CLOUD SECURITY POLICY

INLINE WITH ISO 27001:2022 & SOC 2 TYPE 2

PREPARED BY

Document Name	**Cloud Security Policy**
Classification	**Internal Use Only**

Document Management Information

Document Title:	Cloud Security Policy
Document Number:	ORGANISATION-CLD-SEC-POL
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	Name	Designation
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

Document Name	Cloud Security Policy
Classification	Internal Use Only

CONTENTS

Document Name	Cloud Security Policy
Classification	Internal Use Only

1. PURPOSE

The purpose of this Cloud Security Policy is to define a unified and structured framework for the secure adoption, configuration, operation, and governance of cloud services across **[ORG NAME]**. This policy ensures that all cloud-based resources, data, workloads, and services are protected in accordance with their sensitivity, business criticality, and compliance obligations.

The objectives of this policy are to:

- **Ensure secure design, deployment, and management** of cloud environments across IaaS, PaaS, SaaS, and hybrid models.
- **Preserve the confidentiality, integrity, and availability (CIA)** of information stored, processed, or transmitted through cloud platforms.
- **Prevent unauthorized access, data exposure, misconfigurations, and service misuse** within cloud ecosystems.
- **Align cloud operations with ISO/IEC 27001:2022, SOC 2 Type II, CSA Cloud Controls Matrix (CCM), and applicable legal/regulatory requirements** such as GDPR, DPDP Act, and data residency obligations.
- **Clarify security responsibilities under the Shared Responsibility Model**, ensuring accountability between the organization, cloud service providers (CSPs), and internal stakeholders.
- **Implement standardized controls for identity management, network security, data protection, logging, monitoring, and incident response** within cloud platforms.
- **Ensure that cloud vendors, integrations, and third-party providers follow approved security practices**, contractual commitments, and compliance requirements.
- **Define lifecycle expectations** for cloud resources, including onboarding, configuration, monitoring, and secure exit/termination processes.
- **Reduce operational, security, and compliance risks associated with cloud adoption**, including misconfigurations, insecure APIs, shadow IT, and vendor lock-in.

This policy forms a core component of **[ORG NAME]'s Information Security Management System (ISMS)** and applies to all cloud initiatives undertaken by the organization.

2. SCOPE

This Cloud Security Policy applies to all cloud environments, services, users, data, and technology resources that are created, accessed, stored, processed, transmitted, or managed by **[ORG NAME]** using any cloud platform. The policy is applicable across all business units, applications, teams, and third parties who interact with cloud-based assets or services.

2.1 Covered Users

This policy applies to:

- All **employees**, including full-time, part-time, temporary, and probationary staff
- All **contractors, consultants, and interns**
- All **third-party service providers, vendors, and managed service partners** with access to cloud-hosted resources
- All **customers or external stakeholders** (where applicable) who access [ORG NAME] cloud-hosted applications
- Any individual or entity authorized to use, configure, or manage cloud systems, data, or infrastructure on behalf of [ORG NAME]

2.2 Covered Cloud Environments

This policy applies to all cloud service models used by the organization, including:

Cloud Service Models

- **IaaS** (Infrastructure as a Service) – VMs, networks, storage, security groups
- **PaaS** (Platform as a Service) – managed databases, containers, serverless, application platforms
- **SaaS** (Software as a Service) – business applications, CRM, HRMS, collaboration tools

Cloud Deployment Models

- **Public cloud**
- **Private cloud**

- **Hybrid cloud**
- **Multi-cloud deployments**

This includes, but is not limited to, platforms such as AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud, and any approved SaaS providers.

2.3 Covered Assets

This policy covers any cloud-hosted or cloud-integrated asset, including:

- Virtual machines, compute instances, containers, Kubernetes clusters
- Applications, APIs, web services, microservices
- Databases, storage accounts, buckets, blobs, object stores
- Networking components (VPC/VNet, firewalls, routing, gateways)
- Identity components (IAM, directory services, SSO, service accounts)
- Logs, telemetry, audit trails
- Encryption keys, secrets, tokens, certificates
- Backup and replication systems
- Monitoring and alerting systems
- Cloud-native security tools (CSPM, CWPP, SIEM, WAF, DDoS protection)

2.4 Covered Data Types

This policy applies to all data stored, processed, or transmitted via cloud services, including:

- Personal and sensitive personal data
- Customer data
- Financial, transactional, and business records
- Intellectual property, proprietary information, and source code

- Machine logs, telemetry, and analytics
- Confidential internal communications
- Any data classified as **Restricted, Confidential, Internal Use Only, or Public** per the Data Classification Policy

2.5 Covered Activities

The policy governs all activities related to cloud use, including:

- Cloud onboarding, provisioning, and configuration
- Identity and access management
- Deployment, development, and DevSecOps processes
- Data storage, encryption, transmission, and backup
- Monitoring, logging, and incident detection
- Integration with third-party or on-premise systems
- Vendor management and cloud contract reviews
- Cloud exit, migration, or service termination
- Continuous compliance monitoring and audits

2.6 Exclusions

This policy does **not** apply to:

- Personal cloud accounts or personal devices used outside approved BYOD programs
- Unapproved cloud services used without formal authorization (classified as Shadow IT and subject to remediation and disciplinary action)
- Non-cloud on-premises systems (covered under other information security policies)

3. TERMS AND DEFINITIONS

Term	Definition
Cloud Service Provider (CSP)	A third-party organization that offers cloud-based infrastructure, platform, or software services (e.g., AWS, Azure, GCP, Oracle Cloud).
Cloud Service Model	The type of cloud service provided, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
Shared Responsibility Model	A security model that defines the split of security and compliance responsibilities between [ORG NAME] and the cloud provider. The CSP manages security *of* the cloud, while [ORG NAME] manages security *in* the cloud.
Cloud Resource	Any compute, storage, networking, application, or platform component provisioned within a cloud environment.
IAM (Identity and Access Management)	Cloud-based identity system used to control authentication and authorization for users, roles, systems, and applications.
Service Account	A non-human identity (NHI) used by applications, services, or automated processes to access cloud resources.
Workload	Any application, service, container, VM, or serverless function running within a cloud environment.
VPC / VNet	Virtual Private Cloud (AWS) or Virtual Network (Azure/GCP) used for logically isolating cloud resources.
Security Group / Network Security Group (NSG)	Firewall rules applied to cloud resources to control inbound and outbound traffic.
Encryption at Rest	The protection of stored data using encryption mechanisms such as KMS/HSM-managed keys.

Encryption in Transit	Encryption applied to data transmitted over networks using TLS/HTTPS or secure communication protocols.
KMS / Key Management Service	Cloud-native service for managing cryptographic keys, rotation policies, storage, and access controls.
HSM (Hardware Security Module)	A hardware-based cryptographic module used for highly secure key management.
Data Residency	Legal or contractual requirement dictating the geographic location where data must be stored or processed.
CSPM (Cloud Security Posture Management)	Tools and processes that continuously evaluate cloud configurations to identify misconfigurations and risks.
CWPP (Cloud Workload Protection Platform)	Security controls that protect cloud workloads such as VMs, containers, and serverless functions.
SIEM (Security Information & Event Management)	System that collects, aggregates, and analyzes logs for security event detection and incident response.
API Gateway	Managed cloud service used to securely expose, monitor, and throttle APIs.
Shadow IT	Use of unapproved cloud services or tools without authorization from IT or the Information Security Team.
Infrastructure as Code (IaC)	Managing and provisioning cloud resources using code (e.g., Terraform, CloudFormation, ARM templates).
Cloud Drift	Unauthorized or accidental configuration deviations in cloud environments from approved baselines.
Data Leakage / Data Exfiltration	Any unauthorized transmission or exposure of sensitive data outside approved systems.

