Report Title: Policy Details

Run Date and Time: 2024-05-22 13:46:33 Pacific Daylight Time

Run by: System Administrator

Table name: sn_compliance_policy

Policy

Name:

Information Security Policy

Type:	Policy	State:	Published
Owning group:	App Engine Admins	Valid from:	2024-05-22 13:32:23
Owner:	Susan Orwell	Valid to:	2025-05-22 13:32:26
Compliance score (%):	0	Approval method:	Select approvers
Parent:		Approval rule:	
Policy categories:		Approvers:	Susan Orwell
		Reviewers:	System Administrator
		Contributors:	

Description:

This policy aims to protect the confidentiality, integrity, and availability of information.
The impact ensures data security for cloud services, customer data protection, and cybersecurity resilience.
Relevant Standards: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27032

Policy text:

A. PurposeTo establish a framework for managing and protecting the confidentiality, integrity, and availability of information assets within Emyzer Technology. Thispolicy aims to safeguard data against unauthorized access, disclosure, alteration, and destruction, ensuring the security of cloud services and customer data,and enhancing cybersecurity resilience.B. ScopeThis policy applies to all employees, contractors, consultants, temporary staff, and other workers at Emyzer Technology, including all personnel affiliated withthird parties. It encompasses all information assets, systems, networks, applications, and data owned or managed by Emyzer Technology.C. Definitions1.) Confidentiality: Ensuring that information is accessible only to authorized users.2.) Integrity: Safeguarding the accuracy and completeness of information and processing methods.3.) Availability: Ensuring authorized users can access information and associated assets when required.4.) Information Assets: Data, systems, networks, applications, and other resources that manage information.D. Policy StatementEmyzer Technology is committed to protecting its information assets from all threats, whether internal or external, deliberate or accidental. To achieve this,the organization will:1.) Implement an Information Security Management System (ISMS) following ISO/IEC 27001 standards.2.) Use ISO/IEC 27017 and ISO/IEC 27018 guidelines for cloud service security and personal data protection.3.) Adopt ISO/IEC 27032 standards to enhance cybersecurity measures.4.) Regularly assess and manage risks to information security.5.) Ensure all employees comply with this policy and related procedures.6.) Respond promptly to security incidents and breaches to minimize impact.7.) Continuously improve the ISMS through regular reviews and audits.E. Roles and Responsibilities1.) Information Security Officer (ISO): Responsible for developing, implementing, and maintaining the ISMS. Ensures compliance with relevant standards andregulations.2.) Department Heads: Ensure their teams comply with the information security policy and related procedures. Identify and report security risks.3.) IT Department: Implements technical controls and monitors information systems to protect against security threats.4.) All Employees: Comply with the information security policy, attend training sessions, and report any security incidents or vulnerabilities.F. Procedures1.) Risk Assessment: Conduct regular risk assessments to identify and evaluate security risks. Implement appropriate controls to mitigate identified risks.2.) Access Control: Implement access controls to ensure only authorized personnel can access information assets. Regularly review and update accessrights.3.) Data Protection: Use encryption and other security measures to protect sensitive data. Ensure compliance with data protection regulations.4.) Incident Management: Establish and maintain procedures for detecting, reporting, and responding to security incidents. Conduct root cause analysis andtake corrective actions.5.) Training and Awareness: Provide ongoing information security training and awareness programs for all employees.6.) Audits and Reviews: Conduct regular audits and reviews of the ISMS to ensure compliance with the policy and continuous improvement.G. Compliance and MonitoringCompliance with this policy will be monitored through regular internal audits, security reviews, and risk assessments. Non-compliance will be addressedthrough corrective actions, and significant breaches may result in disciplinary actions.H. Related Documents1.) Risk Management Policy2.) Data Protection and Privacy Policy3.) Incident Response Plan4.) Access Control Policy5.) IT Security Procedures ManualI. Review and RevisionThis policy will be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness. Revisions will be made toaddress emerging threats, regulatory changes, and improvements in best practices.

Knowledge Base

Policy knowledge base:	Governance, Risk, and Compliance	Policy template:	Example Article Template
Published policy:	KB0010003		

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 13:43:04 - System Administrator (Additional comments)
Hello Susan. Please kindly approve this Information Security 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 = 1d7387c2831202101a5f9c50ceaad329
Sort Order: Updated in descending order

1 GRC document versions

Name	Approved on	Approvers	Attachment	Contributors	KB article	Owner	Reason for change	Record	Reviewers
Information Security Policy	2024-05-22 13:44:56	Susan Orwell			KB0010003	Susan Orwell		Policy: Information Security Policy	System Administrator

Related List Title: Approval List
Table name: sysapproval_approver
Query Condition: Source table = sn_compliance_policy AND Approving = 1d7387c2831202101a5f9c50ceaad329
Sort Order: Order in ascending order

1 Approvals

State	Approver	Comments	Approval for	Created
Approved	Susan Orwell	2024-05-22 13:44:55 - Susan Orwell (Comments) Looks great. Approved.		2024-05-22 13:43:04

Related List Title: Policy approvals List
Table name: sn_compliance_policy_approvals
Query Condition: Policy = Information Security 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