



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 Security Awareness Training (SAT) to your employees. At the heart of the SAT 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 SAT

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 the micro-trainings 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, SAT 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!

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 with 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.

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

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 SAT 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

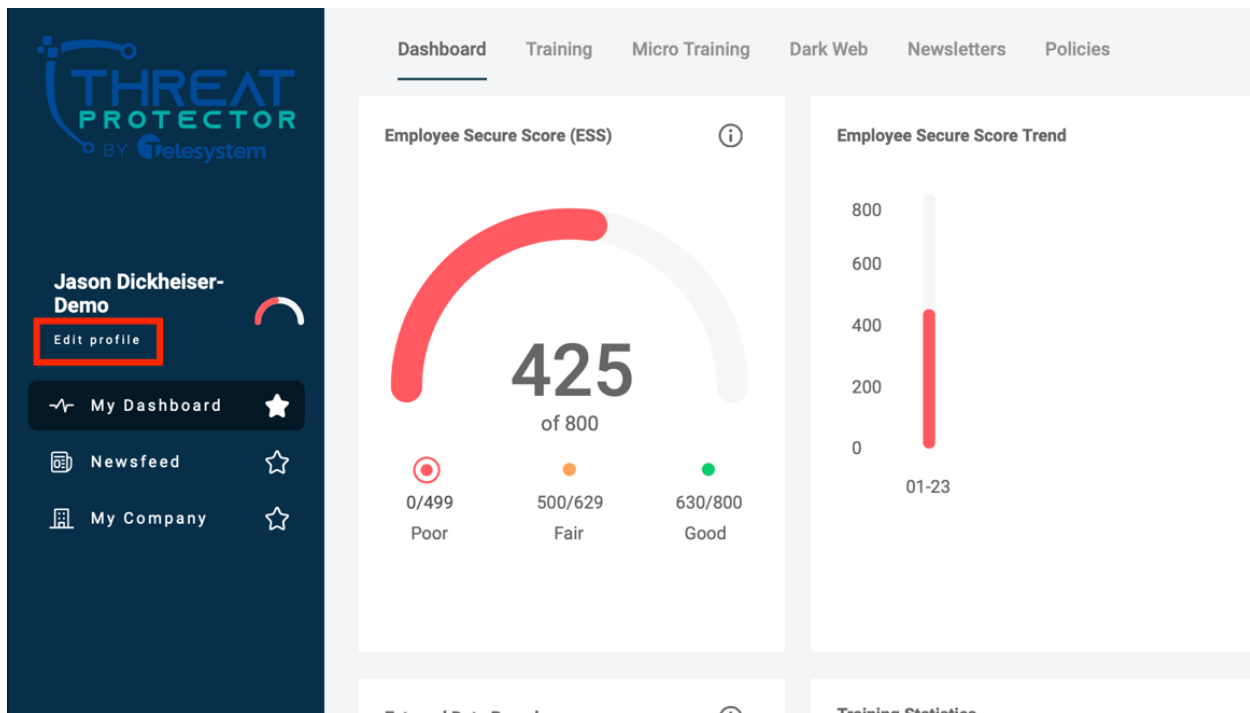
Get employees to update their ESS regularly. Include this as an evaluation metric and stress the importance of cybersecurity. You can help strengthen your weakest links!

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, are safe from the threats cybercriminals pose each day.

Login & Get Started

1. Login to the portal here: <https://portal.pii-protect.com/#/login>
 - a. Can't login? Contact us at support@telesystem.us
2. Complete your profile
 - a. Claim your screen name and start climbing up the leaderboard by pressing **Edit Profile** at the top of the dashboard
 - i. 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. 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

The screenshot displays the Threat Protector user interface. On the left is a dark blue sidebar with the logo and user profile for Jason Dickheiser-Demo. The main content area has a navigation bar with 'Training' highlighted. Below this is the 'Enrolled Courses' section, featuring a card for '2023 Cyber Manager Training' with a 'Watch' button and a 'Final Quiz' button. The 'Completed Courses' section contains a table with one entry: '2023 Cybersecurity Training' with a score of 100 and a completion date of 2023-01-26. The 'Print' button in the actions column is highlighted.

Course Code	Course Name	Score	Date Complete	Actions
SEC-107	2023 Cybersecurity Training	100	2023-01-26	Print Re-Watch Re-Take Quiz

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 support@telesystem.us

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

In the **My Dashboard** 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.

