



Security Awareness Training

User Guide



Why do I need to take a Cybersecurity course?

It seems like we can't go a day without hearing about another data breach or cybercriminal activity in the news. But did you know, there's so many more breaches out there that DON'T get news coverage, even companies just like yours. That means your organization has a big responsibility to prevent one from occurring – and with cybercriminals targeting small to medium-sized businesses more than ever, it's not an easy task to protect your customer's credit cards or employee's W2's.

Unfortunately, human-error accounts for **most** of these data breaches. Whether it's clicking on the wrong link, approving a very convincing request for a fund transfer – FROM THE CEO, or allowing network access to an outsider, data breaches come in all forms, and cybercriminals are relentlessly targeting organizations just like yours to exploit valuable data.

The good news? Most of this can be prevented with ongoing education and routine testing. Threat Protector by Telesystem ensures you are staying up to date on the latest threats and doing your part to protect your business. Technology alone isn't enough anymore.

Being well trained in cybersecurity will go a long way in protecting your organization, and the individuals whose data you may access.



What does this program consist of?

Employee Secure Score

Each employee will be given an Employee Secure Score (ESS). This score is generated by combining many of the key metrics listed below. You can think of your ESS like a credit score for your security strength. The higher the ESS, the more likely you are to defend against a data breach.

Micro-Trainings

Each week, you'll be sent an email to watch a 1–2-minute micro-training video on the latest cybersecurity threats. Complete the 4-question quiz at the end of the video to increase your Employee Secure Score!

Security Policies & Procedures

Your organization's Security Policies & Procedures are uploaded into the portal. You will need to read through each one, verify that you understand the policy/procedure and expectations, and electronically acknowledge your commitment to abide by them.

Dark Web Monitoring

As part of this program, we will continually monitor the Dark Web for your email address and notify you if it is discovered, that way you can take the appropriate next steps, like quickly updating your passwords.

Leaderboard

The leaderboard lets you compete head-to-head with your co-workers to see who has the highest ESS! Don't forget to pick a good screen name! Have fun and enjoy the healthy competition!

Phishing

We will be sending routine phishing emails to test you on the various types of phishing attacks you could encounter in real-life. Phishing is the number one attack method for cybercriminals, so being able to spot a malicious email will go a long way in protecting yourself, and your organization.

Annual Security Awareness Training

You'll be required to complete annual security awareness training. This training course will get you familiar with real-life examples of how data breaches occur, and how you can prevent them. In addition, you'll learn all about how to protect personally identifiable information (PII).

Dark Web Scans

The more you know, the better you can protect yourself and your loved ones. This program allows you to scan your personal, friends', or family members' email addresses to find out if they're out there on the Dark Web. Perform as many scans as you'd like!

Your Employee Secure Score (ESS)

