Report Title: Policy Details

Run Date and Time: 2024-05-22 19:10:49 Pacific Daylight Time

Run by: System Administrator

Table name: sn_compliance_policy

Policy

Name:

Access Control Policy

Type:	Policy	State:	Published
Owning group:	App Engine Studio Users	Valid from:	2024-05-22 19:00:38
Owner:	Susan Orwell	Valid to:	2025-05-22 19:00:43
Compliance score (%):	0	Approval method:	Select approvers
Parent:	Information Security Policy	Approval rule:	
Policy categories:		Approvers:	Susan Orwell
		Reviewers:	System Administrator
		Contributors:	

Description:

Access to information and information systems based on business and security requirements.
Impact: Ensures that only authorized personnel have access to sensitive information, reducing the risk of unauthorized access.
Relevant Frameworks: COBIT, RBAC, and ABAC

Policy text:

A. PurposeTo establish guidelines and requirements for managing access to information systems and data within Emyzer Technology, ensuring confidentiality, integrity, and availability of information through effective access control measures.B. ScopeThis policy applies to all Emyzer Technology employees, contractors, vendors, and authorized users of Emyzer Technology's information systems and data. This includes all departments and activities related to access control management.C. Definitions1. COBIT (Control Objectives for Information and Related Technologies): A framework for developing, implementing, monitoring, and improving IT governance and management practices.2. RBAC (Role-Based Access Control): A method of regulating access to computer or network resources based on the roles of individual users within an enterprise.3. ABAC (Attribute-Based Access Control): An access control method granting rights through combined attribute policies.D. Policy Statement1. Access Authorization: Access to Emyzer Technology's information systems and data shall be granted based on the principles of least privilege and need-to-know.2. Role-Based Access Control (RBAC): Access rights shall be assigned based on predefined roles corresponding to job functions within the organization.3. Attribute-Based Access Control (ABAC): Access decisions shall incorporate user and resource attributes; and environmental attributes to ensure dynamic and context-aware access control.4. User Authentication: All users must authenticate using secure methods (e.g., multi-factor authentication) before accessing systems or data.5. Access Review: Regular access reviews shall be conducted to ensure appropriate access levels and remove or modify access as necessary.6. Access Logs: All access to information systems and data shall be logged and monitored for security and compliance.E. Roles and Responsibilities1. IT Security Team: Responsible for implementing and managing access control measures, conducting access reviews, and monitoring access logs.2. Department Managers: Responsible for identifying role requirements and approving access requests based on job functions and needs.3. Employees and Users: Responsible for adhering to access control policies, safeguarding their authentication credentials, and reporting suspicious access activities.F. ProceduresF.1 Access Request and Approval:F.1.1. Submit an access request form to the IT Security Team.F.1.2. Department Managers review and approve requests based on role requirements.F.1.3. IT Security Team configures access according to approved requests.F.2 Access Review and Audit:F.2.1 Conduct quarterly access reviews to ensure access levels are appropriate.F.2.2 Perform annual audits to verify compliance with access control policies.F.3 Access Revocation:F.3.1 Revoke access immediately upon termination or role change of an employee.F.3.2. Conduct periodic checks to ensure timely revocation of unnecessary access.G. Compliance and Monitoring1. Monitoring: Continuous monitoring of access logs and activities to detect unauthorized access and anomalies.2. Audits: Regularly conducted by the IT Security Team to ensure compliance with this policy.3. Enforcement: Violations of this policy may result in disciplinary action and termination of employment or contract.H. Related Documents1. Information Security Policy2. IT Governance Framework (COBIT)3. Incident Response Plan4. Data Protection PolicyI. Review and RevisionThis policy shall be reviewed annually and revised to address new risks, technologies, and compliance requirements. The IT Security Team is responsible for an up-to-date and effective policy.

Knowledge Base

Policy knowledge base:	Governance, Risk, and Compliance	Policy template:	Example Article Template
Published policy:	KB0010005		

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 19:07:37 - System Administrator (Additional comments)
Hello Susan. Please approve this Access Control 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 = 7043d4da839602101a5f9c50ceaad31f
Sort Order: Updated in descending order

1 GRC document versions

Name	Approved on	Approvers	Attachment	Contributors	KB article	Owner	Reason for change	Record	Reviewers
Access Control Policy	2024-05-22 19:10:00	Susan Orwell			KB0010005	Susan Orwell		Policy: Access Control Policy	System Administrator

Related List Title: Approval List
Table name: sysapproval_approver
Query Condition: Source table = sn_compliance_policy AND Approving = 7043d4da839602101a5f9c50ceaad31f
Sort Order: Order in ascending order

1 Approvals

State	Approver	Comments	Approval for	Created
Approved	Susan Orwell	2024-05-22 19:09:59 - Susan Orwell (Comments) The policy looks fantastic. I like how we're finally incorporating both RBAC & ABAC. Approved.		2024-05-22 19:07:37

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