



Understanding that drafting extensive policy documents can be an overwhelming challenge, we've designed this program to alleviate the burden. It includes 10 comprehensive, pre-written policies that we've identified as universally relevant to all organizations, saving you both time and resources.

Upon activating this feature, users gain access to these policies through the Security Awareness Training web portal. Here, they can easily view, download, and formally acknowledge the policies by navigating to the "Policies" section.

The screenshot shows the ThreatProtector web portal interface. The header includes the ThreatProtector logo, navigation tabs (Dashboard, Training, Micro Training, Dark Web, Newsletters, Policies), and a PII Protect icon. The main content area displays a table of 10 policies. The table has columns for Policy ID, Name, Description, Download, and Acknowledge. Below the table is a pagination control showing '1 - 10 of 10 Items' and '25 Items per page'. At the bottom, there is a link to 'Click here to acknowledge all policies. AGREE'.

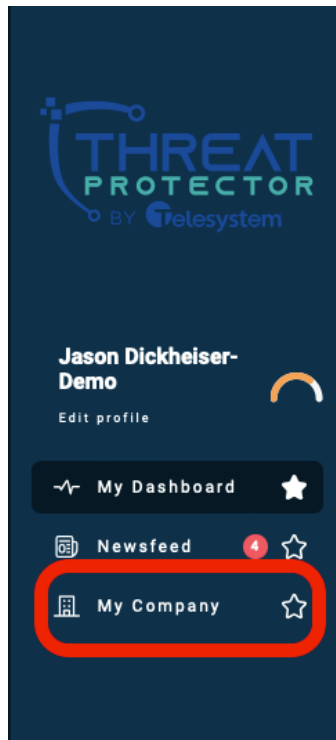
Policy	Name	Description	Download	Acknowledge
1	Written Information Security Policy	Written Information Security Policy (WISP) that defines the administrative, physical and technical safeguards to protect personally identifiable information (PII) and sensitive company information.		<input type="checkbox"/>
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"/>

Individuals assigned as **Administrator** or **Manager Admin** roles within an account are empowered with the flexibility to tailor the policy suite to their organization's specific needs. This includes the option to remove any of the 10 default policies provided and the capability to enrich the policy framework by uploading additional, organization-specific policies.

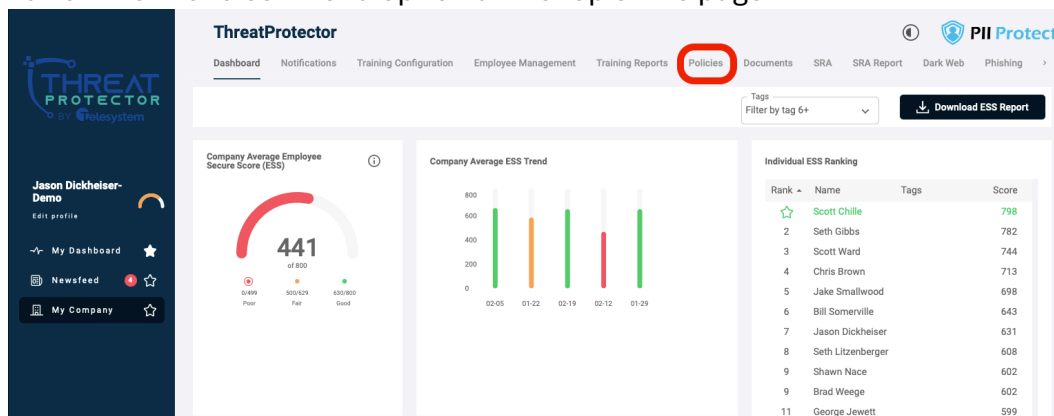
Deleting Policies


The steps outlined below will assist you in efficiently removing any policies from the Security Awareness Training web portal that you deem unnecessary for your organization.