Getting Started

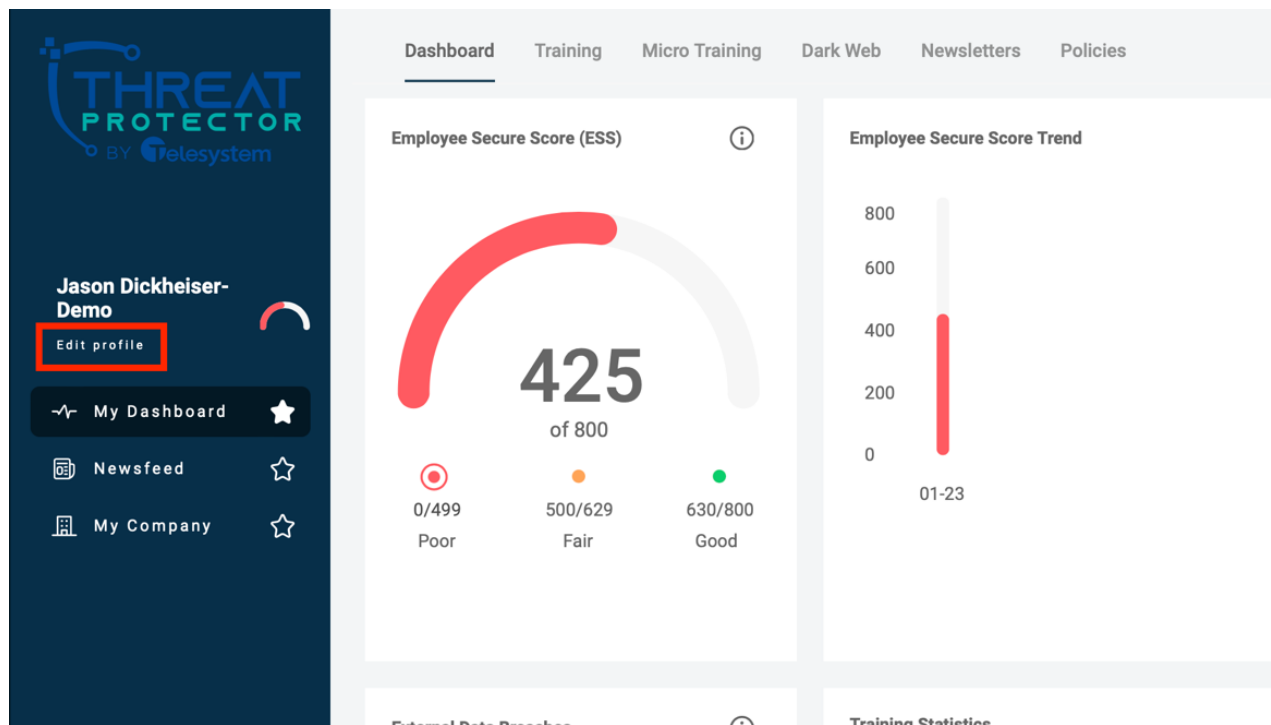
To begin, here are a few steps to successfully set up your screen name in the portal and tips for how you can maximize your Employee Secure Score (ESS).

Tips for maximizing your ESS:

- You'll receive ESS points for acknowledging all policies & procedures. Check with your manager or HR rep to see if there is an expected due date.
- Users with HIPAA Compliance Packages will receive ESS points for completing your annual HIPAA security awareness training. You can retake your quiz at any time to get a higher final score.
- The more micro-training quizzes you miss, the more it will negatively impact your ESS.
- Falling for a phishing email will negatively impact your ESS.
- If you're email address is found on the Dark Web, your ESS will be negatively impacted.

Logging in and Completing Your Profile

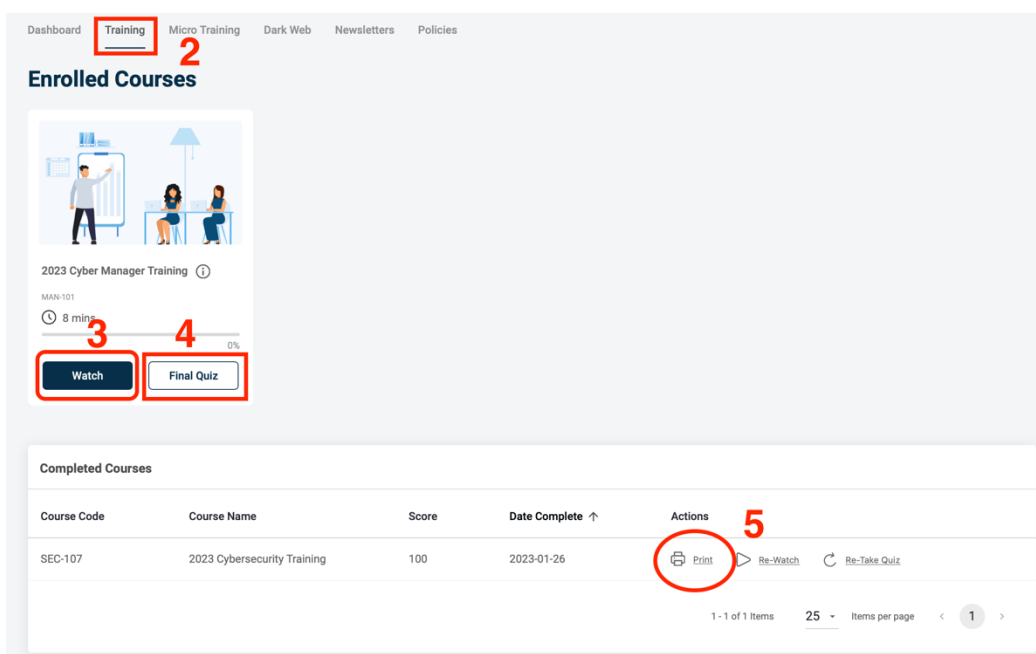
1. Login to your account: <https://portal.pii-protect.com/#/login>
 - Can't log in? Contact: support@telesystem.us
2. Complete your Profile
 - Claim your screen name and start climbing up the leaderboard by clicking **"Edit Profile"** below your name at the top of the dashboard (home screen).