Multi-Tenancy	A cloud architecture where multiple customers share the same underlying infrastructure, logically separated by the CSP.
Cloud Exit / Cloud Service Termination	A controlled process to migrate, delete, export, or decommission cloud services securely without data loss or exposure.
SaaS Application	A software service accessed over the internet, where the CSP manages infrastructure, platform, and the application.
Zero Trust	A security model requiring strict identity verification, least privilege access, and continuous validation regardless of network location.

4. ROLES AND RESPONSIBILITIES

To ensure consistent, secure, and compliant use of cloud services, [ORG NAME] defines clear responsibilities for all stakeholders involved in the planning, deployment, management, and oversight of cloud environments.

Roles outlined below support the Shared Responsibility Model and ensure accountability across the cloud lifecycle.

Role	Responsibilities
Board of Directors / Executive Management	· Approve cloud adoption strategy and ensure alignment with business objectives. · Provide oversight and resources for cloud security initiatives. · Ensure compliance with legal, regulatory, and contractual cloud obligations.

Chief Information Security Officer (CISO)	• Own the Cloud Security Policy and ensure alignment with ISMS and SOC 2 controls. • Define cloud security standards, baselines, and architectural guidelines. • Review and approve cloud service onboarding, risk assessments, and exceptions. • Monitor cloud security posture and oversee incident response for cloud environments.
Cloud Security Architect / Cloud Security Lead	• Design secure cloud architectures and enforce Zero Trust principles. • Define and maintain cloud configuration baselines (CIS, NIST, CSA CCM). • Review IaC templates, security groups, routing rules, and workload protection settings. • Evaluate cloud services for security risks before adoption. • Ensure proper implementation of encryption, IAM, logging, and monitoring controls.
Information Security Team	• Perform cloud risk assessments, configuration audits, and continuous monitoring. • Review alerts, anomalies, and CSPM/CWPP findings. • Validate IAM roles, access rights, and privileged access activities. • Support cloud incident response, investigations, and forensic analysis.
IT Operations / Cloud Engineering / DevOps (SRE)	• Provision, configure, and maintain cloud services according to approved security standards. • Implement secure IaC pipelines, CI/CD controls, and automated enforcement checks.

	• Ensure backups, resilience features, and DR strategies are operational. • Apply patches, updates, and security fixes to cloud workloads. • Implement cloud logging, SIEM integration, and operational monitoring.
Application Owners / Product Teams	• Ensure applications deployed in cloud environments comply with security controls. • Collaborate with cloud security and DevOps teams to enforce secure coding and deployment practices. • Review access privileges and approve data flows, integrations, and API usage. • Own application-specific encryption, API keys, tokens, and secrets.
Data Owners / Data Stewards	• Classify cloud-hosted data according to the Data Classification Policy. • Approve data storage locations, residency requirements, and retention rules. • Authorize data-sharing requests and oversee secure disposal of cloud-stored data.
Vendor Management / Procurement Team	• Conduct due diligence for cloud providers and SaaS vendors. • Ensure cloud contracts contain security, privacy, and compliance clauses. • Validate certifications (ISO 27001, SOC 2, CSA STAR), SLAs, breach notification terms, and exit arrangements.
Legal & Compliance Team	• Review cloud contracts, DPAs, and cross-border data transfer obligations.

	• Advise on regulatory compliance (GDPR, DPDP Act, financial sector regulations). • Evaluate data residency, sovereignty, and retention requirements.
HR & People Operations	• Ensure appropriate onboarding and offboarding workflows for cloud access. • Coordinate identity provisioning and revocation with IT and Security teams. • Support cloud-related awareness and training programs.
Employees / End Users	• Use cloud services only as authorized and approved. • Follow all security controls related to storage, access, data sharing, and authentication in cloud platforms. • Report suspicious activity, misconfigurations, or unauthorized cloud use immediately. • Refrain from using unapproved cloud tools or engaging in Shadow IT.
Third Parties / Managed Service Providers (MSPs)	• Adhere to [ORG NAME]'s cloud security requirements and contractual obligations. • Implement appropriate controls to secure cloud operations handled on behalf of [ORG NAME]. • Cooperate during audits, assessments, and incident investigations.

5. CLOUD ARCHITECTURE & DESIGN PRINCIPLES

The following principles define mandatory requirements for designing, deploying, and managing all cloud environments within **[ORG NAME]**.

5.1 Secure-by-Design Architecture

- All cloud architectures **shall be designed using Secure-by-Design principles**, ensuring security controls are embedded from the initial planning phase.
- All cloud workloads and components **shall be deployed using approved architecture patterns and Infrastructure-as-Code (IaC) templates**.
- Default cloud configurations **shall not be used unless validated and approved** by the Information Security Team.
- Any deviation from approved cloud architecture standards **shall undergo a documented risk assessment and receive prior authorization** from the Information Security Team.
- Cloud deployments **shall not proceed without validated security baselines**, including identity, network, data, and monitoring controls.

5.2 Shared Responsibility Model Compliance

- [ORG NAME] **shall maintain documented responsibility boundaries** for each cloud service in accordance with the cloud provider's Shared Responsibility Model.
- The organization **shall ensure its responsibilities (security *in* the cloud)**—including IAM, network controls, workload security, encryption, logging, and monitoring—are consistently implemented.
- All teams using cloud services **shall acknowledge and adhere to provider-specific shared responsibility requirements** before deployment.
- No cloud service may be onboarded unless responsibility assignments **are formally reviewed and approved** by the Cloud Security Architect or the Information Security Team.

5.3 Zero Trust Cloud Principles

- All cloud environments **shall adopt Zero Trust principles**, treating every access request as untrusted until verified.

- Access to cloud resources **shall be granted strictly on least-privilege and need-to-know basis**.

- Network trust relationships shall not be implicitly granted; all access **shall require strong authentication and authorization controls**.

- Segmentation **shall be enforced between environments, workloads, and network tiers** to limit lateral movement.

- Continuous monitoring and validation **shall be enforced for all cloud identities, sessions, and resource interactions**.

5.4 Cloud Environment Isolation & Segmentation

- Production, staging, UAT, and development cloud environments **shall be logically and physically isolated** using virtual networks, subnets, and access controls.

- Application tiers (web, application, and database) **shall be deployed in separate network zones** to enhance security and containment.

- Sensitive workloads **shall be restricted to private networks** and must not be exposed to the public internet unless explicitly approved.

- Cross-environment communication **shall require formal approval and documented justification**, including monitoring and logging.

- Segmentation configurations **shall be reviewed periodically** to verify compliance with internal policies and regulatory requirements.

5.5 Cloud Service & Provider Onboarding Requirements

- All cloud services and SaaS applications **shall undergo a formal security and compliance evaluation** before use.

- Cloud providers **shall possess recognized security certifications** (e.g., ISO 27001, SOC 2, CSA STAR) appropriate to the service being adopted.

- Data residency, sovereignty, encryption capability, and logging features **shall be validated and approved** as part of onboarding.

- No cloud service shall be activated unless the Information Security Team **has approved documentation of security risks, mitigations, and responsibilities**.

- Unapproved or unsanctioned cloud services **shall not be used** under any circumstances.

