

Information Security and Privacy Storyboard

Slide 1 Title: Introduction

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Welcome to the Information Security and Privacy course. To begin, select the start course button.	Information Security & Privacy Start Course button	Background image:  The title in blue text will fly in with the audio. At the narration prompt, the red “start course” button will appear.	

Slide 2 Title: Welcome

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Thank you for taking the information security and privacy course. Please enter your first name in the text box, then select next to continue.	Hello, I’m Christy. What is your name?	Background image: 	

		Christy avatar appears with a dialogue box. And the text entry box is below that. 	
--	--	--	--

Slide 3 Title: Let's Get Started!			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Excellent! Let's get started. Select the next button to continue.	Nice to meet you, name! Let's Get Started!	Background image:  Christy avatar appears with a dialogue box.	

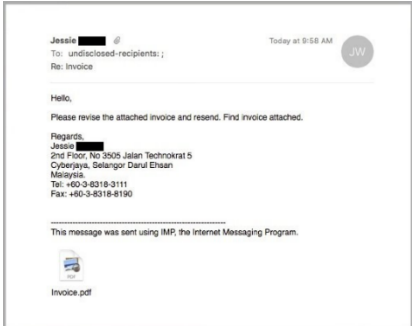
			
--	--	---	--

Slide 4 Title: Navigation			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
To proceed to the next slide, click on the “next” button. To review the previous slide, click the “previous” button. To pause the course, click on the pause button. To move to another slide in the course, click on the title of the slide in the menu to the left. Click Next to continue.	Navigation for the Course	 This photo appears as the backdrop. Following along with the narration, a red arrow appears on screen to draw attention to the navigation features. The user clicks next to continue.	

Slide 5 Title: Course Objectives			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Information Security and privacy are vital to protect and manage the confidentiality, integrity and availability of information and information systems.	Course Objectives	This photo appears on the page with the Course Objectives title.	

After taking this course, you will be able to: Apply the four methods of protecting Personally Identifiable Information, define the three pillars of Cybersecurity, and implement the four methods of protecting Controlled Unclassified Information. Select “next” to continue.	Apply the four methods of protecting Personally Identifiable Information (PII) Define the three pillars of Cybersecurity Implement the four methods of protecting Controlled Classified Information (CUI)	 The “objectives” text, with red boxes and stars, flies in, following the narration. Apply the 4 methods of protecting Personally Identifiable Information (PII) 	
--	--	---	--

Slide 6 Title: Scenario			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Let’s take a look at a typical day at the office. When Christy comes into work, she discovers an email from Jessie, who works in accounting. Jessie has asked her to revise the attached invoice. Christy knows Jessie, so this isn’t an unusual request. She does notice that the email looks a little strange. The email is addressed to “undisclosed recipients.”	What should Christy do?	This is the background photo on screen:  The Christy avatar appears on screen:	

		 An example of a scam email pops up:  To follow the narration, red arrows point out the suspicious elements—the attachment and the recipient's address. At the end of the narration, the slide advances automatically.	
--	--	--	--

Slide 7 Title: Scenario

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
--------	-----------------	---------------------	--------------------

		The background image for the wrong answer:  A red skull and crossbones appears on the screen:  The slide advances automatically.	
--	--	---	--

Slide 8 Title: Why it's Important			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:

Now that you've seen how easily security can be breached, it is important to learn how to keep information safe. Information security and privacy are important because they: - Limit risk and potential consequences by keeping information safe; - Protect individual privacy of Personally identifiable Information; - Identify potential threats to sensitive information; - Limit resource usage violations and vulnerabilities; - Ensure integrity and availability of systems/data for our customers and emergency responders; and - Safeguard Controlled unclassified information entrusted to our care.	Information Security & Privacy Why it's important - Limit Risk - Protect Privacy - Identify Threats - Limit Violations - Ensure data integrity - Safeguard CUI Click next to continue	Background image:  And a text graphic at the left side of screen:  To follow the narration, the list of items appears one at a time on the right side of screen: - Limit Risk - Protect Privacy - Identify Threats - Limit Violations - Ensure data integrity - Safeguard CUI	
---	---	---	--

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Any information that can be used to distinguish or trace your identity is considered personally identifiable information. There are three categories of personally identifiable information classified as sensitive. Use the slider to see examples for each category. Select next to continue.	Sensitive Personally Identifiable Information User the slider to see examples of each category. Category 1 Category 2 Category 3	Pictures to identify each of the categories comes onto screen with a motion path:  Category 1  Category 2  Category 3 A slider at the bottom of the screen allows the user to reveal each layer with examples of the categories: Category 1 Social Security Driver's license State Identification Passport Alien registration Biometric identifiers Category 2 Any medical information such as doctor notes, prescriptions, or medical procedures Category 3 Financial account information, such as bank or credit card statements and tax returns	