How to Complete Annual Security Awareness Training

Getting Started

1. Login to your account: <https://portal.pii-protect.com/#/login>
 - Can't login? Contact: support@telesystem.us
2. Select the "Training" tab at the top of the page.
3. On this screen, begin with **Step 1** to complete your training program
4. Once you've gone through the training course, move on to **Step 2** to complete your 20-question quiz.
5. Once you successfully complete your quiz (with a score of 80% or higher), you will have the option to **print your training certificate in Step 3**.



Security Awareness Training FAQs:

How long does the training take?

- Training should take approximately 40 minutes to complete.

Do I have to complete the training in one sitting?

- No. You can start and stop the training at any point. When you return to finish the training, make sure you click "resume" to pick up where you left off.

What does the training consist of?

- The course is made up of case study-based videos that provide real-life examples of incidents that can happen to anyone, at any time, along with "lessons learned", which will provide details on the incident, the outcome, and how it could have been avoided.

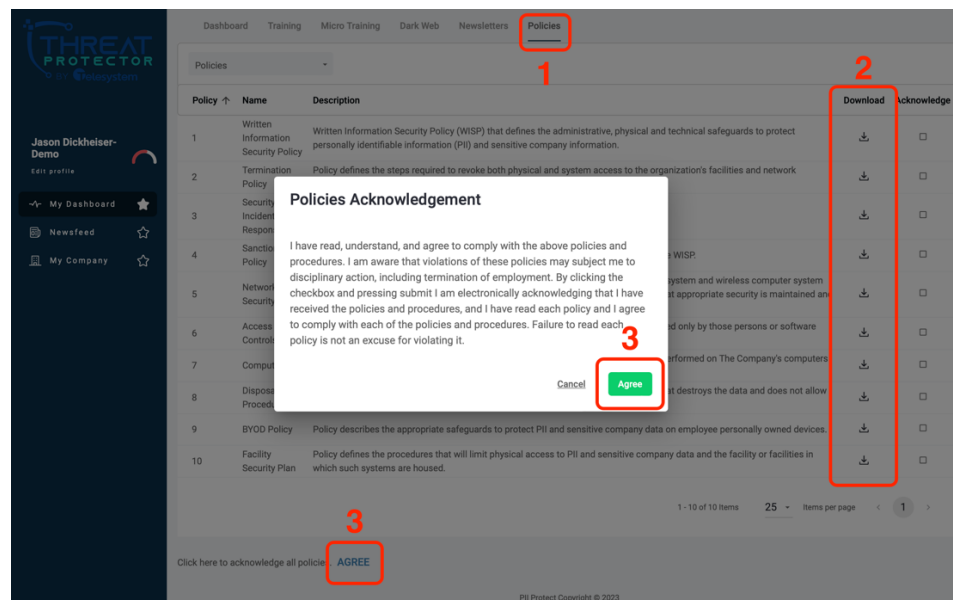
How do I get credit for completing the training?