5.6 Standardized Cloud Configuration Baselines

- All cloud resources **shall comply with hardened configuration baselines** defined by [ORG NAME], referencing CIS, NIST, and CSA standards.
- Configuration baselines **shall define minimum controls** for IAM, networking, workload security, logging, encryption, and monitoring.
- Any workload or resource not aligned with baseline requirements **shall require a formally approved exception**.
- Configuration baselines **shall be reviewed periodically** to ensure relevance and alignment with emerging cloud threats.
- Automated tools (e.g., CSPM) **shall be used to enforce and continuously validate baseline compliance**.

5.7 Approved Architectural Patterns & Infrastructure-as-Code

- All cloud deployments **shall use organization-approved IaC templates**, ensuring consistency and reducing configuration errors.
- Manual provisioning of cloud resources **shall be prohibited**, unless approved as an exception by the Information Security Team.
- All IaC templates **shall be stored in version-controlled repositories**, with changes subject to peer review and approval.
- Infrastructure drift and configuration drift **shall be monitored continuously** and remediated promptly.
- IaC pipelines **shall enforce automated checks** for security, compliance, and configuration accuracy.

5.8 High Availability & Resilience

- Business-critical workloads **shall be designed using multi-zone or multi-region architectures** to ensure resilience.
- All workloads **shall have defined RPO and RTO requirements**, approved by the business owner.
- Backup, snapshot, and replication configurations **shall be implemented and periodically tested** to ensure recoverability.

- Failover and recovery procedures **shall be documented and validated through regular DR exercises**.

- Cloud resources **shall be deployed with fault-tolerant configurations** and automated recovery capabilities where applicable.

5.9 API Security

- All APIs hosted, consumed, or exposed through cloud environments **shall require strong authentication and authorization controls**.

- Public exposure of APIs **shall be prohibited unless formally approved** by the Information Security Team.

- All API communication **shall be encrypted** and protected using an API Gateway, WAF, or equivalent service.

- API access keys, tokens, and secrets **shall be securely stored, rotated, and monitored** according to the Key Management Policy.

- API activity **shall be logged, monitored, and analyzed** for anomalous or malicious behavior.

5.10 Secure Integration & Interconnectivity

- All integrations between cloud and on-premises systems **shall use secure connection mechanisms** such as VPN, Direct Connect, ExpressRoute, or private endpoints.

- Direct public access to databases, administrative interfaces, or internal services **shall be strictly prohibited**.

- Data transferred between environments **shall be encrypted end-to-end** using approved cryptographic protocols.

- Integration patterns **shall be reviewed and approved** by the Cloud Security Architect prior to implementation.

- Multi-cloud and hybrid-cloud connectivity **shall follow standardized security controls**, including routing restrictions, identity validation, and traffic inspection.

5.11 Cloud Service Approval & Change Control

- No cloud workload, configuration, or environment may be deployed without **undergoing the organization's formal change control process**.
- All cloud architecture changes **shall undergo a security review and require approval** from the Information Security Team or CISO.
- Unauthorized creation of cloud resources or environments **shall be treated as a policy violation**.
- All changes impacting cloud security, availability, or data handling **shall be documented and traceable** through the ITSM or change management system.
- Emergency changes **shall follow expedited approval workflows**, with documentation completed immediately after implementation.

6. CLOUD ACCESS MANAGEMENT

[ORG NAME] shall enforce strict identity and access management controls across all cloud platforms to ensure that only authorized users, systems, and services can access cloud resources. All access must follow least privilege principles, undergo continuous validation, and be monitored for misuse or anomalies.

6.1 Identity and Access Governance

- All access to cloud environments **shall be managed through centralized Identity and Access Management (IAM)** systems approved by the Information Security Team.
- Every cloud identity (user, role, service account) **shall have a defined owner**, lifecycle, and documented purpose.
- Cloud identities **shall not be created, modified, or removed** without approval from the respective manager and the Information Security Team.
- Access to cloud resources **shall be granted only after proper authorization** and must map to a documented business requirement.
- Shared accounts, generic accounts, or anonymous cloud identities **shall not be permitted** under any circumstances.

6.2 Least Privilege and Role-Based Access Control (RBAC)

- All cloud access **shall follow the principle of least privilege**, granting users only the minimal access required to perform their duties.
- Access to cloud resources **shall be implemented using Role-Based Access Control (RBAC)** and not via individual custom permissions.
- Privileged roles (e.g., admin, root, owner) **shall be strictly controlled**, limited, and monitored.
- Direct assignment of permissions to users **shall be prohibited** unless no viable alternative exists and an exception is approved.
- Periodic reviews **shall be conducted** to validate that access permissions remain appropriate and aligned with job responsibilities.

6.3 Multi-Factor Authentication (MFA) and Strong Authentication

- Multi-Factor Authentication **shall be mandatory** for all access to cloud consoles, administrative portals, and privileged actions.
- API, CLI, and programmatic access **shall use secure authentication mechanisms**, such as IAM roles, short-lived tokens, or signed requests.
- Password-based cloud access **shall not be used** where token-based or key-based access is available.
- Any identity used for cloud access **shall comply with the Password and Authentication Policy**, including complexity, rotation, and reuse requirements.

6.4 Just-In-Time (JIT) and Time-Bound Access

- Privileged or administrative access to cloud systems **shall be granted only on a Just-In-Time (JIT) basis**, and revoked automatically after the approved duration.
- Temporary elevated access **shall require documented approval**, including justification, requester details, and validity period.
- Standing administrative privileges **shall be minimized** and reviewed regularly to prevent privilege accumulation.
- Expired or unused access **shall be automatically terminated** using cloud-native tools or identity lifecycle automation.

6.5 Service Accounts, Machine Identities, and API Access

- Service accounts and machine identities **shall use unique credentials**, not shared with human users.
- Privileges assigned to service accounts **shall be restricted to the minimum required** for the associated system or application.
- API keys, client secrets, certificates, and tokens **shall be stored in secure, approved secret management solutions** (e.g., KMS, Vault, Secrets Manager).
- Hardcoding secrets in code, IaC templates, scripts, or configuration files **shall be strictly prohibited**.
- All machine identities **shall be rotated periodically** and monitored for anomalous behaviour.

6.6 Access Provisioning and Deprovisioning

- Access provisioning **shall follow a documented workflow**, including request, approval, verification, and logging.
- Revised access or role changes **shall be processed immediately** upon job role updates, internal transfers, or changes in responsibilities.
- Access revocation **shall occur within 24 hours** of user offboarding, contract termination, or privilege removal.
- All offboarding events **shall include the mandatory removal** of cloud access, keys, tokens, and federated identities.
- Access lifecycle records **shall be maintained** for auditing and compliance validation.

6.7 Privileged Access Management (PAM)

- Administrative and high-risk roles (e.g., root, global admin, subscription owner) **shall be restricted to designated individuals** and monitored continuously.
- Root or super-admin accounts **shall not be used for day-to-day operations** and shall remain locked unless explicitly needed.
- Privileged actions **shall be logged, monitored, and reviewed** by the Information Security Team.

- Break-glass or emergency access mechanisms **shall be tightly controlled** and documented after use.

6.8 Federated Access and Single Sign-On (SSO)

- Cloud access **shall integrate with organization-approved Single Sign-On (SSO)** providers using SAML, OAuth, or OpenID Connect.
- Local cloud accounts **shall be prohibited** unless required by the CSP for emergency recovery purposes and approved as exceptions.
- Identity federation **shall enforce MFA**, conditional access rules, and device trust validation.
- Any change to identity federation settings **shall require prior approval** from the Information Security Team.

