Breach Prevention Platform

Employee Cybersecurity Program

Management User Guide

Table of Contents

Know what you're looking for? Jump to the page below!

Successfully Implementing the BPP

This cybersecurity-based program uses ongoing education, gamification, and easy to understand topics to implement proactive security controls to reduce the likelihood of a security incident.
In this guide you will find helpful tips and information to help you roll-out the Breach Prevention Platform (BPP) to your employees. At the heart of the BPP is EVA, our Employee Vulnerability Assessment, which is designed to provide continuous security training to promote a security-focused company culture.

What to expect with the BPP:

Micro-Trainings: Each week we will send out a Micro-Training video via email to you and your employees. These videos are typically 2-3 minutes long and keep you up-to-date with the latest cybersecurity threats. After watching the video, you will want to complete the simple 4 question quiz attached. In total, this should take less than 5 minutes to complete. Watching these weekly security tip videos and completing the quizzes will help improve your Employee Secure Score (ESS), so make sure you do so in a timely basis!

Tip: Sending out reminder emails to your employees to complete these will go a long way!

The Leaderboard: The leaderboard makes this fun for you and your employees! Get creative with your screen name and work your way to the top of the leaderboard by improving your ESS!

Tip: Set the tone with your username and have some fun!

Dark Web Scans: In addition to continuous dark web monitoring of your organization’s domain, BPP also allows you to scan the dark web to find out if your personal information is already out there. The more you know, the better you can protect yourself. This free tool allows you and your employees to scan your personal, friends’, or family members’ email addresses as much as you’d like, so use this tool as you see fit!

Tip: Stay up to date on your accounts and remember to check for any new breaches periodically!

Successfully Implementing the BPP

This cybersecurity-based program uses ongoing education, gamification, and easy to understand topics to implement proactive security controls to reduce the likelihood of a security incident.
In this guide you will find helpful tips and information to help you roll-out the Breach Prevention Platform (BPP) to your employees. At the heart of the BPP is EVA, our Employee Vulnerability Assessment, which is designed to provide continuous security training to promote a security-focused company culture.

What to expect with the BPP:

Security Risk Assessment (SRA): A main component in identifying where your security vulnerabilities lie is with taking an annual Security Risk Assessment (SRA). This comprehensive SRA allows you to see where your security posture lies and put together a long-term plan for working towards becoming cyber-secure.

Tip: Complete the SRA annually and remain on a consistent schedule as years go on.

Annual Security Training: With an emphasis on case studies of real events, users of this training platform will learn practical lessons on how they can lower protect your data & information. A training certificate is provided to employees upon completion of the final quiz..

Tip: Require your employees to complete their training and quiz by a certain deadline.

Security Policies and Procedures: We know writing hundreds of pages of policies can be a daunting task. With this program, we've spared you the effort and expense of having to write your own policies. This program comes Security Policies and a full Privacy Manual. Each policy is complete and uploaded with your organization's name on every document.

Tip: Encourage all staff to read and acknowledge all policies and procedures in a timely manner.

Successfully Implementing the BPP

This cybersecurity-based program uses ongoing education, gamification, and easy to understand topics to implement proactive security controls to reduce the likelihood of a security incident.
In this guide you will find helpful tips and information to help you roll-out the Breach Prevention Platform (BPP) to your employees. At the heart of the BPP is EVA, our Employee Vulnerability Assessment, which is designed to provide continuous security training to promote a security-focused company culture.

What to expect with the BPP:

Employee Vulnerability Assessment (EVA): EVA is an employee risk detection solution that analyzes vital security metrics like dark web compromises, simulated phishing fail rate, security training scores, and policy acknowledgement to identify your organization's human security risks. Based on these metrics, each employee is assigned an Employee Secure Score (ESS). The lower the ESS score, the less secure they are, thus the higher the risk to your organization. EVA allows you to see which employees are on track as well as which employees pose the highest risk to your organization and strengthens them with ongoing education.

Tip: Use the Employee Secure Score (ESS) report as a metric of evaluation for your employees on a regular basis.

Successfully Implementing the BPP

One of the key contributors to a security program's success is top-down buy-in. That means as a leader, you too must take security, seriously. To help you do this, we recommend including cybersecurity in your employee evaluations and quarterly reviews. Leverage the Employee Secure Score (ESS) Report inside the PII Protect portal, as a standardized HR item, employees will understand the seriousness of protecting their data by knowing that their scores are more than just a number but provide insight into their security hygiene.

Keep it fun but stress the importance of caring about cybersecurity, at work and at home.

TRAIN

The first step with BPP should be requiring the staff to complete their annual Security Training. This annual training will help boost every employee's ESS.

ENGAGE

Get employees to complete Micro-Training and quizzes weekly. Automatic emails will be sent from no-reply@security-reminders.com with a link to these weekly videos, but setting standards is key!

UPDATE

Get employees to update their ESS regularly. Include this as an evaluation metric and stress the importance of cybersecurity. You can help strengthen your weakest links!