The screenshot shows the 'Policies' page in the Threat Protector application. The left sidebar contains the user's name 'Jason Dickheiser-Demo' and navigation links for 'My Dashboard', 'Newsfeed', and 'My Company'. The main content area features a table of 10 policies, each with a 'Download' icon and an 'Acknowledge' checkbox. At the bottom, there is a link to 'Click here to acknowledge all policies. AGREE'.

Policy	Name	Description	Download	Acknowledge
1	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.		<input type="checkbox"/>
2	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.		<input type="checkbox"/>
3	Security Incident Response	Procedures for reporting, responding to and managing security incidents.		<input type="checkbox"/>
4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.		<input type="checkbox"/>
5	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.		<input type="checkbox"/>
6	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.		<input type="checkbox"/>
7	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.		<input type="checkbox"/>
8	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.		<input type="checkbox"/>
9	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices.		<input type="checkbox"/>
10	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.		<input type="checkbox"/>

1 - 10 of 10 Items 25 Items per page < 1 >

[Click here to acknowledge all policies. AGREE](#)


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.

Take a 5-minute break and educate yourself on what to look out for this week. The more quizzes you take, the higher your ESS!

Thu, Jan 12, 2023

Weekly Micro Training




Hi Jason,

Weekly Micro Training - Botnet: When Robot Networks Attack

While robot attacks sound like something out of a science fiction movie, the threat of botnets is very real.

In this week's Micro Training, learn about botnet attacks and how to stop your device from becoming part of one.

[Watch Micro Training Video](#)

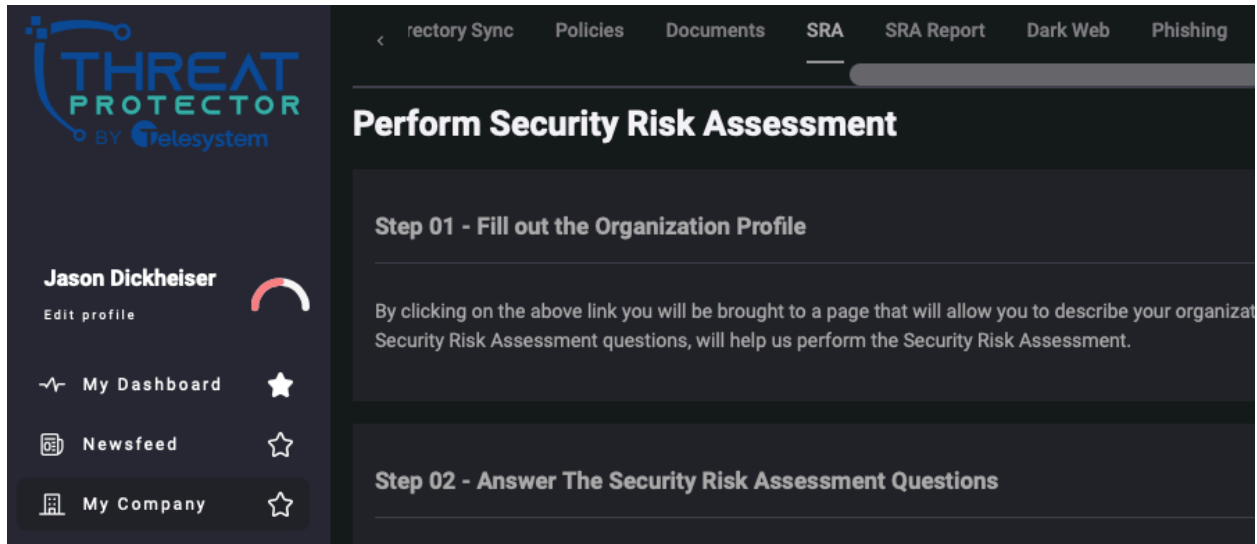
 **Quick Tips**

- If a device is running much slower than normal, it could be part of a botnet.
- Check the security settings on all smart devices.

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”.

The SRA takes about 1 hour to complete and if you have any questions on the content, please contact us at support@telesystem.us.



The screenshot shows the Threat Protector SRA interface. The top navigation bar includes: < rector Sync Policies Documents SRA SRA Report Dark Web Phishing. The main heading is "Perform Security Risk Assessment". Below this, there are two steps: "Step 01 - Fill out the Organization Profile" and "Step 02 - Answer The Security Risk Assessment Questions". The left sidebar shows the user profile for Jason Dickheiser, with options for "Edit profile", "My Dashboard", "Newsfeed", and "My Company".