6.9 Periodic Access Reviews

- All cloud access permissions **shall undergo a formal access review** at least quarterly.
- Privileged access **shall undergo additional review**, at minimum once per month.
- The Information Security Team **shall coordinate access reviews** and ensure that identified issues are remediated promptly.
- Non-compliant access, role creep, or excessive permissions **shall be corrected immediately** to align with least privilege requirements.

6.10 Monitoring, Logging, and Anomaly Detection for Access

- All cloud identity and access activities shall be logged, including login attempts, privilege escalations, role changes, and API requests.
- Anomalous or suspicious authentication events shall trigger automated alerts and be investigated promptly.
- Logs related to identity and access shall be retained and protected as per the Logging and Monitoring Policy.
- Continuous monitoring tools (e.g., CSPM, IAM analyzers, cloud-native threat detection) shall be implemented to detect unauthorized or risky access behavior.

7. CLOUD DATA SECURITY

[ORG NAME] shall ensure that all data stored, processed, or transmitted in cloud environments is protected against unauthorized access, disclosure, alteration, and loss. All cloud data handling must comply with the organization's Data Classification Policy, legal obligations, and industry security standards.

7.1 Data Classification and Handling Requirements

- All data stored or processed in cloud environments **shall be classified** in accordance with the Data Classification, Protection & Retention Policy.
- Cloud resources **shall enforce data handling controls** based on the assigned classification (Restricted, Confidential, Internal, Public).
- Sensitive and regulated data **shall not be stored in cloud services** unless explicitly approved by the Information Security Team.
- Data classified as Restricted or Confidential **shall only be stored in approved cloud services** that provide encryption, access control, and audit logging.
- Unapproved cloud storage locations (e.g., personal cloud drives, consumer-grade services) **shall be strictly prohibited** for storing organizational data.

7.2 Data Storage and Access Controls

- Access to cloud-stored data **shall be restricted to authorized users** based on least privilege and need-to-know principles.
- Cloud storage permissions **shall be managed through IAM roles and policies** rather than through public access settings.
- Public access to cloud storage (e.g., public S3 buckets, public Blob containers) **shall be disabled by default** and only enabled upon documented approval.
- Storage containers, file systems, and databases **shall implement object-level or row-level access controls** where applicable.
- Access logs for data stores **shall be enabled and retained** in accordance with the Logging & Monitoring Policy.

7.3 Data Encryption at Rest

- All data classified as Internal, Confidential, or Restricted **shall be encrypted at rest** using cloud-native encryption services (e.g., KMS, HSM, CMK).
- Customer-managed keys (CMKs) **shall be used** for sensitive workloads where regulatory or contractual requirements apply.
- Encryption keys **shall be rotated periodically** as per the Key Management Policy.
- Unencrypted storage of sensitive data **shall be strictly prohibited**.
- Access to encryption keys **shall be restricted to authorized roles** and shall be logged and monitored for anomalous activity.

7.4 Data Encryption in Transit

- All data transmitted to, from, or within cloud environments **shall be encrypted in transit** using approved protocols (e.g., TLS 1.2+, HTTPS, SSH).
- Plain-text transmission of sensitive data **shall be strictly prohibited** under all circumstances.
- API endpoints, load balancers, and integrations **shall enforce HTTPS-only communication**.
- Insecure or deprecated protocols (e.g., SSL, TLS 1.0/1.1, FTP, Telnet) **shall not be used** for cloud communications.

7.5 Data Residency and Sovereignty

- Data residency requirements **shall be documented and enforced** for all cloud-hosted data.
- Cloud environments storing customer or regulated data **shall be deployed in approved geographic regions** only.
- Cross-border data transfers **shall comply with contractual, regulatory, and legal requirements**, including GDPR, DPDP Act, and sectoral mandates.
- Any request to store data outside approved regions **shall undergo a formal risk assessment** and require CISO approval.

7.6 Backup, Snapshots, and Data Recovery

- All critical cloud data **shall be backed up automatically** using approved cloud-native backup mechanisms.
- Backup frequency, retention, and storage locations **shall comply with the Data Retention Policy** and business continuity requirements.
- Backups **shall be encrypted both at rest and in transit**.
- Backup copies **shall not be stored in the same region or availability zone** as the primary data to avoid single-point failures.
- Backup restoration procedures **shall be tested periodically** to ensure recoverability and integrity.

7.7 Data Loss Prevention (DLP) Controls

- DLP policies **shall be implemented** across cloud services to detect and prevent unauthorized data movement or leakage.
- Sensitive data (e.g., PII, financial data, health data, customer data) **shall be monitored using DLP classifiers and rules**.
- Unauthorized data sharing (e.g., downloading to personal devices, sending to external emails) **shall be blocked or alerted** based on severity.
- Cloud DLP alerts **shall be reviewed regularly** by the Information Security Team to identify misuse or data exfiltration attempts.

7.8 Secure Data Deletion and Purging

- Data that is no longer required **shall be securely deleted** following the Data Retention and Disposal Policy.
- Cloud-native secure deletion methods (e.g., cryptographic erasure, secure purge) **shall be used to ensure irretrievable data destruction**.
- Deletion of sensitive or regulated data **shall be verified and logged**.
- Cloud vendors **shall provide data deletion confirmation** where contractual obligations require proof of destruction.

7.9 Public Sharing and External Transfer Restrictions

- Cloud data **shall not be publicly shared** without explicit approval from the Information Security Team and Data Owner.
- External transfers of sensitive data **shall require encryption**, access control, and documented authorization.
- Sharing data through unsecured channels (e.g., public links, anonymous access, non-approved APIs) **shall be strictly prohibited**.

7.10 Data Integrity and Version Protection

- Cloud data repositories **shall implement integrity protections** such as object locking, versioning, and write-once-read-many (WORM) controls where applicable.
- Cloud applications handling critical transactions **shall implement integrity checks**, including hashing, digital signatures, or checksums.
- Any data integrity violation **shall be logged, investigated, and remediated** under the Incident Management Policy.

7.11 Logging and Monitoring for Data Security

- All access to cloud data stores **shall be logged in real-time** and retained as per policy requirements.
- Logs related to data access, modification, deletion, or export **shall be continuously monitored** for anomalies.
- Automated alerting **shall be configured** for suspicious data-related events (e.g., mass downloads, large deletions, unauthorized changes).
- Data security logs **shall not be disabled, removed, or modified** without authorization.

7.12 SaaS Data Security Requirements

- SaaS providers handling organizational data **shall meet the same data protection requirements** defined in this policy.
- SaaS configurations (e.g., sharing rules, external access, DLP, tenant restrictions) **shall be reviewed and secured** prior to onboarding.

- Export of data from SaaS platforms **shall require Data Owner approval** and encryption-in-transit controls.

8. DATA RETENTION AND DISPOSAL

[ORG NAME] shall implement strong network security controls across all cloud environments to prevent unauthorized access, restrict lateral movement, secure communication paths, and maintain segmentation based on business, regulatory, and security requirements.

8.1 Network Segmentation and Isolation

- All cloud environments **shall be segmented logically and physically** using VPCs, VLANs, subnets, or equivalent isolation constructs.
- Production, staging, development, and testing environments **shall be strictly isolated** and must not share networks, security groups, or routing tables without formal approval.
- Application tiers (web, application, database) **shall operate in separate subnets** with controlled communication paths.
- Sensitive workloads **shall be placed in private subnets** with no direct inbound internet exposure.
- Network segmentation configurations **shall be reviewed regularly** to ensure compliance and identify misconfigurations.