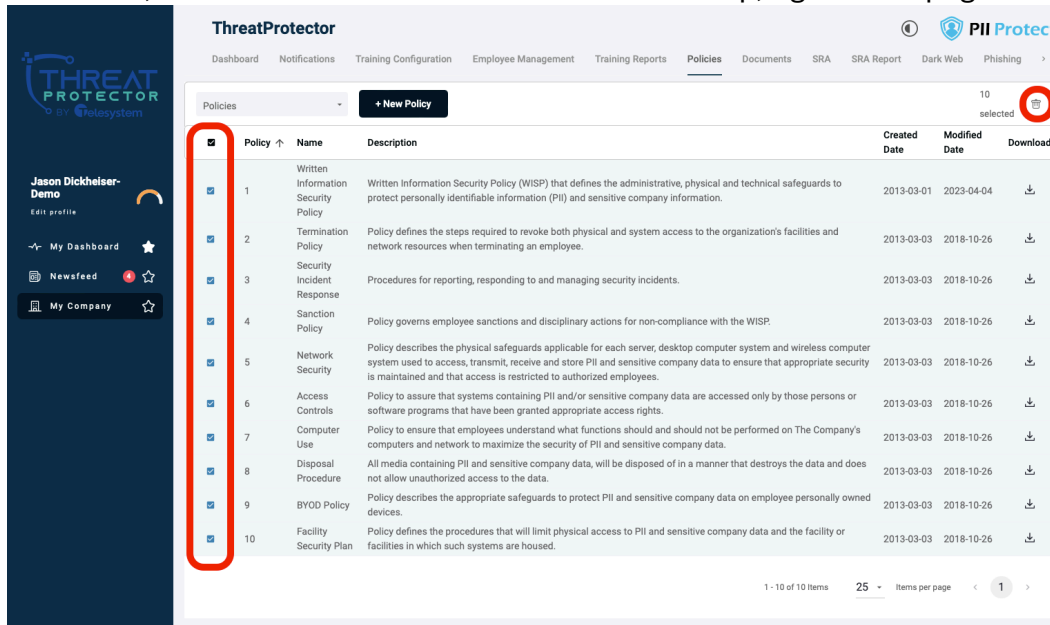
1. Login to the portal with a user account that has Manager Admin role assigned. The portal is accessible via compatible web browsers at <https://portal.pii-protect.com/>
2. Click on the link for “My Company” on the left-hand navigation pane.













3. Click on the “Policies” menu option at the top of the page.



4. Use the check boxes on the left of each row to select the policy or policies you wish to remove, then click on the trashcan icon  at the top, right of the page.



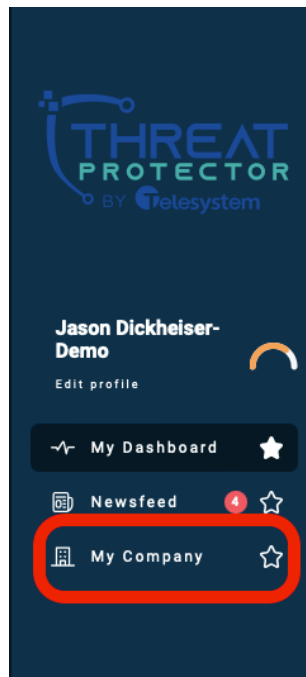
Policy	Name	Description	Created Date	Modified Date	Download
<input checked="" type="checkbox"/>	1	Written Information Security Policy	2013-03-01	2023-04-04	
<input checked="" type="checkbox"/>	2	Termination Policy	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	3	Security Incident Response	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	4	Sanction Policy	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	5	Network Security	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	6	Access Controls	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	7	Computer Use	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	8	Disposal Procedure	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	9	BYOD Policy	2013-03-03	2018-10-26	
<input checked="" type="checkbox"/>	10	Facility Security Plan	2013-03-03	2018-10-26	