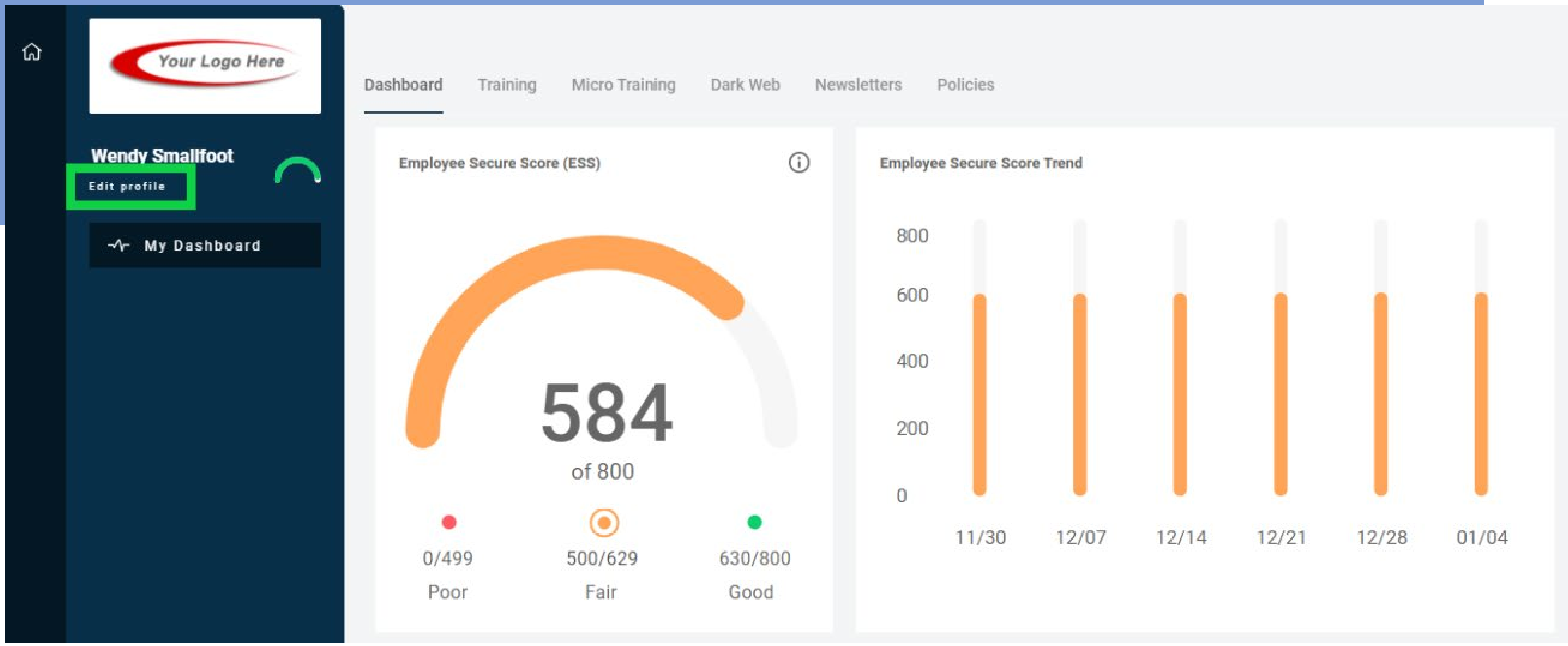
How do I get started & ensure I'm setting a good example?

Success starts with you. By setting the example that this program is to be taken seriously and that no one, not even you, is safe from the threats cybercriminals pose each day.

LOGIN & GET STARTED

1. Login to the portal here: https://portal.pii-protect.com/#/login
2. Complete your profile
3. Claim your screen name and start climbing up the leaderboard by pressing Edit Profile at the top of the dashboard

   Tip: Be creative! Set the tone for your organization by choosing a fun name!



Complete Security Awareness Training

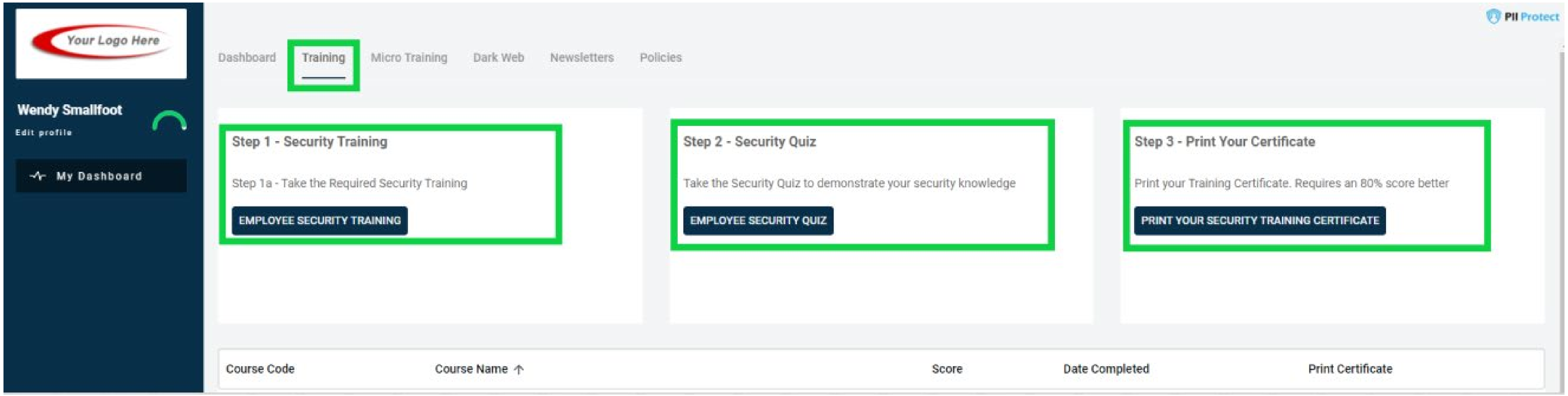
This should take approximately 45 minutes to complete. This training includes case-study based videos to provide an example of how incidents can happen to anyone.

During this course, you can stop and start any time. In order to get credit for this course, you must complete a 20-question quiz that will impact your Employee Secure Score, so you'll want to pay attention!

TAKE TRAINING

At the top of your dashboard, click the "Security Training" tab to get started!

Set a date training MUST be completed by and ensure you're checking-in with those who may be falling behind.



