Title of Course:	Security Measures for Working Remotely		
Introduction:	The GHI company is expanding its business across the United States and offering more employees to work in hybrid or remote settings. To ensure the company's sensitive data information, the purpose of this training is to ensure that employees are taking all safety precautions to secure the data information. GHI company's goal is to reduce potential security breaches by 50% and increase employees' awareness in safeguarding sensitive data information while working remotely.		
Audience:	The primary target audience is for employees working in remote or hybrid settings. This may include employees who take work home.	**Color Palette:**	Khaki: C1B098 Thistle: E9D2F4 Battleship gray: 9B9B93 Jet: 39393A Moonstone: 63B0CD Celadon: B0F2B4
Learning Objectives:	After viewing the video, the learner will be able to: ● Implement security measures while working remotely at home or in a public setting. ● Establish routine antivirus and security software installed and updated at regular intervals. ● Identify potential threats to sensitive data information related to personal employee and client/employer information.	**Font:**	
Outline:	Title Scene Introduction: Potential Security Threats ● Unsecure network ● Video Conferencing uninvited guests ● Hackers ● Passwords ● Viruses Scene: Common Safety Practices ● Strong passwords ● Antivirus and security software ● Safe video conferencing practices Home Office ● Work computer vs. personal computer	**Characters:**	[Narrator] [Tom] [Sally] [Julie]

	Family and pet interference Scene: Public Setting • Avoid Public Wifi • Block line of sight • Securing devices to protect against theft Summary: • Review learning objectives		
Directions for Reviewer(s):		**Global Comments:**	• Each table in this storyboard represents one scene. • The character speaking will be indicated in the audio/script column as [character]. • Audio will be lip synced with character speaking.

Scene # 1		Title Scene: Welcome & Title	
Visuals/Graphics		**Script/Audio**	**Programming/Animation**
Background is a simple background selection Title Banner: Remote Work Security Measures (in large print) Subtitle Banner: Safeguarding technology devices and sensitive data information (in small print)		[Narrator] With more and more people working remotely these days, it's important to ensure you are safeguarding technology devices and sensitive data information against potential threats. Around 2,000 cyberattacks occur each day, with 90% of data breaches related to human error. It is important to identify potential security threats and how to prevent data breaches.	Quiet background music plays. Title banner slides in from the top and is centered on the page. Subtitle banner slides in from the bottom and centered below the title banner.

Scene # 2		Title Scene: Welcome & Title	

Visuals/Graphics	Script/Audio	Programming/Animation
Background is a neighborhood, which shows people working from home in different windows. Background changes to three different scenes of a person working remotely from home or a public setting	Narration from slide 1 continues	Quiet background music plays. Title is timed with audio. Title slides in from the top and is centered on the page. Security images fade in slowing around the title banner.

Scene # 2	Title Scene: Introduction Potential Threats	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is from the color palette. Narrator character stands to the left of the scene. Security threat images fade in and out of the scene one-by-one.	[Narrator] Working in a remote or hybrid setting increases the risk of a security attack and learning how to safeguard data and technology devices is key in reducing potential threats for you and your employer. Throughout this video, you will learn how to implement security measures to safeguard sensitive data information, establish routine intervals to update software, and how to protect your technology devices while working in a remote setting.	Narrator character stands off to the left side and brings attention towards the security threat images fading in and out of the scene one-by-one. Audio will be lip synced with character speaking.

Scene # 3	Title Scene: Common Safety Practices/ Password	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background image is a home-office desk with a clock on the wall.	[Narrator] When working remotely, there are some	Narration audio will be speaking in the background.

| Tom at his desk, facing his computer, typing in a password. | common safety practices that you should implement whether working at home or in a public setting.

A common safety practice is to create a strong and secure password. Passwords should be between 8-14 characters and include letters, numbers, and special characters. Change your password every 30-60 days to ensure data information is protected and updated. Use a safeguard password manager to manage password information. Never write down passwords on paper or share through online sources. | Tom is sitting down at a desk, typing in a password on his laptop. |

Scene # 4	Title Scene: Common Safety Practices/ Anti-virus & Security Software	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background scene same as scene # 3. Tom uploads antivirus and security software on his phone and computer. Camera zooms in on a clock's time slowly changing. Tom updates software on his computer.	[Narrator] Another common safety practice is ensuring you have updated antivirus and security software uploaded on your technology devices. Current antivirus assists in detecting, blocking, and removing viruses and malware. It can also provide warnings about potential threats in websites or links. Security software is critical to reduce cyber-attacks, data breaches, and against major disruptions from computer systems.	Narration audio will be speaking in the background. Tom is sitting down at his computer, uploading antivirus software. Zoom into the clock on the wall and watch the hands change. Zoom back out to full screen. Zooming out, shows Tom with a computer screen showing software update percentage.

Scene # 5	Title Scene: Common Safety Practices/ Video Conference	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**

Background scene same as scene # 3. Tom is in a video conference, and someone is trying to come into the meeting, who should not be there. Computer screen shows a video conference with others. On the computer screen, a pop up box shows that "Jim" is trying to join the meeting. Tom has a bubble thought: "Who is Jim?" Tom declines adding Jim to the video conference.	[Narrator] Video conferencing is a major part of working remotely and another common safety practice that needs to be addressed. Ensure your video software settings are set for privacy purposes and regularly updated. Create either a private link or use waiting rooms to allow accessed to join the video conference.	Narration audio will be speaking in the background. Others appear on the computer screen showing a video conference in progress. An extra window screen pops up to show that "Jim" is trying to join the meeting. Tom's bubble appears after the pop up screen. Tom declines adding Jim to the video call.