5. Existing policies will be removed from the portal and not be accessible to any users within your organization.

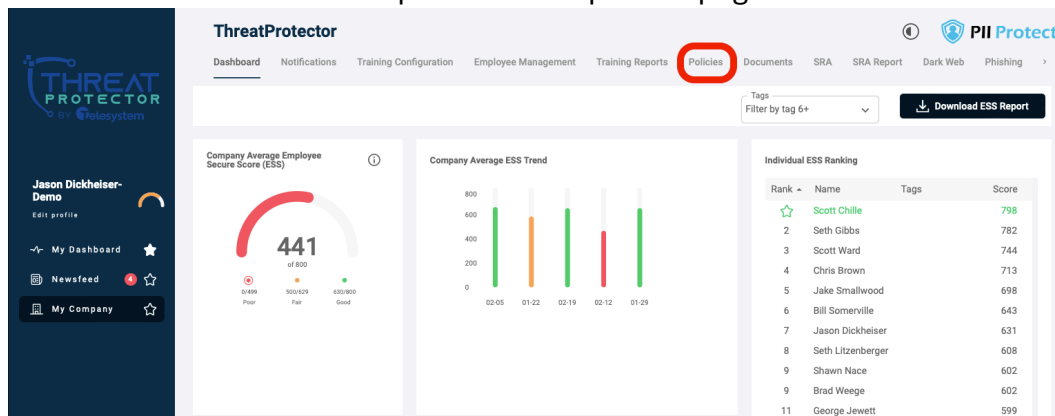
Add Custom Policies

The instructions provided below will lead you through the process of uploading policies to the Security Awareness Training web portal, facilitating the distribution of these important documents to members of your organization. After the policies are in place, users will have the ability to log into the portal to access, download, and formally acknowledge them.

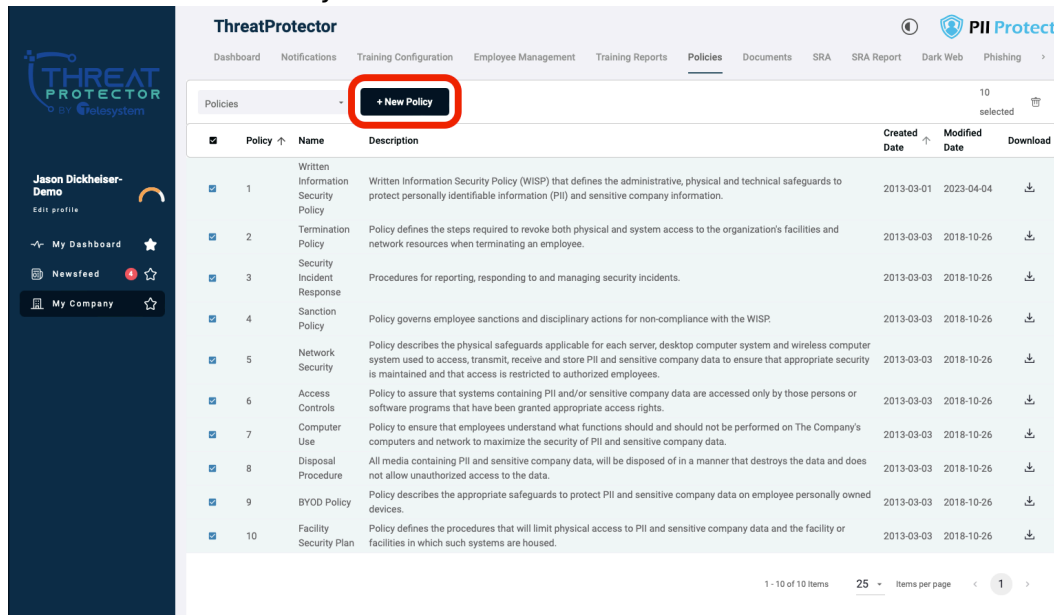
1. Login to the portal with a user account that has Manager Admin role assigned. The portal is accessible via compatible web browsers at <https://portal.pii-protect.com/>
2. Click on the link for “My Company” on the left-hand navigation pane.



