

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.

	Thre Dashbo	atProtecto	DF Micro Training Dark Web Newsletters Policies	•	PII Protect
PROTECTOR BY Gelesystem	Policies				
	Policy 个	Name	Description	Download	Acknowledge (i)
Jason Dickheiser- Demo	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.	₹	
Edit profile	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.	₹	
- My Dashboard 🔶 國 Newsfeed 🚺 公	3	Security Incident Response	Procedures for reporting, responding to and managing security incidents.	₹	
圓 My Company 🏠	4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.	₹	
	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.	₹	
	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.	4	
	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.	4	
	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.	₹	
	9	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices.	*	
	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.	4	
			1 - 10 of 10 Items 25 -	ltems per page	< 1 →
	Click here to a	cknowledge all po	icies. AGREE		

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.

	ThreatProtector		Image:	tect
BY Pelesystem	Uashooard Notrications Fraining	omguration Employee Management Iraining Reports	Policies Jocuments SKA SKA Neport Juan Web Philaning	, t
	Company Average Employee (j) Secure Score (ESS)	Company Average ESS Trend	Individual ESS Ranking	
Jason Dickheiser- Demo		800	Rank - Name Tags Score	
Edit profile		600	☆ Scott Chille 798	
	441	400	2 Seth Gibbs 782	
we my basilooald	of 800	200	3 SCOtt Ward 744	
圆 Newsfeed 🛛 🖒	• •		5 Jake Smallwood 698	
🖩 My Company 🖒	Poor Fair Good	02-05 01-22 02-19 02-12 01-29	6 Bill Somerville 643	
			7 Jason Dickheiser 631	
			8 Seth Litzenberger 608	
			9 Shawn Nace 602	
			9 Brad Weege 602	
			11 George Jewett 599	

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 \overline{m} at the top, right of the page.

• ~ ~	Th	reatPro	tector	©		rotect	
PROTECTOR BY Prelesystem	Policie	25	-	Anny Conngulation Exployee management maning reports Forders Occurrents and and report of Anne Policy	10 selected		
		Policy 个	Name	Description Created Date	Modified Date	Download	
Jason Dickheiser- Demo	2	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.	2023-04-04	¥	
-√ My Dashboard 🔺		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. 2013-03-03	2018-10-26	Ŧ	
國 Newsfeed 🛛 🖒		3	Security Incident Response	Procedures for reporting, responding to and managing security incidents. 2013-03-03	2018-10-26	₹	
III My Company 🟠		4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP. 2013-03-03	2018-10-26	₹	
		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 PTI and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.	2018-10-26	₹	
		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.	2018-10-26	Ŧ	
		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.	2018-10-26	₹	
		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. 2013-03-03	2018-10-26	₹	
		9	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices. 2013-03-03	2018-10-26	Ŧ	
		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.	2018-10-26	¥	
				1 - 10 of 10 items 25 - items per	page < 1) >	

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.

	ThreatProtector	_	© ((PII Protect
	Dashboard Notifications Training Co	Infiguration Employee Management Training Reports Policies	Documents SRA SRA Report Dark We	eb Phishing >
PROTECTOR BY Pelesystem			Filter by tag 6+	nload ESS Report
	Company Average Employee (j) Secure Score (ESS)	Company Average ESS Trend	Individual ESS Ranking	
Jason Dickheiser- Demo		800	Rank - Name Tags	Score
Edit profile		600	☆ Scott Chille	798
	441	400	2 Seth Gibbs	782
-√r My Dashboard 🔶	441		3 Scott Ward	744
圆 Newsfeed 🚺 介	01800	200	4 Chris Brown	713
	0,499 500,4529 650,930 Poor Eair Good	0 02.05 01.22 02.19 02.12 01.29	5 Jake Smallwood	698
III My Company 🟠	1001 101 0000	GLOU UTAL GATE GETA UTAF	6 Bill Somerville	643
			7 Jason Dickheiser	631
			8 Seth Litzenberger	608
			9 Shawn Nace	602
			9 Brad Weege	602
			11 George Jewett	599