8.2 Ingress and Egress Traffic Control

- All inbound and outbound network traffic **shall be restricted using firewall rules, security groups, or network security groups (NSGs)**.
- Default security group or firewall rules **shall deny all traffic by default** (“default deny”) unless explicitly required and approved.
- Any rule allowing inbound internet traffic **shall require documented justification, risk assessment, and prior approval** from the Information Security Team.
- Outbound internet access **shall be restricted and monitored**, especially for sensitive workloads and critical systems.
- Unauthorized, unused, or overly permissive rules **shall be removed immediately** upon detection.

8.3 Public Exposure Restrictions

- Public exposure of cloud resources (e.g., VM public IPs, exposed APIs, publicly accessible databases) **shall be prohibited** unless approved by the Cloud Security Architect.
- Resources requiring public access **shall be protected** using load balancers, WAFs, API gateways, or reverse proxies.
- Direct internet access to administrative ports (SSH, RDP, database ports) **shall be strictly prohibited**; bastion hosts or session managers shall be used instead.
- Public buckets, containers, and storage objects **shall be blocked by default** and must not be made public without Data Owner and Security approval.

8.4 Secure Connectivity for Hybrid and Multi-Cloud Architecture

- Connectivity between cloud and on-premises environments **shall only use approved secure connection mechanisms** (VPN, Direct Connect, ExpressRoute, Interconnect).
- All hybrid cloud links **shall enforce encryption-in-transit** and strong authentication.
- Peering between VPCs/VLANs or cloud regions **shall require formal approval** and must follow segmentation principles.
- Rogue or undocumented network connections **shall be prohibited** and dismantled immediately upon discovery.
- Cross-cloud or cross-region traffic **shall be monitored** and logged to detect anomalous routing or exfiltration attempts.

8.5 DNS Security and Name Resolution Controls

- Cloud-based DNS services **shall enforce secure configurations**, including DNSSEC support where available.
- Internal DNS zones **shall be segregated** from external/public DNS zones to prevent data leakage.
- DNS logging **shall be enabled** to record all DNS queries, failures, and suspicious lookups.

- Critical cloud services **shall not rely solely on public DNS**; fallback internal DNS must be configured when necessary.

- DNS manipulation, poisoning, or unauthorized zone modifications **shall be treated as a security incident**.

8.6 Load Balancers, Gateways, and API Traffic Controls

- All inbound application traffic **shall pass through approved load balancers, WAFs, or API gateways**; direct access to backend systems shall be prohibited.

- TLS termination and certificate management **shall be handled through secure, approved mechanisms**.

- API gateways **shall enforce authentication, authorization, throttling, and rate limits** to protect against abuse.

- WAF rules and signatures **shall be updated continuously** to defend against common web attacks (OWASP Top 10).

8.7 Network Encryption Requirements

- All communication within and across cloud networks **shall be encrypted in transit** using TLS 1.2+ or equivalent secure protocols.

- Internal traffic between microservices, containers, and workloads **shall be encrypted** using mTLS or service mesh technologies where applicable.

- Unencrypted communication between cloud services **shall be strictly prohibited**.

- Deprecated protocols (e.g., SSL, TLS 1.0/1.1, FTP, Telnet) **shall not be used** in any cloud configuration.

8.8 Firewall, Security Group, and ACL Management

- Firewall and security group configurations **shall follow the principle of least privilege**, allowing only necessary ports and protocols.

- Automatic removal of unused rules **shall be enabled**, where supported by cloud-native tools.

- Security groups and ACLs **shall not be configured to allow unrestricted access** (e.g., 0.0.0.0/0) without formal risk acceptance.

- All changes to network ACLs, routing tables, or firewall rules **shall follow the organization's change management workflow**.

- High-risk rules **shall trigger automated alerts** and require immediate review.

8.9 Traffic Monitoring, Inspection, and Threat Detection

- All cloud network traffic **shall be monitored using cloud-native networking logs and IDS/IPS systems** where applicable.

- Advanced threat detection tools (e.g., GuardDuty, Azure Defender, Cloud IDS) **shall be enabled** for continuous analysis.

- East-west (lateral) traffic **shall be monitored** to detect unauthorized movement within cloud environments.

- Alerts involving suspicious or anomalous network behaviour **shall be escalated immediately** for investigation.

- Use of encrypted traffic inspection technologies **shall be implemented where feasible** to detect hidden threats.

8.10 DDoS Protection and Network Resiliency

- All internet-facing workloads **shall use cloud-native DDoS protection services** (e.g., AWS Shield, Azure DDoS Protection).

- High-availability architectures **shall be employed** to mitigate the impact of network-level attacks and failures.

- Rate limiting, connection throttling, and traffic shaping **shall be implemented** for critical workloads.

- Network resiliency controls **shall be reviewed and tested periodically** to ensure effectiveness.

8.11 Prohibited Networking Practices

- Direct internet access to backend, database, or sensitive workloads **shall be prohibited**.

- Flat network architectures without segmentation **shall not be allowed**.

- P2P networking, TOR, anonymizers, or unauthorized tunnels **shall not be used** in cloud environments.
- Hardcoding IPs or bypassing approved network services **shall be prohibited**.
- The use of cloud provider "anonymous access" features **is strictly forbidden** without formal exception approval.

9. CLOUD PLATFORM SECURITY CONTROLS

[ORG NAME] shall implement strong and standardized security controls for all cloud compute platforms, workloads, and managed services. These controls apply to virtual machines, containers, Kubernetes clusters, serverless functions, managed databases, storage services, and any cloud-native components used by the organization.

9.1 Virtual Machines (VMs) and Compute Instances

- All cloud VMs **shall be deployed from approved and hardened images** maintained by [ORG NAME].
- Default or vendor-provided images **shall not be used** unless they are hardened and approved by the Information Security Team.
- Administrative access to VMs **shall be restricted**, requiring MFA and secured through bastion hosts or session management services.
- Direct SSH/RDP access from the internet **shall be strictly prohibited**.
- Operating systems and VM software **shall be patched regularly**, following the Patch and Vulnerability Management Policy.
- VM disks **shall be encrypted at rest** using approved cloud-native encryption technologies.
- Endpoint protection or runtime security agents **shall be installed** on all VMs hosting sensitive workloads.

9.2 Container Security

- All container images **shall be built from approved base images** stored in an internal registry.
- Public container images **shall not be used** unless scanned, validated, and approved by the Information Security Team.

- Container images **shall undergo vulnerability scanning** before deployment and on a continuous basis.
- Containers **shall run as non-root users** unless a documented exception is approved.
- Secrets, passwords, and sensitive configurations **shall not be hardcoded** into container images.
- Runtime security monitoring **shall be enabled** for container workloads to detect behavioural anomalies.

9.3 Kubernetes (K8s) and Orchestrated Workloads

- Kubernetes clusters **shall be deployed using organization-approved configurations** with RBAC, network policies, and admission controls enforced.
- Access to Kubernetes control planes **shall be restricted**, requiring MFA and authenticated connections only.
- Kubernetes API server **shall not be exposed publicly** unless approved by the Cloud Security Architect.
- Kubernetes network policies **shall be implemented** to restrict pod-to-pod and pod-to-service communication.
- Pod security standards (or equivalent) **shall be enforced**, including constraints on privilege escalation, file system access, and capabilities.
- Secrets stored in Kubernetes **shall be encrypted** and managed through approved secret management services.
- Cluster-level logs and audit trails **shall be enabled and retained** according to the Logging and Monitoring Policy.