Update Your Employee Secure Score Regularly

Cybersecurity is an ongoing process.

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.



Managing the Cybersecurity Program Results

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.

Navigating to your Reports

You must be in the **"My Company"** section to access the user reports.

The screenshot displays the Threat Protector dashboard with several key components:

- Navigation:** Top menu includes Training Configuration, Employees, Training Reports (highlighted), Directory Sync, Policies, Documents, SRA, SRA Report, Dark Web (highlighted), Phishing (highlighted), Track, and Employee Ass.
- Company Average Employee Secure Score (ESS):** A gauge chart showing a score of 415 out of 800, with a range from 0/499 (Poor) to 630/800 (Good).
- Company Average ESS Trend:** A bar chart showing scores over time: 12-19, 12-26, 01-02, 01-09, 01-16, and 01-23.
- External Data Breaches:** A gauge chart showing 2 breaches out of 10.
- Training Statistics:** Four progress bars: Phishing Attack Fall Rate (10%), Average Training Score (5%), Average Micro Quiz Score (24%), and Average Micro Quiz Taken (19%).
- Individual ESS Ranking:** A table listing employees by rank, name, tags, and score.
- Actions:** A 'Download ESS Report' button and a 'Tags Filter by tag 6+' dropdown.

Rank	Name	Tags	Score
1	Jason Dickheiser		694
2	Seth Gibbs		677
3	Kelle Bollman		667
4	Dominique Garl...		666
5	George Jewett		620
6	Seth Litzenberger		608
7	Carl Katz	Company A	580
8	Ira Feuerstein	sales	573
9	Brian Curran		564
10	Dawn McDonald		563
11	Patricia Shirey		561
12	Tom Binkowski		556
13	Mo Farhan		551
14	Nancy McGruder		533
15	Bill Wohlhagen		511
16	Paige Hofbauer		501
17	Dionte Pittman		425
18	Chris Schuette		400
18	Nikki Clark		400
20	Camille Lockett		390
20	Scott Levick		390
20	Jason Dickheiser		390

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

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

Name	Score	Date Completed ↓	View
Jason Dickheiser-Demo	100	2023-01-26	
Seth Gibbs	100	2023-01-19	
Kelle Bollman	80	2023-01-08	

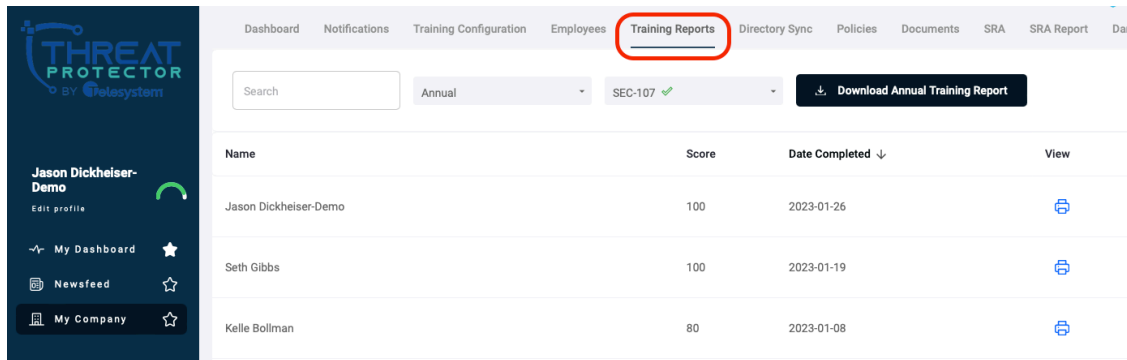
To view the **“Annual”** training results, select **“Annual”** in the drop-down list. Here you can see the Full Report for all employees who have completed the training for the current module. It will show the employee’s name, score, date completed, and give you the option to access the Certificate for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

Name	Score	Date Completed ↓	View
Jason Dickheiser-Demo	100	2023-01-26	
Seth Gibbs	100	2023-01-19	
Kelle Bollman	80	2023-01-08	