Step 1 - Security Training

Step 1a - Take the Required Security Training

Step 2 - Security Quiz

Take the Security Quiz to demonstrate your security knowledge

Step 3 - Print Your Certificate

Print your Training Certificate. Requires an 80% score better

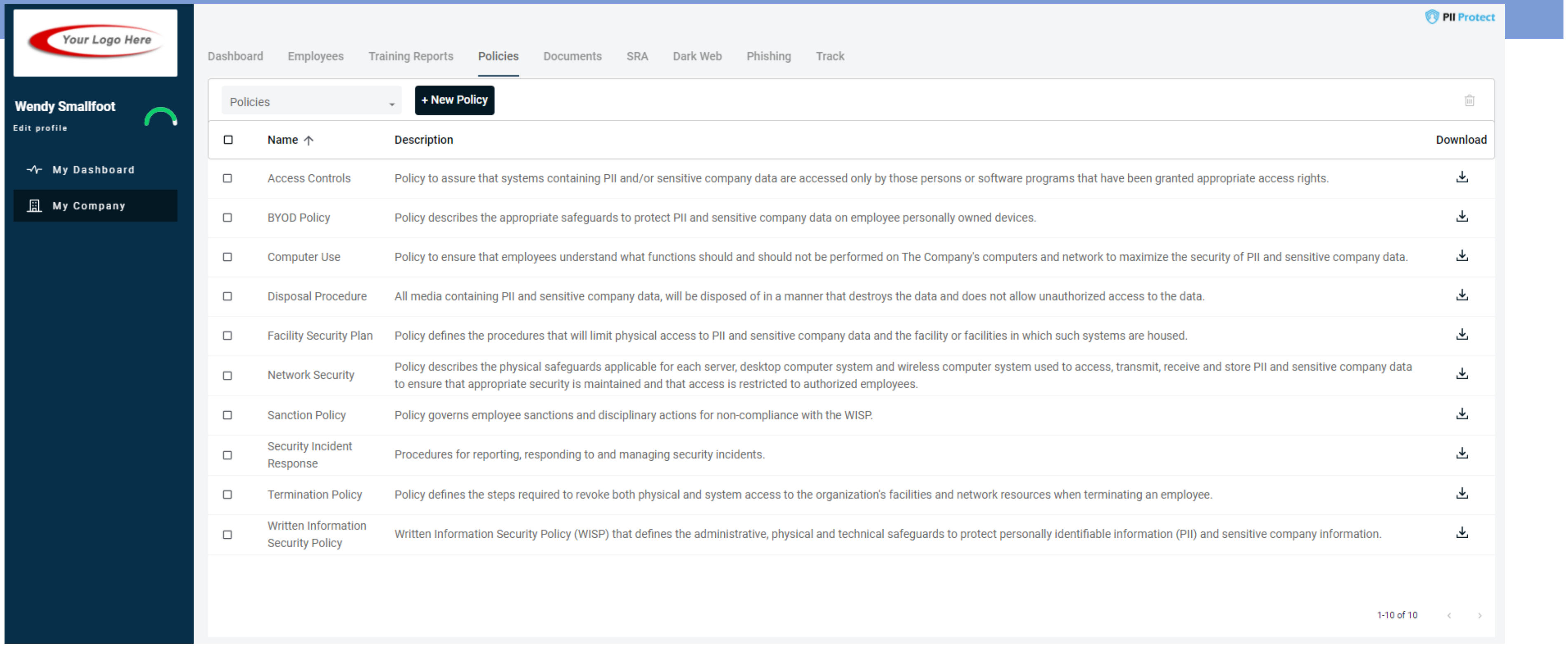
Course Code	Course Name ↑	Score	Date Completed	Print Certificate

Acknowledge Security Policies & Procedures

Your security policies have been uploaded into one convenient location for you to reference. If you would like any changes to any of the documents, please contact us at [Email Address].

Tip: Set a date these MUST be signed off on and ensure all employees have acknowledged the policies.

In the My Company section, click the "Policies" tab. Once these policies are approved and adopted, each employee can review the policies and sign-off that they've read and understand the content.

