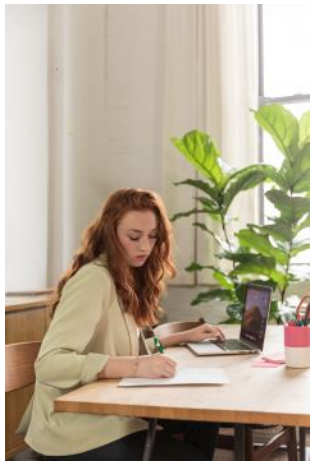
Slide 1.8a
Screen Layer: Stop

Audio	On-Screen text	Functionality	On- Screen Graphics
[1] If you suspect that computer security or confidential information has been compromised [2] you need to stop everything immediately! • [3] Do not try to fix the problem yourself • [4] Do not turn off the affected systems • [5] Do not allow others to use the affected system • [6] Do not share removable media	Title Bar: How should I respond? [2] Step 1: Stop • [3] Do not try to fix the problem yourself • [4] Do not turn off the affected systems • [5] Do not allow others to use the affected system • [6] Do not share removable media Click the X to close (small text beside the X icon)	[1]Image floats in from bottom on the left side of screen. Title and bullet points are on the right side of the screen. [2] Text appears on screen as a bolded title [3] Bullet point fades in from right. [4] Bullet point fades in from right. [5] Bullet point fades in from right. [6] Bullet point fades in from right. X icon will appear after the conclusion of narration and will hide the “Stop” layer when clicked. “Click the X to close” will appear after the conclusion of narration with the X icon.	Image of person on a computer in distress on the left side of the screen  Title text and bullet points are on the right side of the screen. X icon 

Slide 1.8b Screen Layer: Call			
Audio	**On-Screen text**	**Functionality**	**On- Screen Graphics**
[2] Step 2 is call If you suspect a security breach you should… • [3] Call your ISO and the X Call Center immediately • [4] Follow all instructions provided by the Helpdesk	Title Bar: How should I respond? [2] Step 2: Call • [3] Call your Information Security Officer (ISO) and the X Call Center immediately • [4] Follow all instructions provided by the Helpdesk Click the X to close (small text beside the X icon)	[1]Image floats in from bottom on the left side of screen before audio starts. Audio will begin with [2] Title and bullet points are on the right side of the screen. [2] Text appears on screen as a bolded title [3] Bullet point fades in from right. [4] Bullet point fades in from right. X icon will appear after the conclusion of narration and will hide the “Call” layer when clicked. “Click the X to close” will appear after the conclusion of narration with the X icon.	Image of telephone with hands dialing on the left side of the screen  Title text and bullet points are on the right side of the screen. X icon ✖

Slide 1.8c Screen Layer: Email			
Audio	**On-Screen text**	**Functionality**	**On- Screen Graphics**
[2] Step 3 is Email. If you experience a data breach or spillage you should.. • [3] Send a mitigating email to the same recipients of the original breached email or data spill. • [4] Delete any email or data in question from your email folder and remove the email from the recycle bin.	Title Bar: How should I respond? [2] Step 3: Email • [3] Send a mitigating email to the same recipients of the original breached email or data spill. • [4] Delete any email or data in question from your email folder and remove the email from the recycle bin. Click the X to close (small text beside the X icon)	[1]Image floats in from bottom on the left side of screen before audio starts. Title and bullet points are on the right side of the screen. [2] Text appears on screen as a bolded title [3] Bullet point fades in from right. [4] Bullet point fades in from right. X icon will appear after the conclusion of narration and will hide the “Email” layer when clicked. “Click the X to close” will appear after the conclusion of narration with the X icon.	Image of hands typing on computer  X icon ✖

Slide 1.8d
Screen Layer: Write

Audio	On-Screen text	Functionality	On- Screen Graphics
[2] Step 4 is Write. After suspicious activity occurs you should document any information that may be helpful to investigators such as: • [3] Date and time of the incident • [4] What you were doing at the time you first noticed the suspicious activity • [5]What you observed • [6]Names of others who may have observed the same activity	Title Bar: How should I respond? [2] Step 4: Write • [3] Date and time of the incident • [4] What you were doing at the time you first noticed the suspicious activity • [5]What you observed • [6]Names of others who may have observed the same activity Click the X to close (small text beside the X icon)	[1]Image floats in from bottom before audio starts. [2] Text appears on screen as a bolded title [3] Bullet point fades in from right. [4] Bullet point fades in from right. [5] Bullet point fades in from right. [6] Bullet point fades in from right. X icon will appear after the conclusion of narration and will hide the “Write” layer when clicked. “Click the X to close” will appear after the conclusion of narration with the X icon. Next button will appear when this layer is closed. User will click next to continue.	Image of person writing on left side of the screen  Title text and bullet points are on the right side of the screen. X icon ✖

Slide 1.9
Screen Title: Follow Up

Audio	On-Screen text	Functionality	On- Screen Graphics
[1] After a security incident has occurred it is important that you do not use the affected systems until you are cleared to do so. [2] The ISO will need time to [3] Review the incident [4] Follow up of reports to improve recovery efforts	Title Bar: When can I resume working? [2]The ISO will need time to • [3] Review the incident • [4] Follow up of reports to improve recovery efforts	[1] Image will float in from bottom. Text [2], [3], [4] will fade in from the right as timed with narration. User will click next to continue.	Picture of two people working on a computer. 