3. Click on the “Policies” menu option at the top of the page.



4. Click on the “+New Policy” button.

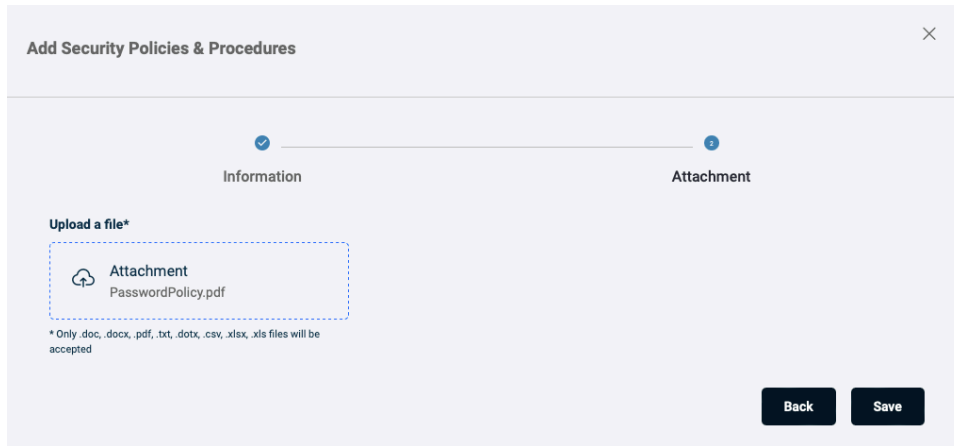


5. Provide a Name, Description, and Details for the policy. The name and description will display to users when they go to the “Policies” page of their Security Awareness Training Portal. The Details are what would display when a user clicks on the policy. We recommend the details contain the full text of the policy being added. You may only add one policy at a time. Fill out each of these required fields and then click “Next”.

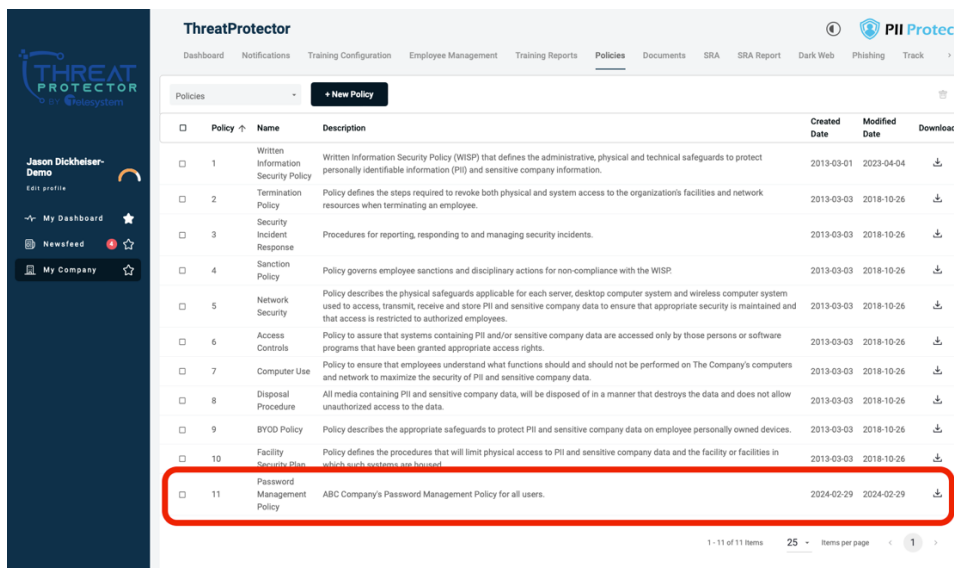
The screenshot shows the 'Add Security Policies & Procedures' form. The form is divided into two sections: 'Information' and 'Attachment'. The 'Information' section contains three required fields: 'Name *', 'Description *', and 'Details *'. The 'Name' field contains 'Password Management Policy'. The 'Description' field contains 'ABC Company's Password Management Policy for all users.' The 'Details' field contains 'Purpose: The purpose of this policy is to establish a standard for the creation, protection, and usage of passwords within [Organization Name]. This policy aims to protect the integrity and confidentiality of sensitive information by preventing unauthorized access.' A 'Next' button is located at the bottom right of the form.