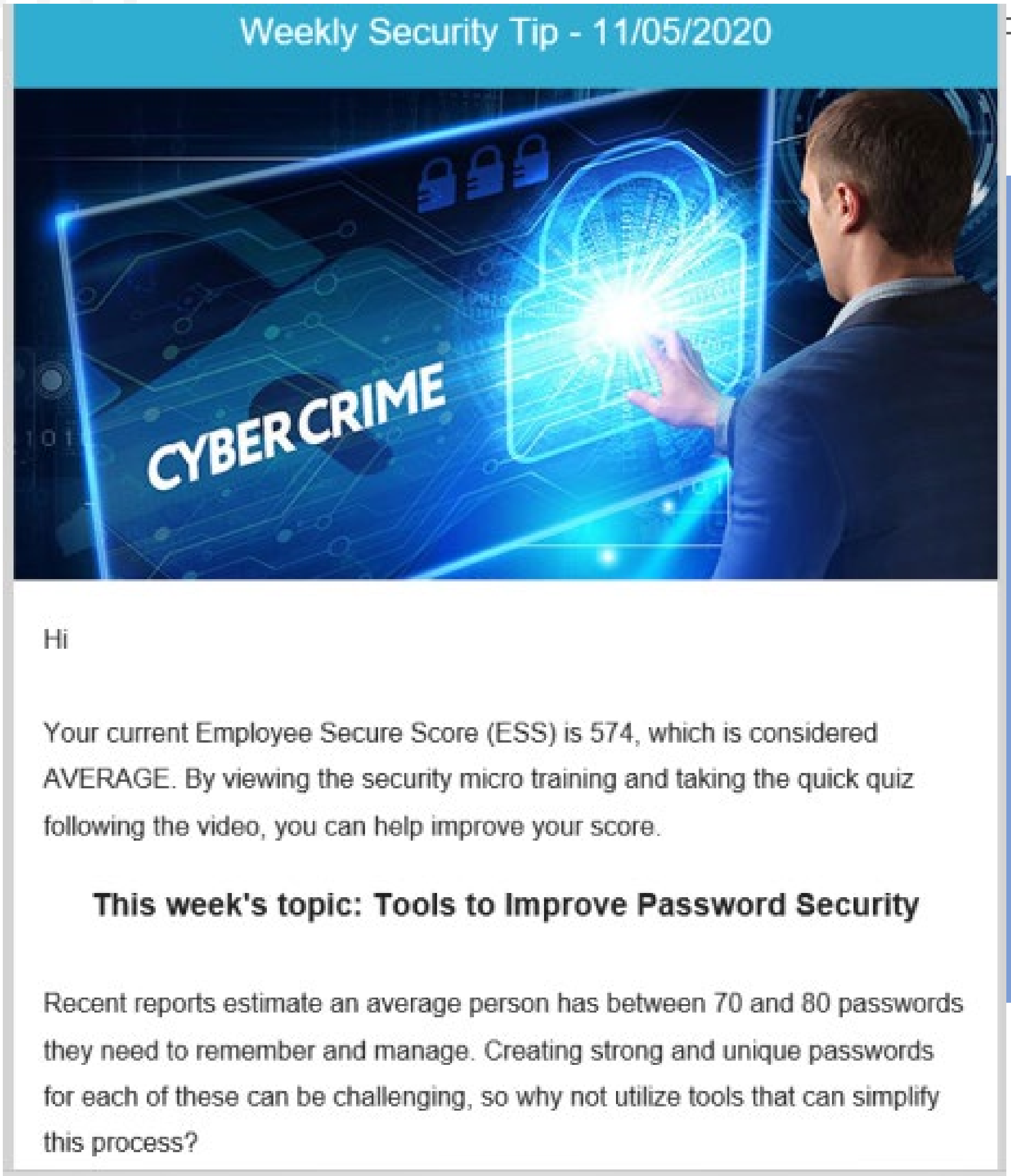


☐	Name ↑	Description	Download
☐	Access Controls	Policy to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights.	⤓
☐	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices.	⤓
☐	Computer Use	Policy to ensure that employees understand what functions should and should not be performed on The Company's computers and network to maximize the security of PII and sensitive company data.	⤓
☐	Disposal Procedure	All media containing PII and sensitive company data, will be disposed of in a manner that destroys the data and does not allow unauthorized access to the data.	⤓
☐	Facility Security Plan	Policy defines the procedures that will limit physical access to PII and sensitive company data and the facility or facilities in which such systems are housed.	⤓
☐	Network Security	Policy describes the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.	⤓
☐	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.	⤓
☐	Security Incident Response	Procedures for reporting, responding to and managing security incidents.	⤓
☐	Termination Policy	Policy defines the steps required to revoke both physical and system access to the organization's facilities and network resources when terminating an employee.	⤓
☐	Written Information Security Policy	Written Information Security Policy (WISP) that defines the administrative, physical and technical safeguards to protect personally identifiable information (PII) and sensitive company information.	⤓

1-10 of 10 ‹ ›

Complete Micro-Training Quizzes Regularly

Each week you'll receive an email from no-reply@security-reminders.com with a link to our weekly micro-training videos. Following each video, you will see a short quiz based on the content.



Weekly Security Tip - 11/05/2020

Hi

Your current Employee Secure Score (ESS) is 574, which is considered AVERAGE. By viewing the security micro training and taking the quick quiz following the video, you can help improve your score.

This week's topic: Tools to Improve Password Security

Recent reports estimate an average person has between 70 and 80 passwords they need to remember and manage. Creating strong and unique passwords for each of these can be challenging, so why not utilize tools that can simplify this process?

Take a 5-minute break and educate yourself on what to look out for this week!

Take a break!

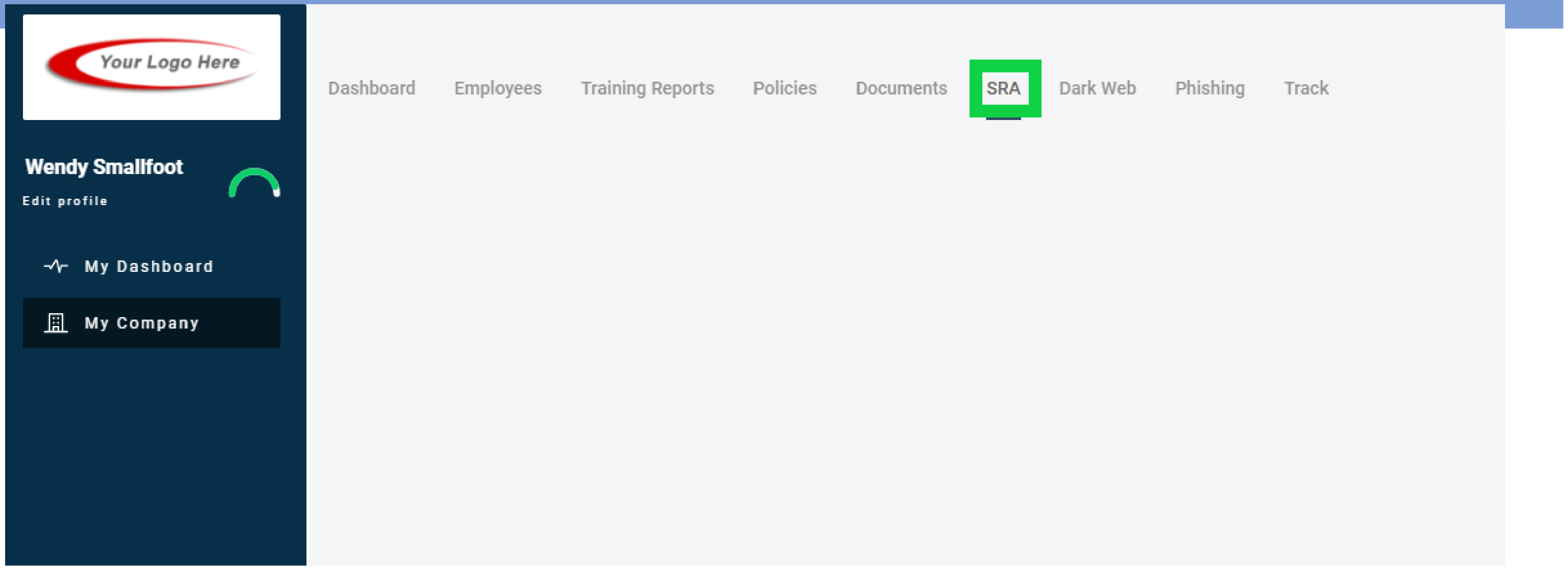
The more quizzes you take, the higher your ESS!