Slide 10 Title: Protect your SPII

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Base Layer: So, now that you know what personally identifiable information is, how can you protect it? Select the boxes to learn more. Layers Audio: [Safeguard] To safeguard information: Do not leave personal information unattended on your desk Keep personal information in a safe place Keep your personal items in your possession Lock any personal possessions or information in your desk or office [Procedures] Remember to follow these procedures when teleworking. Always use a secure Wi-fi connection Use SPAM detection apps to screen calls Keep all passwords in a secure place	Base Layer: Protect your SPII Safeguard Information Follow Procedures Non-Disclosure Authorized Personnel Click on the boxes to learn more [Safeguard layer] Do not leave PI on your desk Keep PI in a safe place Keep your personal items in your possession Lock any personal possessions in your desk or office [Procedures layer] Always use a secure Wi-fi connection Use SPAM detection apps to screen calls	Background image:  On left side of screen, red boxes with each category grow into screen one at a time.  Layers [Safeguard] On left side of screen an image:	

[Disclosure] Follow these non-disclosure procedures: Do not give out any personal information in an email from an unknown source Do not reveal sensitive information over the phone to an unauthorized person Do not click on any links or open attachments from an unknown source [Authorized] Comply with these authorization procedures. Only reveal personal information to your HR manager Ensure that information is only given to an authorized representative of the company If you are not sure of the source, report it to your supervisor immediately [Last image] It is our responsibility to safeguard sensitive information. Be careful not to disclose information or make it available anywhere without your written consent.	Keep all passwords in a secure place [Disclosure layer] Do not give PI in an email from an unknown source Do not reveal PI over the phone to an unauthorized person Do not click on links or attachments from an unknown source [Authorized layer] Only reveal personal information to your HR manager Ensure information is given to an authorized representative If you are not sure of the source, report it to your supervisor	On the right side, each text box flies into screen along with narration [Procedures] On the left side of screen an image: On the right side, each text box flies into screen along with narration [Disclosure] On the left side of screen an image:	
---	---	--	--



On the right side, each text box flies into screen along with the narration

[Authorized]

On the left side of screen an image:



On the right side, each text box flies into screen along with the narration

Final image appears with “last image” narration:

			
--	--	---	--

Slide 11 Title: Knowledge Check			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments :
Now it's time for a knowledge check. Read the following scenario and select the best answer.	Knowledge Check Christy is in her office when she receives an email from Dave, in IT, requesting her username and password to update the software on her computer. What should Christy do?	The avatar, Christy:	

	(In a dialogue box above avatar's head): Is Dave the tall guy with black hair? I think I ran into him in the break room. Answer choices: A. Pay attention to the sender's email address. If it looks suspicious, report it to the manager. B. Ignore the email, and he'll go away. C. Click on the attachment to see if there are any more instructions. D. Give Dave your username and password. You can trust him.	 With dialogue box: Is Dave the tall guy with black hair? I think I ran into him in the break room.	
--	---	---	--

Slide 11b Title: Response Feedback A (Right Answer)			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Good job! You made the right call. Click "next" to continue.	Christy is in her office when she receives an email from Dave, in IT, requesting her username and	The avatar, Christy:	

	password to update the software on her computer. What should Christy do? A. Pay attention to the sender's email address. If it looks suspicious, report it to the manager.	 With dialogue box: Yes! You made the right call! If you are not sure about who is asking for the information, don't give it out!	
--	--	---	--

Slide 11c Title: Response Feedback B (Close, but not right)			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments :
Although this seems like a good option, it's always best to report any suspicious activity. Click "next" to continue.	Christy is in her office when she receives an email from Dave, in IT, requesting her username and password to update the software on her computer. What should Christy do? B. Ignore the email, and he'll go away.	The avatar, Christy:  With dialogue box: So Close! It is easy to ignore, but even if this trick didn't work on you, it might on someone else. Report it.	

Slide 11d: Response Feedback C (Not quite)

Audio:	On-screen text:	On-screen graphics:	Reviewer comments :
Not quite. Remember opening any attachments or links from an unknown source could be dangerous. Click “next” to continue.	Christy is in her office when she receives an email from Dave, in IT, requesting her username and password to update the software on her computer. What should Christy do? C. Click on the attachment to see if there are any more instructions.	The avatar, Christy:  With dialogue box: If you are unsure of the source, don't open any attachments or click any links.	

