Report Title: Policy Details

Run Date and Time: 2024-05-22 20:31:07 Pacific Daylight Time

Run by: System Administrator

Table name: sn_compliance_policy

Policy

Name:

Incident Management Policy

Type:	Policy	State:	Published
Owning group:	App Engine Studio Users	Valid from:	2024-05-22 20:17:54
Owner:	Susan Orwell	Valid to:	2025-05-22 20:17:58
Compliance score (%):	0	Approval method:	Select approvers
Parent:	Information Security Policy	Approval rule:	
Policy categories:		Approvers:	Susan Orwell
		Reviewers:	System Administrator
		Contributors:	

Description:

Provides a framework for detecting, reporting, and responding to information security incidents.
Importance: Ensures timely and effective response to security incidents, minimizing impact.
Relevant Frameworks: ISO/IEC 27035, NIST SP 800-61, and GDPR

Policy text:

A. PurposeA structured and consistent approach to managing information security incidents within Emyzer Technology. This policy aims to minimize the impact of incidents on operations, protect sensitive information, and ensure compliance with ISO/IEC 27035, NIST SP 800-61, and GDPR frameworks.B. ScopeThis policy applies to all departments and activities within Emyzer Technology, including but not limited to IT, Human Resources, Legal, and any third-party vendors or contractors that handle Emyzer Technology's information assets.C. Definitions1. Incident: An unexpected event that compromises confidentiality, integrity, or availability of information.2. Incident Response Team (IRT): A group responsible for managing and responding to incidents.3. Personal Data: Any information about an identifiable natural person.4. GDPR: General Data Protection Regulation, a regulatory framework that sets guidelines for the collection and processing of personal data of individuals within the European Union.D. Policy StatementEmyzer Technology promptly identifies, reports, and responds to information security incidents. All incidents must be managed under ISO/IEC 27035, NIST SP 800-61, and GDPR requirements to protect the organization's information assets and ensure regulatory compliance.E. Roles and Responsibilities1. Information Security Officer (ISO): Oversees the incident management process and ensures compliance with relevant standards and regulations.2. Incident Response Team (IRT): Manages the detection, analysis, containment, eradication, and recovery of incidents.3. Department Heads: Ensure teams comply with the incident management policy.4. All Employees: Report any suspected or actual information security incidents immediately to the ISO or the IRT.F. ProceduresF.1. Incident Identification and Reporting:F.1.1. All employees must report suspected incidents to the IRT immediately.F.1.2. The IRT logs the incident in the incident management system.F.2. Incident Analysis:F.2.1 The IRT conducts a preliminary analysis to determine the scope and impact of the incident.F.2.2. The GDPR breach notification procedures are initiated if personal data is involved.F.3. Containment:F.3.1. The IRT implements measures to contain the incident and prevent further damage.F.4. Eradication:F.4.1. The IRT identifies and removes the cause of the incident.F.5. Recovery:F.5.1. The IRT restores affected systems and services to normal operation.F.6. Post-Incident Review:F.6.1. A post-incident review is conducted to identify lessons learned and improve future incident response efforts.G. Compliance and Monitoring1. The Information Security Officer will monitor compliance with this policy through regular audits and incident reviews.2. Non-compliance with this policy may result in disciplinary action including termination of employment or contract.H. Related Documents1. Information Security Policy2. Data Protection Policy3. Business Continuity Plan4. IT Incident Response PlanI. Review and RevisionThis policy will be reviewed and revised annually or as needed to ensure its effectiveness and compliance with relevant standards and regulations. The next review date is set for [insert review date one year from the current date].

Knowledge Base

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

Published policy:	KB0010006

Acknowledgement Setup

Frequency:		Allow users to decline policy:	false
First acknowledgement:		Allow users to request exception:	false
Number of days to respond:			
Next acknowledgement:			
Audience:			
Reference material URL:			

Exception Setup

Maximum exception duration (days):	7

Activity

Additional comments:

2024-05-22 20:21:15 - System Administrator (Additional comments)
Hello Susan. Please approve this Incident Management Policy.

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 = a70560de839602101a5f9c50ceaad34a
Sort Order: Updated in descending order

1 GRC document versions

Name	Approved on	Approvers	Attachment	Contributors	KB article	Owner	Reason for change	Record	Reviewers
Incident Management Policy	2024-05-22 20:29:59	Susan Orwell			KB0010006	Susan Orwell		Policy: Incident Management Policy	System Administrator

Related List Title: Approval List
Table name: sysapproval_approver
Query Condition: Source table = sn_compliance_policy AND Approving = a70560de839602101a5f9c50ceaad34a
Sort Order: Order in ascending order

1 Approvals

State	Approver	Comments	Approval for	Created
Approved	Susan Orwell	2024-05-22 20:29:58 - Susan Orwell (Comments) Great work. Approved.		2024-05-22 20:21:15

Related List Title: Policy approvals List
Table name: sn_compliance_policy_approvals
Query Condition: Policy = Incident Management Policy
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