- You must complete a 20-question quiz following the course. You will need to receive a passing score of 80% to satisfy this requirement. Upon successful completion, you will receive a training certificate indicating that you have passed the course.

How to Acknowledge Policies & Procedures

Getting Started

1. In the **My Dashboard** section, select the **"Policies"** tab at the top of the page.
2. Here you will see your policies & procedures. Click each policy to view the quick description. The full policy can be downloaded and viewed.
3. Once you have read and understand all the policies & procedures, you're ready to acknowledge your cooperation with your organization's policies & procedures. To do so, click **"Agree"** at the bottom of the page. In the confirmation box that appears click **Agree** to indicate your acknowledgement.



Policies & Procedures FAQs:

Why do I have to acknowledge policies & procedures?

- You can't follow the rules if you don't know them, right? That's why it is extremely important that you know about each one of your organization's policies & procedures. Not only do you need to know these policies & procedures exist, but you must understand them and agree to comply with them.

Are the policies and procedures built into the portal?

- Yes. All of your policies and procedures have been uploaded into one convenient location for you to reference.

What if I have questions or don't understand one of the policies or procedures?

- It is critical that you understand expectations with all policies and procedures. If you have any questions or would like to discuss any of these items, please contact a member of your organization's management team.

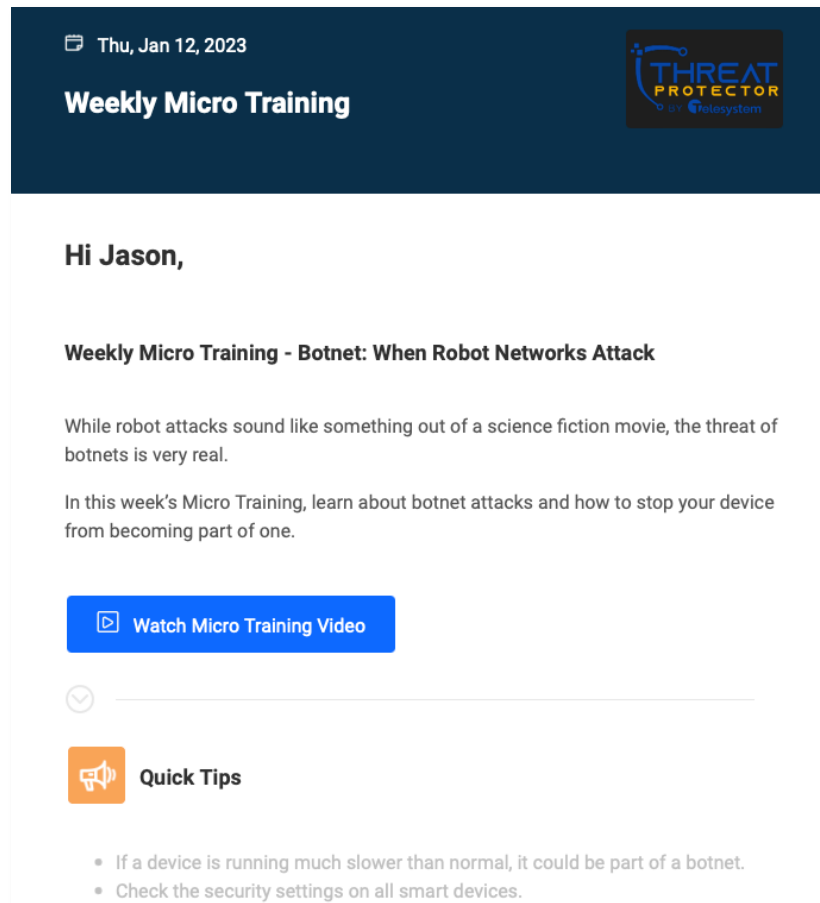
What do I do after I've reviewed and understand all our policies and procedures?