4. Click on the "+New Policy" button.

	Th	reatPro	tector			🛞 Pii F	rotect
	Dash	board No	otifications	Training Configuration Employee Management Training Reports Policies Documents SRA SRA F	teport Dar	k Web Phis	shing >
PROTECTOR BY Gelesystem	Policie	s	(+ New Policy		10 selec	rted 🗇
		Policy 🛧	Name	Description	$\begin{array}{c} \text{Created} \\ \text{Date} \end{array} \uparrow$	Modified Date	Download
Jason Dickheiser- Demo		1	Written Information Security Policy	Written Information Security Policy (VISP) that defines the administrative, physical and technical safeguards to protect personally identifiable information (PII) and sensitive company information.	2013-03-01	2023-04-04	7
-⁄γ- My Dashboard 🔺		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.	2013-03-03	2018-10-26	₹
圆 Newsfeed 🛛 🖒	Ø	3	Security Incident Response	Procedures for reporting, responding to and managing security incidents.	2013-03-03	2018-10-26	
III My Company 分		4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.	2013-03-03	2018-10-26	₹
	Ø	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 enailyte company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.	2013-03-03	2018-10-26	Ŧ
		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.	2013-03-03	2018-10-26	₹
		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.	2013-03-03	2018-10-26	₹
		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.	2013-03-03	2018-10-26	
		9	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices.	2013-03-03	2018-10-26	₹
		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.	2013-03-03	2018-10-26	₹
				1 - 10 of 10 Items 25	 Items per p 	age <	1 >

5. Provide a Name, Description, and Details for the policy. The name and description will display to users when the 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".

Information Attachment Attachment Name* Password Management Policy Description* ABC Company's Password Management Policy for all users. Details* 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.	d Security Policies & Procedures	>
Information Attachment Name * Password Management Policy Description * ABC Company's Password Management Policy for all users. Details * 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.	0	Ø
Name* Password Management Policy Description* ABC Company's Password Management Policy for all users. Details* 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.	Information	Attachment
Password Management Policy Description* ABC Company's Password Management Policy for all users. Details* Details* 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.	Name *	
Description * ABC Company's Password Management Policy for all users. Details * 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.	Password Management Policy	
ABC Company's Password Management Policy for all users. Details * 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.	Description *	
Details * 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.	ABC Company's Password Management Policy for all users.	
Details * 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.		
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.	Details *	
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.	Purpose:	
aims to protect the integrity and confidentiality of sensitive information by preventing unauthorized access.	The purpose of this policy is to establish a standard for the creation, prot	ection, and usage of passwords within [Organization Name]. This policy
	aims to protect the integrity and confidentiality of sensitive information b	y preventing unauthorized access.
		Next
Next		

6. 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.

dd Security Policies & Procedures	
Ø	
Information	Attachment
Upload a file*	
Attachment PasswordPolicy.pdf	
* Only .doc, .docx, .pdf, .txt, .dotx, .csv, .xlsx, .xls files will be accepted	
	Back Save

7. 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.

÷—	Th	reatPro	tector	raining Configuration	Employee Management	Training Reports	Policies	Documents	SRA SRA R	eport Dar	() k Web	PII F	Protect
	Policie	3		+ New Policy									÷
	0	Policy 个	Name	Description						1	Created Date	Modified Date	Download
Jason Dickheiser- Demo		1	Written Information Security Policy	Written Information S personally identifiable	ecurity Policy (WISP) that d e information (PII) and sensi	efines the administrat tive company informa	ive, physical an ation.	d technical safe	guards to protect	:	2013-03-01	2023-04-04	÷
Edit profile		2	Termination Policy	Policy defines the ste resources when termi	ps required to revoke both p inating an employee.	hysical and system a	ccess to the org	anization's facil	ities and network		2013-03-03	2018-10-26	*
-사 My Dashboard 🔶 🏫		3	Security Incident Response	Procedures for report	ting, responding to and man	aging security inciden	its.			:	2013-03-03	2018-10-26	Ŧ
📓 My Company 🏠	0	4	Sanction Policy	Policy governs employ	yee sanctions and disciplina	ary actions for non-co	mpliance with t	he WISP.		:	2013-03-03	2018-10-26	4
	•	5	Network Security	Policy describes the p used to access, transi that access is restrict	physical safeguards applical mit, receive and store PII an ted to authorized employees	ble for each server, de d sensitive company	sktop compute data to ensure t	r system and wi hat appropriate	reless computer s security is mainta	ined and	2013-03-03	2018-10-26	4
		6	Access Controls	Policy to assure that a programs that have be	systems containing PII and/ een granted appropriate acc	or sensitive company cess rights.	data are acces	sed only by thos	e persons or soft	ware	2013-03-03	2018-10-26	*
		7	Computer Use	Policy to ensure that e and network to maxim	employees understand what nize the security of PII and s	t functions should and ensitive company dat	i should not be ta.	performed on Ti	he Company's cor	nputers	2013-03-03	2018-10-26	*
	0	8	Disposal Procedure	All media containing unauthorized access	PII and sensitive company d to the data.	ata, will be disposed	of in a manner t	hat destroys the	data and does n	ot allow	2013-03-03	2018-10-26	7
		9	BYOD Policy	Policy describes the a	appropriate safeguards to pr	otect PII and sensitiv	e company data	on employee p	ersonally owned o	devices.	2013-03-03	2018-10-26	*
		10	Facility Security Plan	Policy defines the pro which such systems a	cedures that will limit physi are housed	cal access to PII and	sensitive compa	iny data and the	facility or facilitie	rs in	2013-03-03	2018-10-26	Ŧ
	•	11	Password Management Policy	ABC Company's Pass	word Management Policy fo	or all users.				:	2024-02-29	2024-02-29	Ŧ
									1 - 11 of 11 Items	25 -	ltems per	page < (1 >