- Add a downloadable version of the policy for users to save. Supported file types include: .doc, .docx, .pdf, .txt, .dotx, .csv, .xlsx, .xls.

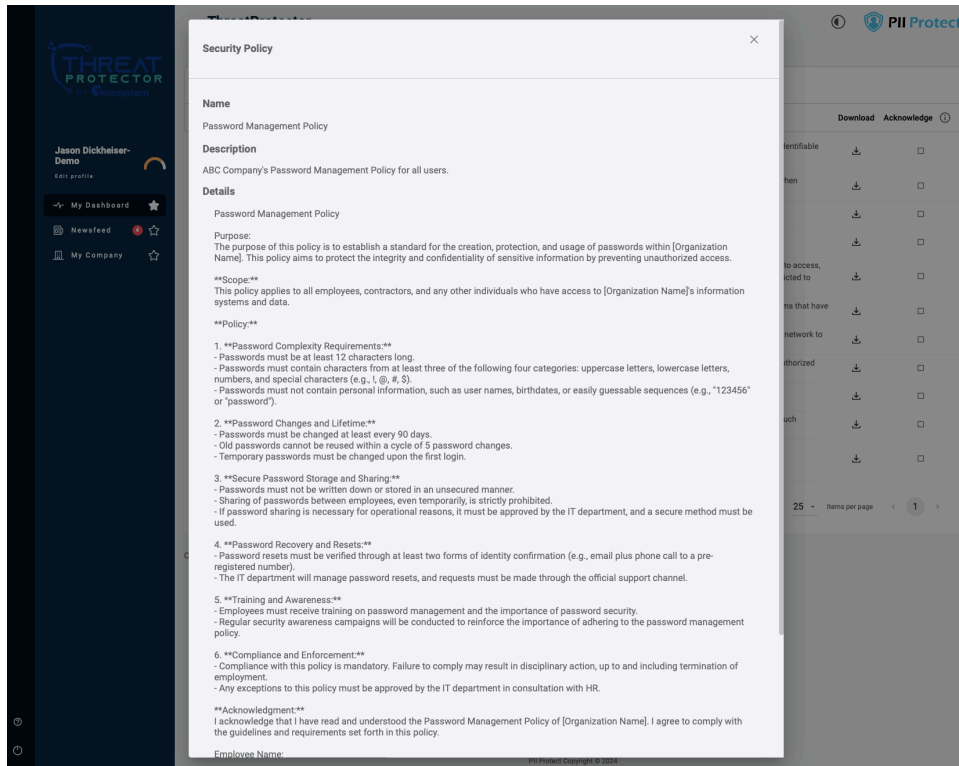
To upload a document you can drag and drop a file icon from your computer's local file directory to the portal or use the "Browse" link to access your computer's file storage and select the document. Once the file has been successfully uploaded (a "File Attached" message will briefly display at the bottom of the screen for approximately 3 seconds), click the "Save" button.



- The new policy will display at the bottom of the policy list. Note that unlike the default policies provided by Telesystem, policies you upload to the system will not have a download option on this page until you navigate away from the page and back again.



8. When end users login to their portal and navigate to **My Dashboard > Policies**, they will see the policy available to them. When users click on the policy, it will display the Name, Description and Details as shown below.



9. Users may then download the file copy of the policy that was uploaded and click the acknowledge they have read the policy.

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"/>
11	Password Management Policy	ABC Company's Password Management Policy for all users.	↓	<input type="checkbox"/>