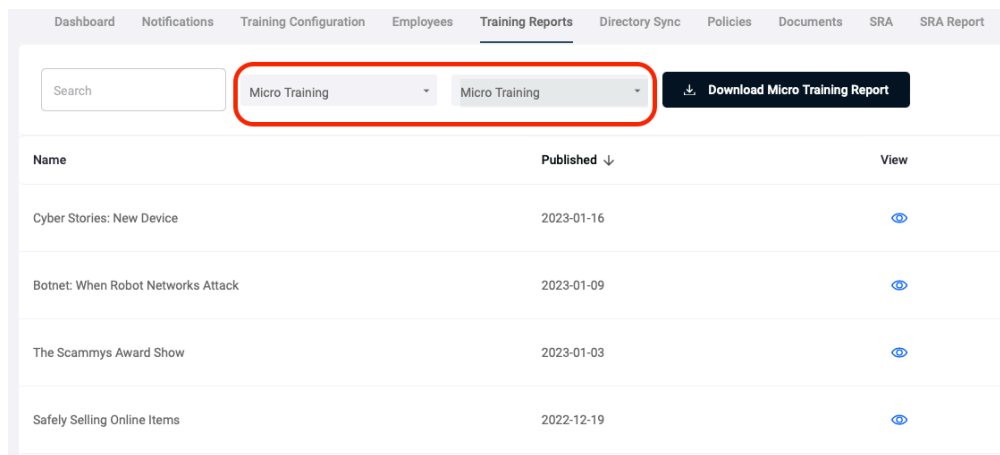
All staff must receive an 80% or higher on the Final Quiz to pass & receive a certificate. Employees with scores lower than 80% should be encouraged to retake the training and quiz.

Access Micro Training Reports

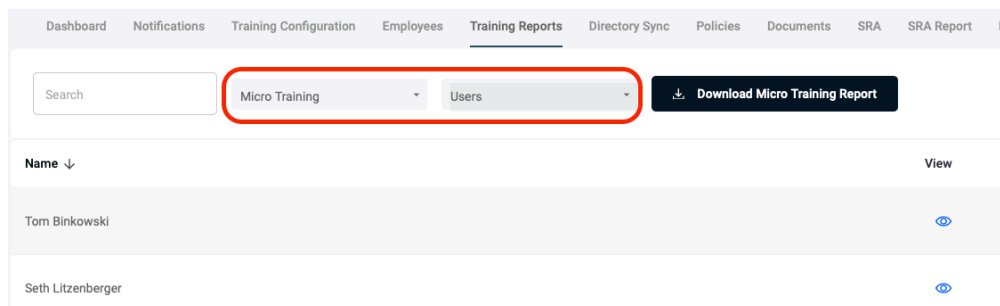
In the **My Company** section, click on the **“Training Reports”** tab.



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.

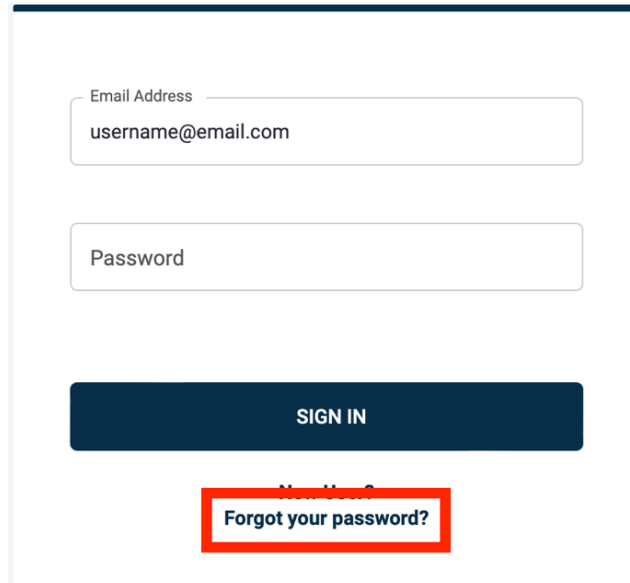


A Micro Training Report can also be downloaded providing the full results for all employees.

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?"**

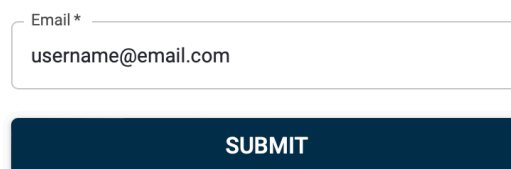


The screenshot shows a login form with two input fields: 'Email Address' containing 'username@email.com' and 'Password'. Below the fields is a dark blue 'SIGN IN' button. Underneath the button is a link that says 'New User?' with 'Forgot your password?' written below it. This link is highlighted with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

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 screenshot shows a form for password reset. It has a label 'Email *' above an input field containing 'username@email.com'. Below the input field is a dark blue 'SUBMIT' button.

