Report Title: Policy Details

Run Date and Time: 2024-06-10 16:25:16 Pacific Daylight Time

Run by: System Administrator

Table name: sn_compliance_policy

Policy

Name:

Security Awareness Policy Training

Type:	Policy	State:	Published
Owning group:	App Engine Admins	Valid from:	2024-06-11 16:10:16
Owner:	Chuck Farley	Valid to:	3030-06-30 16:10:26
Compliance score (%):	0	Approval method:	Select approvers
Parent:	NIST CSF - Awareness and Training (PR.AT)	Approval rule:	
		Approvers:	Isabel Sorkin
Policy categories:		Reviewers:	Susan Orwell
		Contributors:	

Description:

The Security Awareness Training Policy at ViemmaRx outlines the requirements and guidelines for educating all employees, contractors, and third-party users about cybersecurity best practices. The policy mandates initial and annual refresher training, along with role-based training for specific positions. It covers essential topics such as phishing, password management, data protection, and compliance with relevant laws and regulations. The training is delivered through online modules, in-person workshops, and interactive simulations. The policy emphasizes the importance of reporting security incidents and maintaining vigilance to protect the company's information assets. Compliance is monitored, and non-compliance may result in disciplinary actions.

Policy text:

Cybersecurity Policy: Security Awareness Training

1. Purpose

The purpose of this policy is to establish a framework for security awareness training at [Company Name]. This policy aims to ensure that all employees, contractors, and third-party users understand their responsibilities in safeguarding the company's information assets and are equipped with the knowledge to recognize and respond to security threats.

2. Scope

This policy applies to all employees, contractors, and third-party users who have access to [Company Name]'s information systems, data, or networks.

3. Policy

3.1 Training Requirements

Mandatory Training: All new employees, contractors, and third-party users must complete security awareness training within 30 days of their start date.Annual Refresher Training: All employees, contractors, and third-party users must complete an annual security awareness refresher course.Role-Based Training: Additional specialized training will be provided to employees based on their role and access to sensitive information (e.g., IT staff, finance, HR).

3.2 Training Content

Security awareness training will cover, but is not limited to, the following topics:

Importance of cybersecurity and information protectionIdentification and reporting of security incidentsPhishing and social engineering attacksPassword management and authentication best practicesSafe use of email and the internetData protection and privacyPhysical securityRemote work securityCompliance with relevant laws, regulations, and company policies

3.3 Delivery Methods

Training will be delivered through a combination of:

Online modules and quizzesIn-person workshops and seminarsInteractive simulations and exercises (e.g., phishing simulations)Regular updates and newsletters on emerging threats and best practices

3.4 Tracking and Reporting

Training Records: Human Resources will maintain records of all security awareness training completed by employees, contractors, and third-party users.Compliance Monitoring: The Information Security Team will monitor compliance with training requirements and report non-compliance to management.Training Effectiveness: Periodic assessments and feedback surveys will be conducted to evaluate the effectiveness of the training program and make necessary improvements.

4. Responsibilities

4.1 Employees, Contractors, and Third-Party Users

Complete all required security awareness training in a timely manner.Apply the knowledge gained from training to protect [Company Name]'s information assets.Report any security incidents or suspicious activities to the Information Security Team immediately.

4.2 Managers

Ensure that their team members complete the required security awareness training.Support and reinforce security best practices within their teams.

4.3 Information Security Team

Develop and maintain the security awareness training program.Provide ongoing support and resources for security awareness.Monitor and report on training compliance and effectiveness.

4.4 Human Resources

Ensure that new hires complete the mandatory security awareness training.Maintain accurate records of training completion.

5. Policy Compliance

5.1 Compliance Measurement

The Information Security Team will verify compliance with this policy through various methods, including but not limited to, periodic audits, monitoring, and feedback mechanisms.

5.2 Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with company policies and procedures.

6. Review and Revision

This policy will be reviewed annually by the Information Security Team and updated as necessary to ensure its continued relevance and effectiveness.

Knowledge Base

Policy knowledge base:	Governance, Risk, and Compliance	Policy template:	Example Article Template
Published policy:	KB0010002		

Acknowledgement Setup

Frequency:	Quarterly	Allow users to decline policy:	false

First acknowledgement:	2024-06-11	Allow users to request exception:	false
Number of days to respond:	3		
Next acknowledgement:			
Audience:	Facility Setup		
Reference material URL:			

Exception Setup

Maximum exception duration (days):	

Activity

Additional comments:

2024-06-10 16:19:35 - System Administrator (Additional comments)
Hi Isabel,
I need this reviewed policy draft approved for publication.

2024-06-10 16:18:13 - System Administrator (Additional comments)
Hi Susan,
I need you to review this policy draft asap and respond in order to meet the deadline.

Settings

Functional domain:

Related List Title: GRC document version List
Table name: sn_irm_shared_cmn_document_version
Query Condition: Document table = sn_compliance_policy AND Record = 9631659847b202109f7a9889316d43f1
Sort Order: Updated in descending order

1 GRC document versions

Name	Approved on	Approvers	Attachment	Contributors	KB article	Owner	Reason for change	Record	Reviewers
Security Awareness Policy Training	2024-06-10 16:23:16	Isabel Sorkin			KB0010002	Chuck Farley		Policy: Security Awareness Policy Training	Susan Orwell

Related List Title: Approval List
Table name: sysapproval_approver
Query Condition: Source table = sn_compliance_policy AND Approving = 9631659847b202109f7a9889316d43f1
Sort Order: Order in ascending order

1 Approvals

State	Approver	Comments	Approval for	Created
Approved	Isabel Sorkin			2024-06-10 16:19:35

Related List Title: Policy approvals List
Table name: sn_compliance_policy_approvals
Query Condition: Policy = Security Awareness Policy Training
Sort Order: Name in ascending order

None

Related List Title: Control List
Table name: sn_compliance_control
Query Condition: Control objective in () AND Exempt = true
Sort Order: Number in ascending order

None

Related List Title: Evidence List
Table name: sn_grc_advanced_evidence_response
Query Condition: Sys ID in
Sort Order: Number in ascending order

None