Complete Your
Security Risk Assessment Annually

It is important for all businesses to complete a thorough Security Risk Analysis (SRA) on their organization. An SRA can identify your organizations strengths and weaknesses. In the “My Company” section, click “SRA”.

This SRA takes about 1 hour to complete.

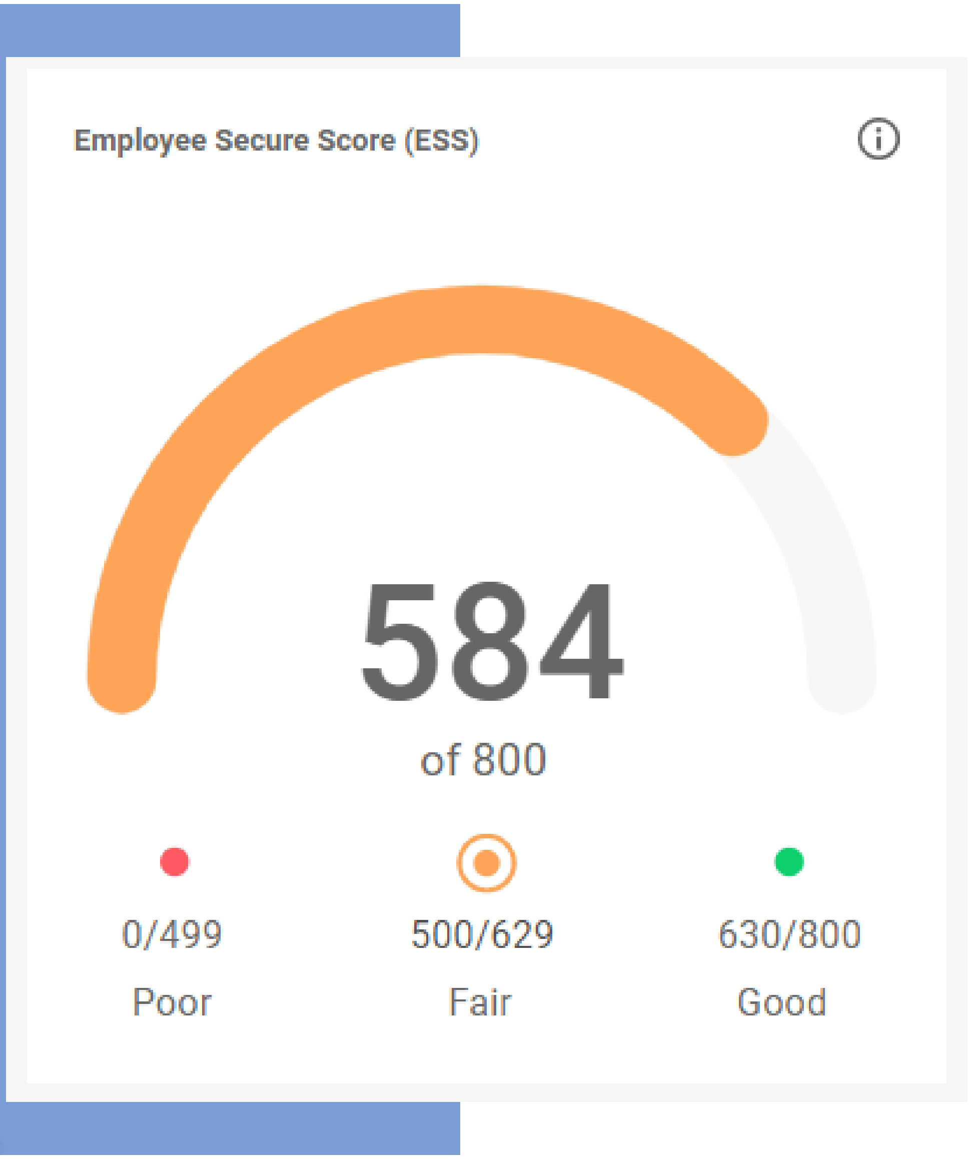
For more information on completing your SRA, click here.



Update Your Employee Secure Score Regularly

You've done the basics! Thank you for actively playing a role in your Security and Cybersecurity Program and setting an example for how important protecting patient information truly is. 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.