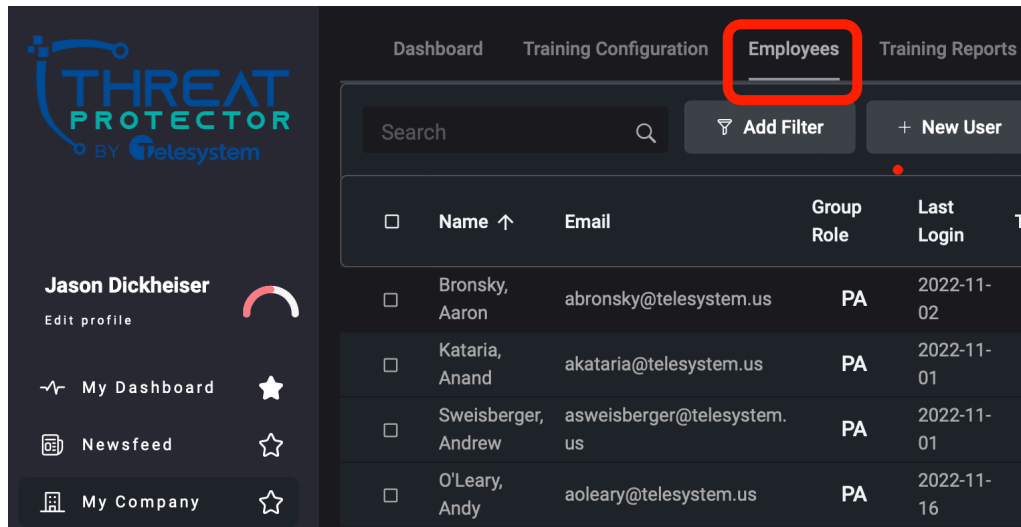
3. An email will be sent to the address you entered in the step above with a prompt to reset your password.

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

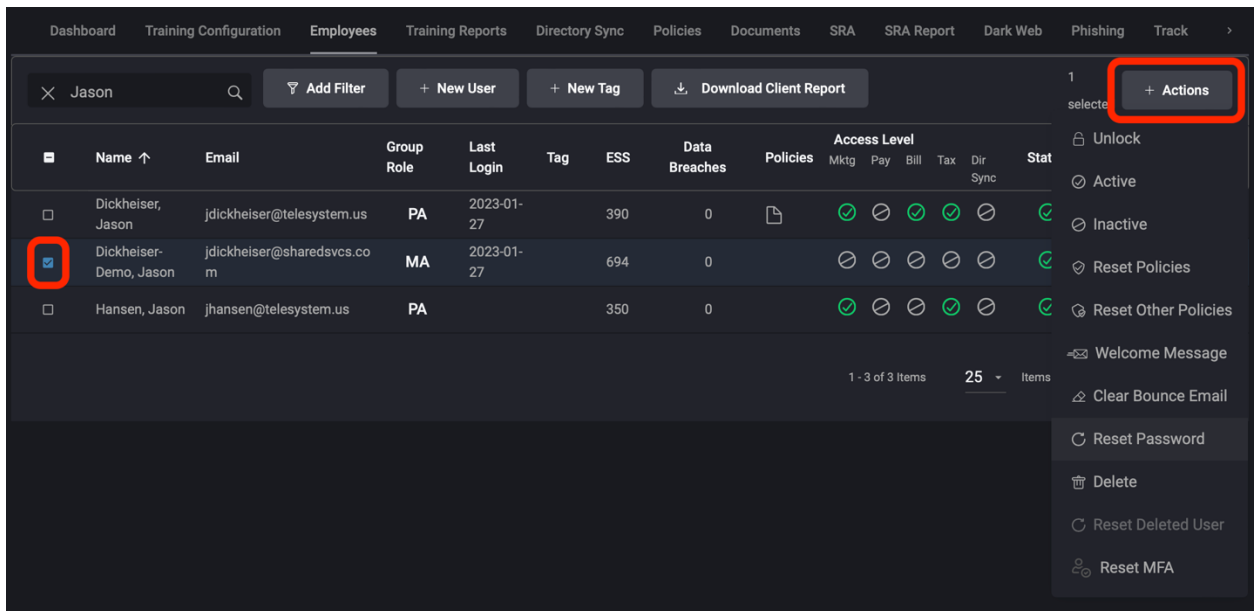
Resetting Employee Passwords

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 then click the **+Actions** button on the right side of the screen.



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.