Scene # 6	Title Scene: Home Office Environment/ Personal vs. Work	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is a different home office or home environment then what appears in scenes #3-5. Sally will be working at her desk. Sally appears upset as she sent an email that was meant for personal reasons not meant for work. Two computers appear after the incident to keep work and personal computers separate.	[Narrator] When working from home, it is best practice to keep personal and work on separate computers. This avoids potential data threats and human errors that often occur when the two are combined. Sally is upset that an email that was personal was accidentally sent to one of her co-workers by mistake.	Narration audio will be speaking in the background. Computer screen shows an email that was just sent. Sally appears upset and frustrated.

Scene # 7	Title Scene: Home Office Environment/ Protect Devices	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is same as scene #6. Sally will be working at her desk. Her child ran up next to her chair and accidently knocked over a drink sitting nearby onto the computer. Her cat appears and jumps up on the desk. The cat walks across the keyboard. A thought bubble appears showing what Sally finds on the computer screen, "File deleted or an error occurred.".	[Narrator] It is a challenge to consider that family or pets could be potential threats while working from home, not to mention disruptive to your work schedule. Setting up a space and keeping family and pets away from your work, reduces potential risks of damage to technology devices and privacy data being shared or deleted.	Background noise is sounds of home life. Narration audio will be speaking in the background. Child runs in from the left up to Sally and knocks into the drink causing it to spill. Sally appears shocked when the drink spills on the keyboard. The cat jumps up on the desk and walks around the keyboard. A thought bubble appears showing what appears on the computer screen.

Scene # 8	Title Scene: Public Setting/ Wifi Hackers	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is a public setting (cafe or coffee shop). Julie is sitting in the center of the cafe working on her laptop with a coffee and pastry on the table. To the right corner of the cafe, sits a	[Narrator] When working remotely in a public setting, never connect your devices to a public wi-fi or use public charging stations. This leaves your computer open and vulnerable to hackers to potentially let them collect sensitive privacy information.	Background cafe sounds. Narration audio will be speaking in the background. Hacker is sitting at another table watching Julie.

| man (Hacker) who is watching Julie and appears to be typing.

Julie shows to be connecting to the Cafe's Wifi.

After Julie connects to the Wifi, the man appears happy as he now accesses her computer information.

Thought bubble appears for the Hacker showing what he is collecting from Sally's information. | Best practice is to connect to a secure VPN or a hotspot. | Hacker changes to happy when he obtains Julie's data information.

In time with the audio, "Best practice," Julie shows the correct way to connect to a secure VPN or hotspot.

Hacker appears angry that he didn't get her data information. |

Scene # 9	Title Scene: Public Setting/ Block Sight Line	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is same as scene #8. Julie is sitting in the center of the cafe working on her laptop with a coffee and pastry on the table. People walk by in the background and look at Julie's computer. Julie moves to a corner table with her back to the wall.	[Narrator] Another public safety practice is to sit in an area that doesn't leave your computer screen vulnerable to public eyes. This preventive measure also safeguards sensitive privacy information that may be displayed on your computer screen.	Background cafe sounds. Narration audio will be speaking in the background. People walk across the scene behind Julie and appear to be looking at her computer. In time with the audio, "preventive measure," Julie moves to a corner table with her computer screen facing the wall.

Scene # 10	Title Scene: Public Setting/ Unattended Devices	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is same as scene #8.	[Narrator]	Background cafe sounds.

Julie is sitting in the center of the cafe working on her laptop with a coffee and pastry on the table. Julie gets up and walks over to the drink fountain leaving her belongings unattended. A theft appears and takes the laptop without Julie being aware.	Leaving unattended devices opens the possibility of damages, invasion of privacy information, or theft. Always secure your belongings in public, even if that is getting up to get a drink refill or to use the restroom.	Narration audio will be speaking. Julie gets up to walk over to the drink fountain. A theft enters and swipes the computer and disappears. In time with the audio, "always secure," zoom in on Julie packing up her devices before getting up out of her chair.

Scene # 11	Title Scene: Summary	
Visuals/Graphics	**Script/Audio**	**Programming/Animation**
Background is from the color palette. Narrator stands to the right of the scene. He directs learners' attention to the infographic image below that is to the left of the narrator. It slowly scrolls from top to bottom while the narrator speaks.	[Narrator] Increasing your awareness of potential threats while working remotely, you can reduce possible cyber attacks, data breaches, and common human errors. Develop routine habits to practice remote work safety procedures by implementing security measures on all technology devices, establishing a regular routine to update software, and be aware of potential threats to private data information.	Audio will be lip synced with narrator character speaking. The infographic will be slowly scrolling from top to bottom on the screen.

SAFETY TIPS FOR REMOTE WORK

1 SECURE NETWORK AND PASSWORD
- **Avoid** public Wi-Fi and charging stations
- Use Secure VPN
- Create a strong password

2 MAINTAIN ANTIVIRUS AND SECURITY SOFTWARE
- **Do not** open suspicious websites or links
- Use current antivirus and security software
- Develop a habit to update routinely

3 VIDEO CONFERENCING
- **Do not** allow suspicious people to join
- Create private links
- Use waiting rooms
- Use current and updated software

4 IDENTIFY POTENTIAL THREATS
- **Do not** leave devices unattended
- Hackers/thefts
- Cyber-attacks or data breaches