Cybersecurity is an Ongoing Process



Employee Secure Score (ESS)

584

of 800

● 0/499 Poor

◉ 500/629 Fair

● 630/800 Good

Managing the Cybersecurity Program Results

Navigating to your Reports

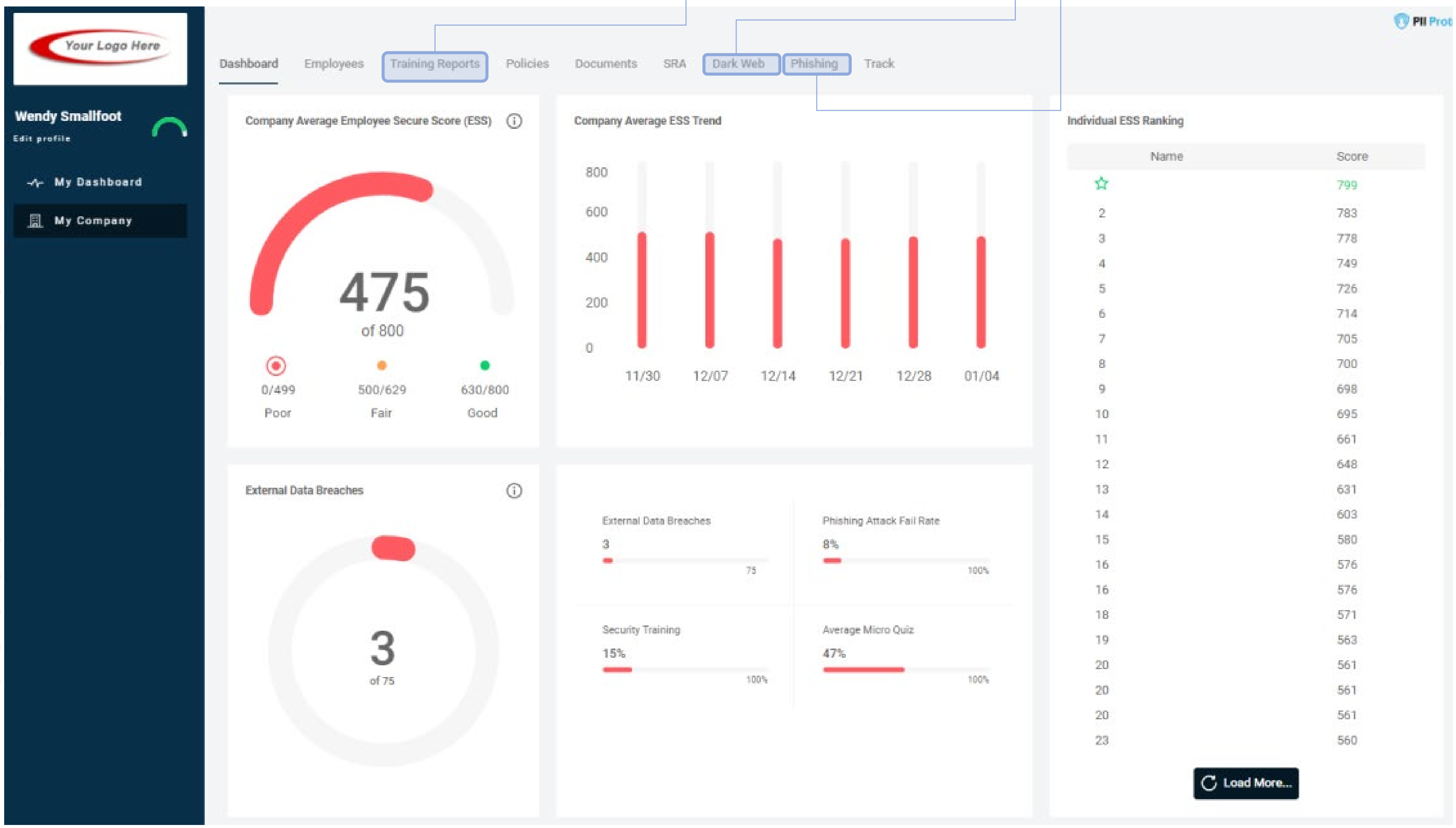
You must be in the “My Company” section to access the user reports.

You should be monitoring your manager reports monthly. Take time to evaluate your employees and help them stay on track. The fewer ‘high-risk’ employees you have, the better protected you are.

View the Training and Micro Training reports

View the Dark Web report

View the Phishing report



External Data Breaches 3 (75)

Phishing Attack Fail Rate 8% (100%)

Security Training 15% (100%)

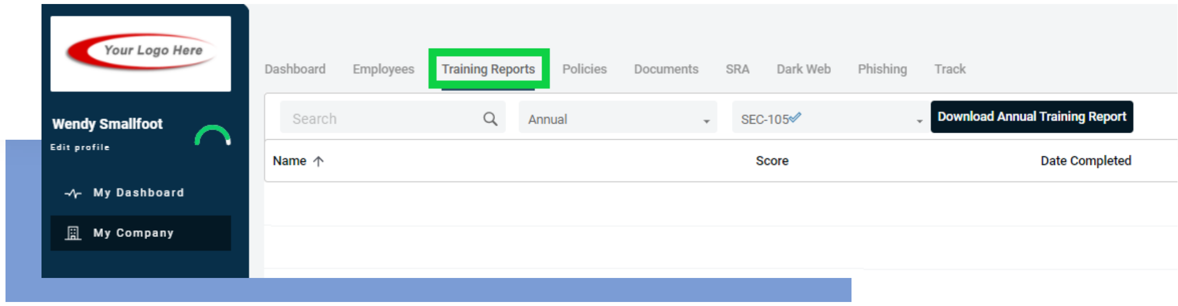
Average Micro Quiz 47% (100%)

Individual ESS Ranking

Name	Score
☆	799
2	783
3	778
4	749
5	726
6	714
7	705
8	700
9	698
10	695
11	661
12	648
13	631
14	603
15	580
16	576
16	576
18	571
19	563
20	561
20	561
20	561
23	560

On a quarterly basis, we recommend adding this report to your employee evaluations. Discuss with each employee their status and how they are helping protect your business and their personal information. Encouragement is key!