9.4 Serverless (Function-as-a-Service) Security

- Serverless functions **shall follow least privilege principles**, using tightly scoped IAM roles.
- Functions **shall not embed secrets**, API keys, or credentials in code or environment variables.

- All external calls from serverless functions **shall use secure communication channels** (TLS 1.2+).

- Function logs **shall be enabled**, including execution logs, errors, and invocation metadata.

- Each function **shall be monitored for abnormal invocation patterns**, high error rates, or suspicious access attempts.

- Serverless environments **shall be scanned regularly** for vulnerabilities in runtimes, dependencies, and libraries.

9.5 Managed Databases and PaaS Workloads

- Managed databases (SQL, NoSQL, cache services) **shall not be publicly accessible** under any circumstances unless explicitly approved.

- Encryption at rest and in transit **shall be enabled by default** for all managed database services.

- Database authentication **shall use IAM roles or identity-based access** rather than embedded credentials where supported.

- Automated backups, point-in-time recovery, and failover **shall be enabled** for critical database workloads.

- Database audit logging **shall be activated**, capturing access, changes, queries (where applicable), and security events.

- Database parameter groups **shall be configured according to approved hardening standards**.

9.6 Storage Services and Object Stores

- Storage services (buckets, blob stores, file shares) **shall be private by default** with no public ACLs or anonymous access.

- Sensitive or regulated data **shall not be stored** in object storage without encryption and DLP enforcement.

- Object versioning **shall be enabled** for critical storage buckets to prevent accidental deletion or overwrite.

- Access to storage objects **shall be logged**, including read, write, delete, and permission-change events.

- Object lifecycle rules **shall be configured** to enforce retention periods and secure deletion.

9.7 Workload Hardening and Baseline Enforcement

- All cloud workloads **shall comply with organization-approved hardening benchmarks**, including CIS, NIST, and cloud platform baselines.

- Baseline configurations **shall define minimum security controls** for compute, storage, databases, identity, and networking.

- Any deviation from the baseline **shall require a documented exception**, approved by the Information Security Team.

- Hardening checks **shall be automated wherever possible** using CSPM, IaC scanning, or continuous compliance tools.

9.8 Patch Management and Vulnerability Remediation

- All workloads running in the cloud **shall be patched regularly** and in accordance with the Patch and Vulnerability Management Policy.

- High-severity vulnerabilities in cloud workloads **shall be remediated within defined SLA timelines**.

- Unpatched workloads hosting sensitive data **shall be isolated** until remediation is complete.

- Cloud-native vulnerability assessment tools **shall be enabled** and integrated into the security pipeline.

9.9 Logging, Monitoring, and Telemetry Controls

- Cloud-native logging (e.g., CloudTrail, Activity Logs, Audit Logs) **shall be enabled** for all workloads and services.

- Logs for compute, containers, databases, serverless functions, and platforms **shall be forwarded to the central SIEM**.

- Tampering, disabling, or modifying logging configurations **shall be prohibited** without authorization.

- Monitoring and alerts **shall be configured** for CPU spikes, memory anomalies, privilege escalations, network deviations, and suspicious user actions.

9.10 Workload Identity and Secret Management

- Machine identities and workload identities **shall be controlled through IAM roles, service principals, or managed identities**.
- Secrets, tokens, and credentials **shall be stored only in approved secret management systems** (e.g., KMS, Vault, Secrets Manager).
- Secret rotation **shall be automated** wherever possible.
- Any workload accessing secrets **shall use least-privilege access policies**.

9.11 Prohibited Workload Practices

- Hardcoded secrets in code, containers, scripts, IaC, or configurations **shall be strictly prohibited**.
- Running privileged containers, root-access workloads, or unapproved images **shall not be permitted**.
- Unsupported, outdated, or unpatched workloads **shall not be deployed** in any cloud environment.
- Direct database access over the public internet **is strictly forbidden** unless approved through formal exceptions.

10. CLOUD CONFIGURATION MANAGEMENT

[ORG NAME] shall implement standardized, automated, and continuously enforced configuration management controls across all cloud environments to ensure secure, consistent, and compliant deployments. Configuration changes shall follow approved baselines, undergo security validation, and be monitored for drift, improper modifications, or risky configurations.

10.1 Standard Configuration Baselines

- All cloud resources **shall adhere to standardized configuration baselines** defined by [ORG NAME], referencing CIS Benchmarks, NIST guidelines, and CSA CCM requirements.
- Cloud configuration baselines **shall include mandatory controls** for IAM, networking, encryption, storage, databases, logging, monitoring, and workload

security.

- No cloud workload or resource may be deployed unless **it meets or exceeds the approved baseline**.

- Configuration baselines **shall be reviewed and updated periodically** to address evolving threats, cloud provider changes, and compliance obligations.

10.2 Infrastructure-as-Code (IaC) Requirements

- All cloud deployments **shall be performed using approved Infrastructure-as-Code (IaC) templates**, unless an exception is approved.

- IaC templates **shall be stored in secured, version-controlled repositories** with access restricted to authorized personnel.

- Changes to IaC templates **shall undergo mandatory peer review**, automated security scanning, and approval prior to deployment.

- IaC templates **shall not contain hardcoded secrets** or sensitive information under any circumstances.

- Drift between IaC templates and deployed resources **shall be detected and remediated promptly** using automated tools where possible.

10.3 Configuration Drift Detection and Remediation

- All cloud environments **shall be continuously monitored** for configuration drift, unauthorized changes, or deviations from approved baselines.

- Any detected drift **shall be reviewed immediately** and remediated according to risk severity.

- Unauthorized configuration changes **shall be treated as security incidents** and escalated according to the Incident Management Policy.

- Cloud-native and third-party configuration monitoring tools (e.g., CSPM, IaC scanners) **shall be implemented** to enforce continuous compliance.

10.4 DevSecOps & CI/CD Security Controls

- All CI/CD pipelines **shall enforce security checks**, including IaC validation, vulnerability scanning, secret detection, and compliance verification.

- Deployments to cloud environments **shall not bypass CI/CD pipelines** unless formally approved under emergency procedures.
- Build and deployment artifacts **shall be signed, validated, and tracked** to maintain supply chain integrity.
- Privileged operations within pipelines **shall require strong authentication** and proper access control.
- CI/CD systems **shall be isolated from production environments**, and their access shall be restricted to least privilege.

10.5 Configuration Change Management

- All changes to cloud configurations **shall follow the organization's Change Management Policy**, including risk assessment, testing, approval, and documentation.
- Emergency configuration changes **shall be logged, reviewed, and formally documented** immediately after implementation.
- No configuration change may be applied directly in production **without formal approval** and required validations.
- High-impact or high-risk changes (network, IAM, encryption, logging) **shall require CISO or Cloud Security Architect approval**.

10.6 Preventing Misconfigurations

- All cloud s**ervices shall enable guardrails**, such as cloud-native policies, SCPs, OPA policies, or Config Rules, to prevent insecure settings.
- Misconfigurations identified by CSPM, CI/CD, or monitoring tools **shall be remediated within defined SLA timelines** based on severity.
- Any configuration that introduces public exposure, wide access, or insecure defaults **shall be automatically blocked or quarantined**, where supported.
- Teams **shall not disable CSPM, logging, or monitoring tools** without an approved exception.