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.

ί <u>τ</u> μ	IREAT	Security Policy ×	M	0	PII Protect
	Gelesystem	Name Password Management Policy		Download	Acknowledge i
Jason Di Demo	ickheiser-	Description	lentifiable	Ŧ	
	·	Details	hen	Ł	
	ashboard 🜟	Password Management Policy		Ł	
News	sfeed 🕘 🏠	Purpose: The purpose of this policy is to establish a standard for the creation, protection, and usage of passwords within [Organization		¥	
	ompany M	Name; in its policy aims to protect the integrity and controlemainty or sensitive information by preventing unauthorized access. **Scope.** This nolicy annies to all employees contractors and any other individuals who have access to [Ornanization Name]'s information	to access, icted to	¥	
		systems and data.	ns that have	¥	
		Policy:	network to	.4.	
		 *Password Complexity Requirements.** -Passwords must be aten 12 characters long. -Passwords must contain characters from at least three of the following four categories: uppercase letters, lowercase letters, 	ithorized	*	
		numbers, and special characters (e.g., t, (e), #, s). - Passwords must not contain personal information, such as user names, birthdates, or easily guessable sequences (e.g., "123456" or "password").		*	
		2. **Password Changes and Lifetime.** - Passwords must be changed at least every 90 days. - Old passwords cannot be reused within a cycle of 5 password changes.	uch	*	
		Temporary passwords must be changed upon the first login. 3.**Secure Desavord Storage and Sharing** -Passwords must not be written down or stored in an unsecured manner. -Sharing of passwords between employees, even temporarily, in strictly prohibited. -If password sharing is necessary for operational reasons, it must be approved by the IT department, and a secure method must be used.	25 - Ib	ems per page	< 1 >
		 4. **Password Recovery and Resets:** - Password resets must be verified through at least two forms of identity confirmation (e.g., email plus phone call to a pre- registered number). - The IT department will manage password resets, and requests must be made through the official support channel. 			
		 Training and Avareness. Employees must receive training on password management and the importance of password security. Regular security avareness campaigns will be conducted to reinforce the importance of adhering to the password management policy. 			
		6. **Compliance and Enforcement** - Compliance with this policy is mandatory. Failure to comply may result in disciplinary action, up to and including termination of employment. - Any exceptions to this policy must be approved by the IT department in consultation with HR.			
		Acknowledgment: I acknowledge that I have read and understood the Password Management Policy of [Organization Name]. I agree to comply with the guidelines and requirements set forth in this policy.			
		Employee Name: Pri Protect Copyright © 2024			

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

Thre	eatProtecto	r	•	PII Protect
Dashbo	ard Training	Micro Training Dark Web Newsletters Policies		
Policies				
Policy 🛧	Name	Description	Download	Acknowledge (i)
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.	Ŧ	
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.	₹	
3	Security Incident Response	Procedures for reporting, responding to and managing security incidents.	₹	
4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.	Ŧ	
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.	Ŧ	
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 hav been granted appropriate access rights.	е Т	
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.	₹	
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.	₹	
9	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices.	₹	
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.	Ŧ	
11	Password Management Policy	ABC Company's Password Management Policy for all users.	Ŧ	
		1-11 of 11 litems 25 -	Items per page	< 1 →