Access Annual Training Reports



Annual

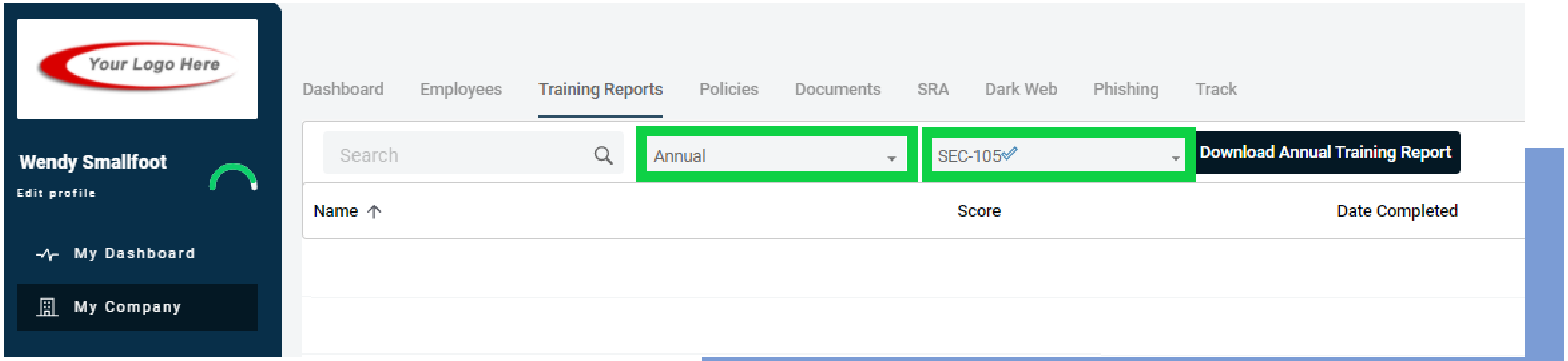
SEC-105

Name Score Date Completed

In the My Company section, click on the **“Training Reports”** tab.

To view the “Annual” training results, select “Annual” in the drop-down list. Here you can see the Full Report for all employees who have completed the training for the current module. It will show the employee name, score, date completed, and give you the option to access the Certificate for passing students. Previous training course results can be accessed by selecting the previous course codes from the drop-down list.

All staff must receive an 80% or higher on the final Quiz to pass & receive a certificate. Employee’s with scores lower than 80% should be encouraged to retake the training and quiz.

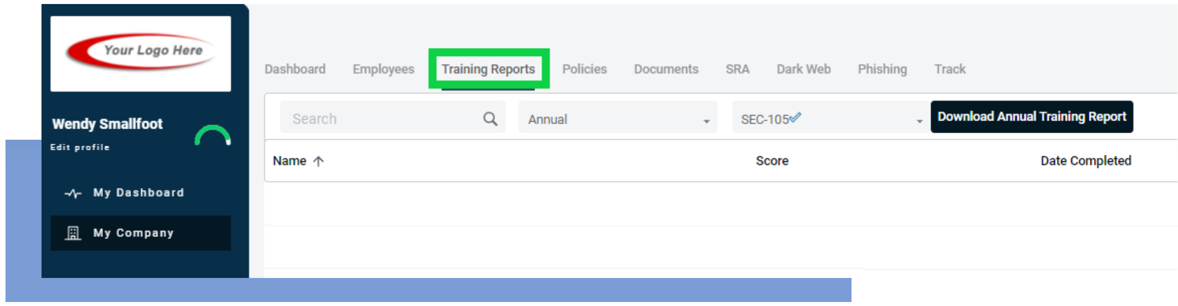


Annual

SEC-105

Name Score Date Completed

Access Micro Training Reports

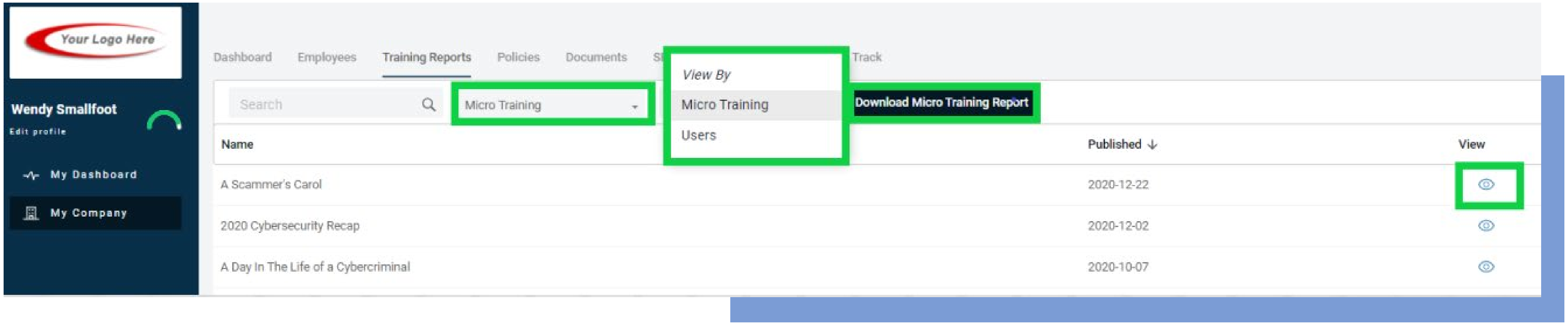


In the My Company section, click on the **“Training Reports”** tab.

To view the “Micro” training results, select “Micro Training” in the drop-down list. Here you can see the full list of Micro Trainings, beginning with the most recent. Selecting “View” will show the employees who had attempted that Micro Training Quiz and their score.

Additionally, you can view the Micro Training results for each individual employee. Using the dropdown selector, select View By “Users”. This will show each registered employee with the option to view their specific Micro Training results.

A Micro Training Report can also be downloaded providing the full results for all employees.