10.7 Tagging, Metadata, and Resource Identification

- All cloud resources **shall follow the organization's mandatory tagging and naming standards** for ownership, environment, classification, and lifecycle management.
- Untagged or improperly tagged resources **shall be flagged and corrected** through automated workflows.
- Tags assigned to cloud resources **shall not be removed, modified, or falsified** without authorization.
- Resource metadata **shall remain consistent with asset inventory and CMDB records**.

10.8 Compliance Automation

- Continuous compliance checks **shall be automated** using CSPM, IaC scanners, and policy-as-code frameworks.
- Configuration non-compliance **shall trigger real-time alerts** sent to the responsible teams and Information Security.
- Compliance results **shall be reviewed regularly** as part of operational and governance meetings.
- Repeated or systemic non-compliance **shall require a corrective action plan (CAPA)** approved by the Information Security Team.

10.9 Prohibited Configuration Practices

- Direct manual editing of cloud configurations in production **is prohibited**, except under approved emergency conditions.
- Hardcoding credentials, API keys, or tokens in configurations **shall be strictly prohibited**.
- Publicly accessible configurations (e.g., open security groups, public storage) **shall not be allowed** without formal risk acceptance.
- Disabling encryption, logging, monitoring, or security controls **shall not be permitted** without authorized exceptions.

11. VENDOR & THIRD-PARTY CLOUD SECURITY

[ORG NAME] shall ensure that all cloud vendors, third-party service providers, and SaaS platforms are evaluated, onboarded, monitored, and managed in accordance with the organization's security, privacy, and compliance requirements. No third-party cloud service may be used unless approved through the organization's vendor security due diligence process.

11.1 Vendor Security Due Diligence

- All cloud vendors and SaaS providers **shall undergo a formal security due diligence assessment** before onboarding.
- Vendor assessments **shall evaluate security controls, compliance certifications, data protection practices, and operational resilience**.
- Cloud vendors lacking adequate security controls or certifications **shall not be approved** for use without compensating controls and risk acceptance.
- The Information Security Team **shall review and approve** the security posture of all vendors prior to contract execution.

11.2 Mandatory Security and Compliance Requirements

- Cloud vendors handling [ORG NAME] data **shall maintain valid security certifications**, such as ISO 27001, SOC 2 Type II, or CSA STAR.
- Vendors processing regulated or sensitive data **shall demonstrate compliance** with applicable legal frameworks (GDPR, DPDP Act, HIPAA, PCI, etc.).
- Vendors **shall maintain documented security policies**, incident response procedures, and business continuity plans.
- Vendors lacking required certifications **shall be considered high risk** and may be rejected unless the CISO grants an approved exception.

11.3 Contractual and Legal Requirements

- All vendor contracts **shall contain mandatory security, confidentiality, and data protection clauses**, including encryption, breach notification, access management, and audit rights.
- Contracts **shall specify data residency, retention, and deletion obligations** for cloud-stored data.

- Data Processing Agreements (DPAs) **shall be executed** for vendors processing personal or sensitive personal data.

- Contracts **shall require the vendor to provide evidence of secure data deletion** upon service termination.

- Vendors **shall be legally bound** to notify [ORG NAME] of any security incident affecting organizational data within the agreed SLA.

11.4 Third-Party Access Management

- Third-party users or support personnel **shall receive access only after formal approval** and must comply with [ORG NAME]'s access control requirements.

- Vendor access **shall be time-bound, role-based, and least-privileged**.

- Persistent or standing third-party access **shall be prohibited**, unless explicitly approved.

- All vendor access sessions **shall be logged, monitored, and subject to review**.

- Access for third parties **shall be immediately revoked** upon contract completion, project closure, or inactivity.

11.5 Cloud Vendor Risk Monitoring

- Vendors **shall be monitored continuously** for changes in security posture, compliance status, or emerging risks.

- The Vendor Management Team **shall review vendor performance and risk reports** at least annually.

- External threat intelligence and breach monitoring **shall be used** to detect vendor-related risks.

- Vendors found to have critical vulnerabilities or security weaknesses **shall be required to remediate issues** within defined SLA timelines.

- High-risk vendors **shall undergo enhanced monitoring** or may be removed from service if risks cannot be mitigated.

11.6 SaaS Application Security Requirements

- All SaaS applications used by [ORG NAME] **shall enforce strong access controls**, encryption, audit logging, and data protection settings.
- SaaS configuration settings (sharing restrictions, access rules, external collaboration) **shall be reviewed and hardened** during onboarding.
- SaaS applications **shall integrate with the organization's SSO and MFA** solutions wherever possible.
- SaaS providers **shall not be granted unrestricted API access** unless required and approved by the Information Security Team.

11.7 Data Handling by Third Parties

- Vendors handling organizational data **shall store, process, and transmit data only in approved geographic regions**.
- Sensitive and regulated data **shall be encrypted at rest and in transit** by the vendor.
- Vendors **shall not subcontract or transfer data** to other entities unless explicitly permitted by contract.
- Any vendor unable to meet minimum data protection requirements **shall not be allowed** to handle [ORG NAME] data.

11.8 Termination and Offboarding of Vendor Services

- Upon termination of a cloud vendor or SaaS service, vendors **shall securely delete all organizational data**, including backups and replicas.
- Vendors **shall provide written confirmation of data deletion**, including logs or certificates of sanitization.
- All vendor access credentials, tokens, and integrations **shall be revoked immediately** upon contract termination.
- A formal offboarding checklist **shall be completed** to ensure that no data or access remains with the vendor.

11.9 Prohibited Third-Party Activities

- Vendors **shall not use organizational data for analytics, profiling, model training, or secondary purposes** without explicit written permission.
- Vendors **shall not store data in unapproved cloud locations** or transfer data across borders without authorization.
- Unauthorized subcontracting, shadow IT services, or unapproved integrations **shall be strictly prohibited**.
- Vendors failing to comply with contractual or security requirements **shall be subject to corrective action, contract termination, or legal escalation**.

12. LOGGING, MONITORING & INCIDENT DETECTION

[ORG NAME] shall implement comprehensive logging, monitoring, and threat detection mechanisms across all cloud environments to ensure timely identification of security events, unauthorized activities, and anomalies. All logs and monitoring configurations must comply with organizational, regulatory, and contractual requirements.

12.1 Mandatory Cloud Logging Requirements

- All cloud platforms **shall have logging enabled by default**, including platform logs, resource logs, and audit logs.
- Administrative actions, configuration changes, authentication events, privilege escalations, API calls, and access attempts **shall be fully logged**.
- Cloud-native logging services (e.g., CloudTrail, Azure Activity Logs, GCP Audit Logs) **shall be activated for all accounts, regions, and subscriptions**.
- Logs **shall not be disabled, altered, truncated, or overwritten** without authorized approval.
- Missing, incomplete, or misconfigured logging **shall be treated as a security incident**.

12.2 Centralized Log Collection & Retention

- All cloud logs **shall be forwarded to the organization's centralized SIEM** or log management platform.

- Logs **shall be retained for the duration required** under the Logging & Monitoring Policy, regulatory mandates, and contractual obligations.
- Storage and retention for logs **shall be secure, tamper-proof, and encrypted**.
- Logs **shall not be stored on local instances or ephemeral storage** where they may be lost or deleted.