Slide 1.10 Screen Title: Summary			
Audio	**On-Screen text**	**Functionality**	**On- Screen Graphics**
[1] In this lesson you have learned to identify the most common types of security incidents that you may encounter while completing daily tasks. They are: • [2] Sending confidential reports to unauthorized viewers • [3] Allowing unauthorized persons to use your computer or credentials • [4] Equipment, media, and documents that are lost damaged, or stolen. • [5] Viruses, phishing emails, and social engineering attacks that compromise information systems.	Title Bar: Summary • Sending confidential reports to unauthorized viewers • Allowing unauthorized persons to use your computer or credentials • Equipment, media, and documents that are lost damaged, or stolen. • Viruses, phishing emails, and social engineering attacks that compromise information systems. Click the icons to review how you should respond. (appears in small text at the top right hand side of the screen.)	[1] Image of office scene will fade onto right hand side of screen. [2] Sending confidential reports to unauthorized viewers appears as timed with narration. [3] Allowing unauthorized persons to use your computer or credentials appears as timed with narration. [4] Equipment, media, and documents that are lost damaged, or stolen appears as timed with narration. [5] Viruses, phishing emails, and social engineering attacks that compromise information systems appears as timed with narration.	Picture of an office scene with multiple people working.  Bulleted text will be on the right side of the screen over a dark teal background.

A quick response time is important when dealing with security breaches. [6] Click each icon to review the steps on how you should respond.	Marker Arrow Popup Box: **Time** Every second counts during a security breach. Respond immediately! Marker 1 Popup Box: **Stop!** Stop all use of affected systems until you are cleared by your ISO. Marker 2 Popup Box: **Call** All your ISO and X Call Center immediately. Marker 3 Popup Box: **Email** Email recipients of the original breached email. Delete any email in question and remove it from the recycle bin. Marker 4 Popup Box: **Write** Write down any information that may be useful to investigators. Click next to continue. (Appears in small text at the bottom of the screen.)	[6] User will click each marker and a popup box with review information will appear. An arrow- clock 1- Computer 2- phone 3- computer 4- pencil “Click next to continue” appears after the state of all markers is selected.	Numbered markers will appear over the scene as follows: An arrow- clock 1- Computer 2- phone 3- computer 4- pencil

Slide 1.11 Screen Title: Quiz			
Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Quiz The next three slides will ask you questions about the information you have learned about reporting and responding to security incidents. Read each question, choose the correct answer, and then press submit. • You can not advance to the next slide until the question is answerd. You must receive 100% to pass this course.	User will click continue to move to the next slide.	

Slide 1.12
Screen Title: Quiz Question 1

Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Quiz Question 1 You have just experienced a security breach on your computer. Order the steps that you need to follow in order to report the incident.	Question will be a graded sequencing drop down. Correct Answer: Stop Call Email Write User will click submit to move to the next slide.	

Slide 1.13 Screen Title: Quiz Question 2			
Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Quiz Question 2 Your computer system was involved in a security breach. You followed the four steps to respond and report the incident. What is your next step? Answer choices: Get back to work. You have already wasted too much time. Go home. This day was very stressful. Wait for clearance to continue working from your ISO. Call your coworker and discuss the incident.	Question will be a graded multiple choice question. Get back to work. You have already wasted too much time. Go home. This day was very stressful. Wait for clearance to continue working from your ISO. (correct answer) Call your coworker and discuss the incident. User will click submit to move to the next slide.	

Slide 1.14
Screen Title: Quiz Question 3

Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Quiz Question 3 It is your responsibility to report incidents as soon as you notice them. Which of the following would be considered a threat of computer security? Choose 3 answers. Answer Choices: A virus has been detected on your computer. You receive an email from your boss. You notice that part of your computer equipment is missing. An unauthorized person has logged in using your credentials.	Question will be a graded multiple response question. A virus has been detected on your computer. (correct) You receive an email from your boss. You notice that part of your computer equipment is missing. (correct) An unauthorized person has logged in using your credentials. (correct) User will click submit to move to the next slide.	

Slide 1.15 Screen Title: Quiz Results			
Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Quiz Results Your Score: Passing Score:	Score will be generated from the graded quiz questions. Quiz will have the option to retake to achieve passing score. User will click next to continue.	

Slide 1.16 Screen Title: Course Complete			
Audio	On-Screen text	Functionality	On- Screen Graphics
No Audio	Title Bar: Course Complete **Congratulations!** You have successfully completed the Introduction to Incident Response and Reporting.		Image of person (same one from slide 1.3) with thumbs up. 