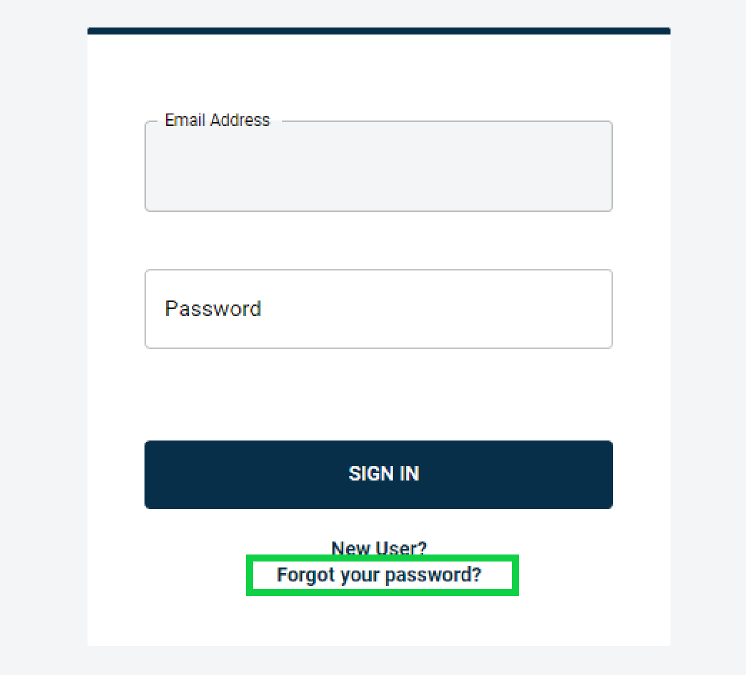


Name	Published ↓	View
A Scammer's Carol	2020-12-22	👁
2020 Cybersecurity Recap	2020-12-02	👁
A Day In The Life of a Cybercriminal	2020-10-07	👁

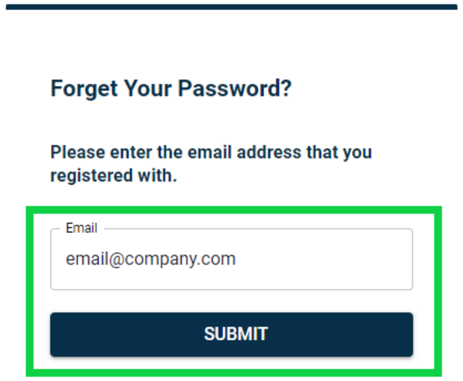
Resetting Your Password

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?"**



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



Forget Your Password?

Please enter the email address that you registered with.

Email: email@company.com

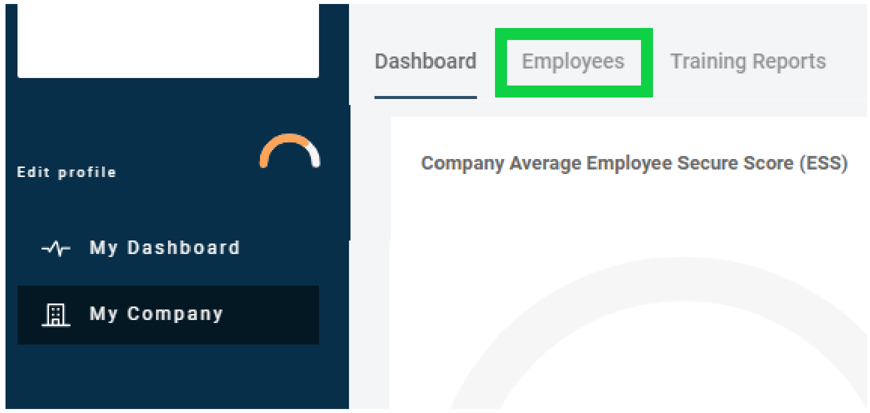
3. An email will be sent to the address you entered in the step above with a prompt to reset your password.

Having trouble resetting your password? Reach out to OXEN Technology and we'd be happy to help!

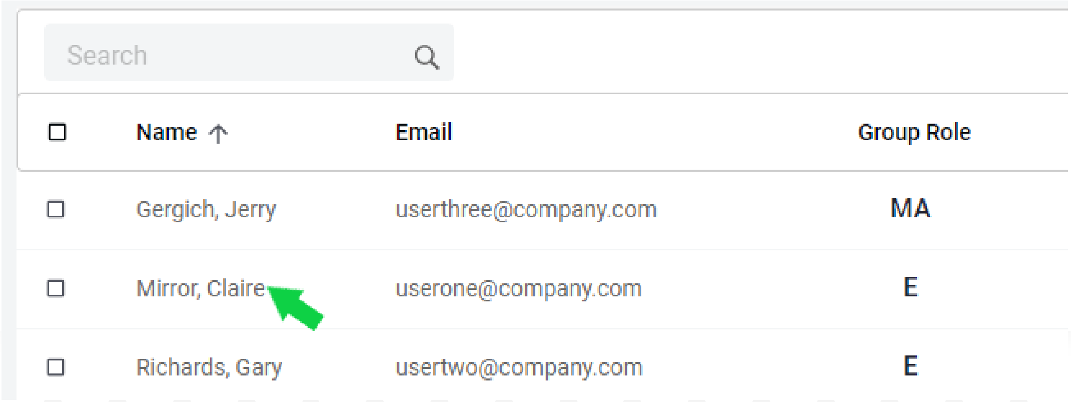
Resetting Employee Passwords

Need to reset an employee password or manage their account?

1. In the "**My Company**" section, click on the "**Employees**" tab.



2. Click on the employee you wish to adjust.



□	Name ↑	Email	Group Role
□	Gergich, Jerry	userthree@company.com	MA
□	Mirror, Claire	userone@company.com	E
□	Richards, Gary	usertwo@company.com	E

3. From here, you can adjust multiple aspects of all employee accounts, including creating a new password. Enter the new password in **"Password"** and then **"Confirm Password"**. Next, click the **"Submit"** button at the bottom to save the changes.