Slide 11e Title: Response Feedback D (Wrong Answer)

Audio:	On-screen text:	On-screen graphics:	Reviewer comments :
Remember, you do not want to give out any personal information to someone you don't know. Next time, report this email as suspicious. Click “next” to continue.	Christy is in her office when she receives an email from Dave, in IT, requesting her username and password to update the software on her computer. What should Christy do?	The avatar, Christy:	

	D. Give Dave your username and password. You can trust him.	 With dialogue box: Bad Call! Avoid giving any information, especially if you are unsure of the source.	
--	--	---	--

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
An organization can't have effective privacy without information security and it is most important in regard to Cybersecurity. The three common pillars to Cybersecurity are integrity, availability and confidentiality. Select each of the pillars to learn more. Layers: Integrity A computer worm infiltrates a computer system and modifies system software, causing the system to malfunction while	Cybersecurity & Privacy The three pillars to Cybersecurity are Integrity Availability Confidentiality To learn more, click on the tabs to the right. Layers:	On the left side of the screen, this image grows as soon as narration starts: 	

providing false system status. The integrity of the system's software was violated in this attack.

Availability

You return to your workstation and no longer can access your computer because someone else has locked you out. This is a breach of Availability because information is only allowed to be accessed by anyone authorized to do so in an appropriate manner and timeframe.

Confidentiality

Information on one of your documents shows project information assigned to you and is labeled Confidential. If your document was shared without your authorization, this is a breach of Confidentiality.

[Integrity] A computer worm could infiltrate a computer, compromising the integrity of the entire system.

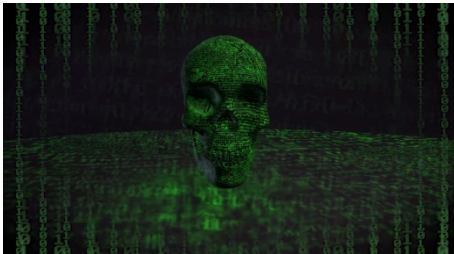
[Availability] If you've been denied access to your computer, a breach of availability has occurred.

[Confidentiality] Information shared without consent is a breach of confidentiality

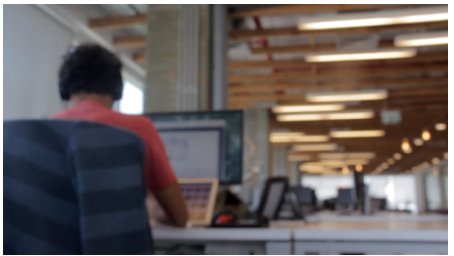
Along with the narration, the words integrity, availability, and confidentiality fly into the right side of the screen.

Layers:

[Integrity]
A video as the background plays on loop. Text appears on the screen.



[Availability]
A video as the background plays on loop. Text appears on the screen.



[Confidentiality]
A video as the background plays on loop. Text appears on the screen.

			
		User clicks next to continue.	

Slide 13 Title: CUI			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Base Layer Now that you know how to identify and protect personally identifiable information, it's time to learn about controlled unclassified information. Click on each of the pictures to learn more. Layers: CUI Controlled Unclassified Information (CUI), is information that has a degree of confidentiality and if it is lost, misused, accessed without authorization or modified, its confidentiality could be compromised and adversely affect the national interests, the company, or you. LDMs	Controlled Unclassified Information Click on each picture to learn more. What is CUI? LDMs NARA Protect Layers: CUI Controlled Unclassified Information is confidential, and if comprised, could have potential adverse impact. LDMs	On screen images: What is CUI?  LDMs  NARA	

LDM stands for limited dissemination marking. Using LDMs limits and clarifies the type of CUI information you may share, and with whom. Click the resources tab to see Limited Dissemination Markings and their definitions. NARA The National Archives and Records Administration (NARA) provides training tools on their website. For best practices on dissemination, markings, and sharing CUI. Click on the resources tab for more information. Protect We provide protection by safeguarding information and information systems from unauthorized access, use, disclosure, modification or destruction. This is particularly important for CUI, since misuse or unauthorized change or access can compromise national interests. CUI is protected by restrictions of how, who, and when information can be shared and used. These limitations provide the best protection for CUI. Select the next button to continue.	LDMs, or Limited Dissemination Markings, clarify what information is shared and with whom. Click the Resources tab to learn more. NARA The NARA website has training tools for how to handle CUI. Click the Resources tab to learn more. Protect CUI is protected by restrictions of how, who, and when information can be shared and used. These limitations provide the best protection for CUI.	 PROTECT  When each layer is revealed, the text appears—the base slide is visible the whole time.	
---	---	---	--

