Report Title:	Policy Details
Run Date and Time:	2024-05-22 18:28:07 Pacific Daylight Time
Run by:	System Administrator
Table name:	sn_compliance_policy

Policy

Name:

Risk Management Policy

Type:	Policy	State:	Published
Owning group:	App Engine Admins	Valid from:	2024-05-22 18:18:00
Owner:	Susan Orwell	Valid to:	2025-05-22 18:18:06
Compliance score (%):	0	Approval method:	Select approvers
Parent:	Information Security Policy	Approval rule:	
Policy categories:		Approvers:	Susan Orwell
		Reviewers:	System Administrator
		Contributors:	

Description:

This policy defines the approach for identifying, assessing, and managing information security risks.
Importance: Critical for proactive identification and mitigation of security risks.
Relevant Frameworks: NIST SP 800-37, COSO ERM, and CIS RAM

Policy text:

A. Purpose:The purpose of this policy is to establish a comprehensive risk management framework for Emyzer Technology that integrates the principles of NIST SP 800-37 (Risk Management Framework - RMF), COSO ERM (Enterprise Risk Management – Integrated Framework), and CIS RAM (Center for Internet Security Risk Assessment Method). This policy aims to identify, assess, manage, and mitigate risks that could impact the organization’s ability to achieve its objectives.B. Scope:This policy applies to all departments and activities within Emyzer Technology, including but not limited to Information Technology, Human Resources, Finance, Operations, and Legal. It encompasses all types of risks, including strategic, operational, financial, compliance, and information security.C. Definitions:1. Risk: The potential for loss or harm to an organization’s assets, operations, or reputation.2. Risk Management Framework (RMF): A structured process to identify and manage risks.3. COSO ERM: A framework for identifying, assessing, and managing risks across an enterprise.4. CIS RAM: A methodology for assessing and managing information security risks.5. Risk Assessment: Identifying, analyzing, and evaluating risks.6. Mitigation: Actions taken to reduce the likelihood or impact of a risk.D. Policy Statement:Emyzer Technology is committed to managing risks proactively and systematically to protect its assets, ensure the continuity of operations, and maintain compliance with applicable laws and standards. The organization will implement a risk management framework incorporating NIST SP 800-37, COSO ERM, and CIS RAM to guide risk identification, assessment, mitigation, monitoring, and reporting.E. Roles and Responsibilities:1. Risk Management Committee: Oversees the risk management program, approves policies and procedures, and reviews risk assessments and mitigation plans.2. Chief Risk Officer (CRO): Leads the risk management efforts, ensures the integration of risk management into business processes, and reports to senior management and the board on risk-related issues.3. Department Heads: Identify and manage risks within their areas of responsibility, ensuring that risk management activities are aligned with the overall risk management framework.4. Risk Owners: Individuals assigned to manage specific risks, and responsible for implementing and monitoring mitigation plans.5. All Employees: Understand and comply with the risk management policy, report identified risks, and participate in risk management activities as required.F. Procedures:1. Risk Identification: Identify risks using a combination of risk assessments, audits, incident reports, and employee feedback.2. Risk Assessment: Assess identified risks using qualitative and quantitative methods, considering the likelihood and impact of each risk.3. Risk Mitigation: Develop and implement risk mitigation plans to reduce the likelihood or impact of risks to acceptable levels.4. Risk Monitoring: Continuously monitor risks and the effectiveness of mitigation measures, adjusting plans as necessary.5. Risk Reporting: Regularly report on the status of risks and mitigation efforts to senior management and the Risk Management Committee.G. Compliance and Monitoring:Compliance with this policy will be monitored through regular audits, reviews of risk management activities, and performance metrics. Non-compliance will be addressed through corrective actions and, if necessary, disciplinary measures.H. Related Documents:1. Information Security Policy2. Business Continuity Plan3. Incident Response Plan4. IT Risk Management ProceduresI. Review and Revision:This policy will be reviewed annually and revised to ensure its continued relevance and effectiveness in managing risks. The Risk Management Committee will approve any changes.

Knowledge Base

Policy knowledge base:	Governance, Risk, and Compliance	Policy template:	Example Article Template
Published policy:	KB0010004		

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 18:25:56 - System Administrator (Additional comments)
Hello Susan. Please approve this Risk 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 = bc99085e835602101a5f9c50ceaad37f
Sort Order:	Updated in descending order

1 GRC document versions

Name	Approved on	Approvers	Attachment	Contributors	KB article	Owner	Reason for change	Record	Reviewers
Risk Management Policy	2024-05-22 18:27:01	Susan Orwell			KB0010004	Susan Orwell		Policy: Risk Management Policy	System Administrator

Related List Title:	Approval List
Table name:	sysapproval_approver
Query Condition:	Source table = sn_compliance_policy AND Approving = bc99085e835602101a5f9c50ceaad37f
Sort Order:	Order in ascending order

1 Approvals

State	Approver	Comments	Approval for	Created
Approved	Susan Orwell	2024-05-22 18:27:01 - Susan Orwell (Comments) This looks great. Approved.		2024-05-22 18:25:56

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