- Once you've gone through each one of our policies and procedures and understand expectations, you're ready to electronically acknowledge that you agree to abide by them.

Micro-Training Videos & Quizzes

Weekly Email

Each week you'll receive an email from No-reply@security-reminders.com with a link to our weekly Micro-Training videos



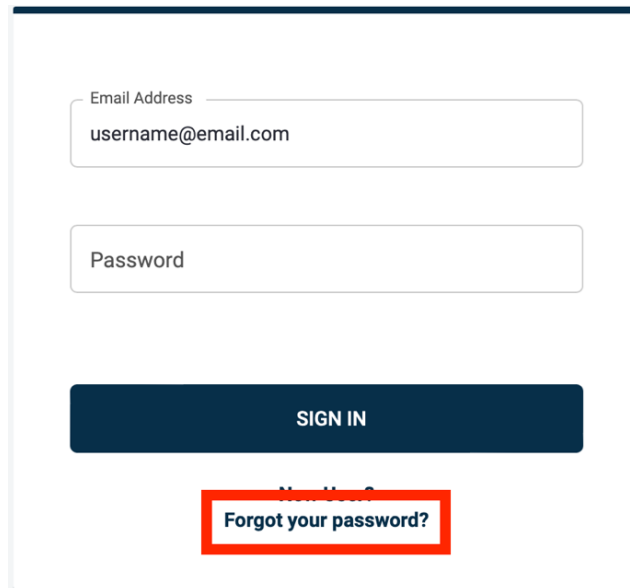
Important Information

- Videos are typically between 2-3 minutes long.
- Following the video, you will see a short 4-question quiz based on the content you just watched.
- The more quizzes you take, the higher your ESS, so take the 5-minute break and educate yourself on what to lookout for this week!
- You will receive a micro-training email every week. 3 weeks out of the month the email will contain a video and a quiz. Once per month your micro-training email will include a Security Newsletter.

Resetting Your Password

Did you forget your password? No problem! Follow these steps and we'll promptly email you a new one!

1. On the login page, Enter your Email Address then click **"Forgot Your Password?"**

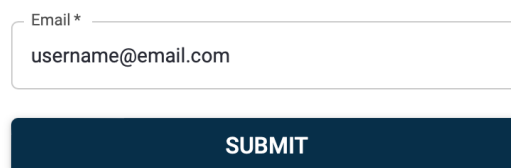


The image shows a login form with two input fields: 'Email Address' containing 'username@email.com' and 'Password'. Below the fields is a dark blue 'SIGN IN' button. Underneath the button is a link that says 'New User?' followed by 'Forgot your password?'. The 'Forgot your password?' link is highlighted with a red rectangular border.

2. Enter your email address you registered with or the one that was used by your organization to register you. Click **"Submit"**.

Forgot Your Password?

Please enter the email address that you registered with.



The image shows a form for resetting a password. It has a single input field labeled 'Email *' containing 'username@email.com'. Below the field is a dark blue 'SUBMIT' button.

3. An email will be sent to the address you entered in the step above with a prompt to reset your password.

Still having trouble resetting your password? Reach out to Telesystem support and we will be happy to help!

Cybersecurity is a Continuous Process

Cybercriminals never stop learning new tricks to get into our network and our data, which means we can't stop learning either!

You've done the basics! Thank you for your help in keeping our workplace safe! Keep it up! We know you're busy and we appreciate all your hard work. Help us protect each other by staying up to date. Keep in mind, it takes all of us to stop cybercriminals!



Remember, having a strong cybersecurity program is critical for many reasons, including having strong safeguards to fight cybercriminals, and most importantly to protect the client data we store, access, or transmit.

Thank you for doing your part!