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Let's look at the ways to protect CUI. Click on each tab to learn more.	Physical Network Session Infrastructure Layers: Physical Controls The CUI must be physically protected via locks, such as card key access, surveillance cameras, or detection sensors. Network Controls The CUI must be protected at the network layer. Switches, routers, and firewalls must all work to prevent unauthorized access. Session Controls The CUI must be protected via authentication and authorization mechanisms or encryption. Infrastructure Controls Infrastructure that supports the CUI systems can take many forms, including virtual machines, physical servers, storage area networks, and backup systems	The background image:  This is an accordion slide feature. As each tab is clicked, the text is revealed for each layer. The user selects next to continue.	

Slide 15: Knowledge Check

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Now it's time for another knowledge check. Use the drag and drop method to match the correct responses. When you've chosen your answers, select the submit button.	Knowledge Check For each of the methods of protection for CUI, match the correct example. Answer Choices: Network Controls, Infrastructure Controls, Physical Controls, Session Controls Firewalls, Protected Servers, Card Key Locks, Authentication Systems	The avatar, Christy:  The drag and drop feature appears on the slide just under the avatar. With a correct response, a correct check mark appears with the text: That's right! You selected the correct response. With an incorrect response, an X mark appears with the text: That is incorrect. Please try again. The correct matching is: - Physical Controls – Card Key Locks - Network Controls – Firewalls - Session Controls – Authentication Systems - Infrastructure Controls – Protected Servers	

Slide 16: Summary

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Understanding the basics about information security and privacy will help you integrate a solid foundation of “best practices” into your daily work and projects. Now that you’ve completed the course, you have learned how to: Apply the four methods of protecting personally identifiable information Define the three pillars of Cybersecurity and Implement the four methods of protecting controlled unclassified information	Summary In this course, you have learned how to: Apply the four methods of protecting personally identifiable information Define the three pillars of Cybersecurity Implement the four methods of protecting controlled unclassified information	The avatar, Christy:  The text will “slide” onto the screen, following the narration.	

Slide 17: Application Activity

Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
Now it’s time to apply what you’ve learned. You will take a graded assessment: a drag and drop quiz with 10 situations that need to be placed in a “Do” or “Don’t” category When you are ready to begin, select the start button.	Application Activity Now it’s time to apply what you’ve learned! You need to score at least an 80% to pass. When you are ready to begin, select the start button.	Christy, the avatar is on the screen:	

		 When prompted by the narration, the red start button appears.	
--	--	--	--

Slide 18 Title: Activity 1			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
	Drag and Drop the Answers to the Correct Column Choices: Lock personal items in office when unattended Keep all passwords in a secure place Report suspicious requests for sensitive information Give sensitive information to an unknown source	A green “DO” header over a “drop” box  A red “DON’T” header over a “drop” box  “Do” Answers: Lock personal items in office when unattended Keep all passwords in a secure place	

	Click on links or attachments in emails or texts	Report suspicious requests for sensitive information “Don’t” Answers: Give sensitive information to an unknown source Click on links or attachments in emails or texts	
--	--	---	--

Slide 19 Title: Activity 2			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
	Drag and Drop the Answers to the Correct Column Choices: Keep key cards in your possession at all times Use LDMs on sensitive information Report any spam or malware on your computer Use any wi-fi source available when telecommuting Leave an envelope marked “confidential” on your desk	A green “DO” header over a “drop” box  A red “DON’T” header over a “drop” box  “Do” Answers: Keep key cards in your possession at all times Use LDMs on sensitive information Report any spam or malware on your computer	

		“Don’t” Answers: Use any wi-fi source available when telecommuting Leave an envelope marked “confidential” on your desk	
--	--	--	--

Slide 20 Title: Results			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:
	Results Your Score: Passing Score: Result: Review Quiz	If the learner passes, the green check mark appears with the text: Congratulations, Name, you passed! If the learner fails, a red X appears with the text: I’m sorry, Name. You did not pass.	

Slide 21 Title: Congratulations!			
Audio:	On-screen text:	On-screen graphics:	Reviewer comments:

Thank you for completing the course.
If you'd like more information about
the Privacy Act, click on the
resources tab.
To exit, select the exit course button.

Thank you for completing
the course!

Exit Course



Background picture

Text flies into screen, following narration.
A red arrow indicates the resources tab.
“Exit Course” button appears at end.