12.3 Monitoring of Cloud Workloads and Services

- All cloud workloads (VMs, containers, serverless functions, databases, APIs) **shall be continuously monitored** using cloud-native or third-party monitoring tools.
- Resource performance, errors, failures, and unusual patterns **shall generate alerts** for investigation.
- Monitoring configurations **shall not be disabled or modified** without approval from the Information Security Team.
- Monitoring dashboards, metrics, and alerts **shall be reviewed regularly** by responsible teams.

12.4 Threat Detection and Cloud-native Security Services

- Cloud-native threat detection services (e.g., GuardDuty, Defender for Cloud, Security Command Center) **shall be enabled and monitored** in all cloud environments.
- Threat intelligence-driven alerts **shall be reviewed promptly** and escalated according to severity.
- Automated threat detection tools **shall monitor for anomalous behavior**, including credential misuse, unusual data access, and network anomalies.
- Suppressing or disabling threat detection alerts **is prohibited**, except under authorized change control.

12.5 API and Identity Activity Monitoring

- All API activity **shall be logged and monitored** for suspicious or unauthorized requests.

- Unusual identity behavior (e.g., impossible travel, excessive access attempts, privilege escalation) **shall trigger automated alerts**.

- Service accounts and machine identities **shall be monitored** for anomalous access patterns or abuse.

- Failed authentication attempts, MFA bypass attempts, and access denials **shall be investigated** as potential security incidents.

12.6 Network Traffic Monitoring

- All inbound, outbound, and internal network traffic in the cloud **shall be logged and inspected** using approved tools.

- Network monitoring **shall detect unauthorized connections**, lateral movement, or communication with suspicious endpoints.

- Traffic mirroring or packet inspection tools **shall be used** where required for compliance, threat detection, or forensic analysis.

- Sudden spikes, unusual data transfers, or unexpected connections **shall trigger alerts** and require investigation.

12.7 Alerting, Correlation, and Automated Response

- Alerts from cloud platforms, SIEM, CSPM, CWPP, and other security tools **shall be correlated** to identify patterns and potential compromises.

- Critical alerts **shall trigger automated notifications** to the Information Security Team.

- Automated remediation workflows (e.g., policy-as-code, Lambda functions, Logic Apps) **shall be used** where feasible to reduce exposure time.

- Repeated or ignored alerts **shall be escalated** to management and treated as operational non-compliance.

12.8 Log Integrity and Protection

- Logs **shall be protected against unauthorized access, modification, and deletion**.

- Log integrity checks **shall be implemented** to detect tampering or corruption.

- Access to logs **shall be strictly limited** to authorized personnel.
- Any attempt to manipulate or delete logs **shall be treated as a major security violation**.

12.9 Incident Detection and Escalation

- Any event indicating a potential security compromise **shall be classified as a security incident** and escalated according to the Incident Management Policy.
- Cloud platform alerts for data exfiltration, privilege escalation, policy violations, or suspicious activities **shall be investigated immediately**.
- Incidents involving cloud resources **shall follow the same triage, response, containment, and reporting processes** as on-premises incidents.
- High-risk incidents **shall be escalated to the CISO immediately** and reported according to regulatory timelines if applicable.

12.10 Continuous Improvement and Tuning

- Logging, monitoring, and alerting configurations **shall be reviewed periodically** to improve detection accuracy.
- False positives, noise, or redundant alerts **shall be tuned** to enhance detection effectiveness without reducing security coverage.
- Lessons learned from incidents **shall be incorporated** into monitoring improvements and control enhancements.
- Monitoring rules **shall evolve** to address emerging threats, cloud provider updates, and changes in business operations.

13.CLOUD BACKUP, CONTINUITY & DISASTER RECOVERY

[ORG NAME] shall implement robust cloud backup, business continuity, and disaster recovery (DR) controls to ensure the availability, integrity, and recoverability of cloud-hosted data and services. All critical workloads must be architected for resilience and tested regularly to validate continuity capabilities.

13.1 Backup Requirements

- All critical cloud data, applications, and configurations **shall be backed up using approved cloud-native or enterprise backup solutions**.

- Backups **shall be automated**, consistent, and configured to meet business-defined RPO (Recovery Point Objective) and RTO (Recovery Time Objective).
- Backup data **shall be encrypted at rest and in transit** using approved cryptographic mechanisms.
- Backups **shall not be stored in the same availability zone or same physical location** as the primary workload to avoid single points of failure.
- Backup failures **shall be monitored and investigated**, and corrective actions must be taken immediately.

13.2 Snapshot, Replication, and Versioning Controls

- Snapshots of critical workloads (VMs, databases, storage volumes) **shall be taken at defined intervals** and retained for the required duration.
- Replication across regions or availability zones **shall be enabled** for mission-critical workloads requiring high availability.
- Storage versioning (where supported) **shall be enabled** to protect against accidental or malicious modification or deletion.
- Snapshot retention policies **shall comply with the Data Retention Policy** and legal or contractual requirements.

13.3 Disaster Recovery Architecture

- All cloud workloads classified as critical **shall have a documented Disaster Recovery plan** approved by the business owner and the Information Security Team.
- DR architectures **shall include multi-zone or multi-region redundancy**, based on business impact and regulatory requirements.
- DR environments **shall maintain equivalent security controls** as production environments.
- DR failover and failback procedures **shall be documented, tested, and periodically reviewed**.
- Any modifications to the DR architecture **shall follow the formal change management process**.

13.4 Business Continuity Requirements

- Cloud-based applications supporting essential business services **shall be included** in the organization's Business Continuity Plan (BCP).
- Continuity capabilities **shall be validated annually**, including performance, failover, and recovery.
- Dependencies on third-party cloud services **shall be evaluated and incorporated** into continuity plans.
- Alternative communication, access, and operational procedures **shall be documented** to maintain essential services during disruptions.

13.5 Testing of Backup and DR Capabilities

- Backup restoration tests **shall be performed regularly**, at least semi-annually, to validate integrity and recoverability.
- DR simulations and failover exercises **shall be conducted annually**, including full or partial failover validation.
- Testing results **shall be documented**, and any identified gaps shall be remediated through a corrective action plan.
- High-risk or mission-critical applications **shall undergo more frequent testing** based on business needs.

13.6 Data Recovery Procedures

- Recovery procedures **shall be documented, accessible, and tested** by authorized personnel.
- Recovery steps **shall include verification of restored data integrity**, post-restoration access validation, and functional application checks.
- Only authorized personnel **shall perform recovery actions** to prevent unauthorized data restoration or manipulation.
- Data restored from backups **shall follow the same access control, privacy, and security requirements** as production data.

13.7 Monitoring and Alerting for Continuity Controls

- Backup jobs, replication processes, and snapshot operations **shall be continuously monitored**.
- Alerts for failed backups, replication delays, or corrupted snapshots **shall be escalated immediately** to the responsible teams.
- Continuity and DR systems **shall integrate with the organization's SIEM and monitoring tools** for centralized visibility.

13.8 Protection Against Ransomware and Data Loss Events

- Immutable backups or write-once-read-many (WORM) storage **shall be used** for critical systems to protect against ransomware.
- Backup isolation ("air-gapped" or logically isolated backups) **shall be implemented** where applicable.
- Any suspicious mass deletion, encryption attempt, or large-scale modification **shall trigger immediate investigation**.
- Recovery plans **shall include scenarios for ransomware, data corruption, insider threats, and availability failures**.

13.9 Prohibited Backup and Continuity Practices

- Backups **shall not use unencrypted storage**, temporary volumes, or personal cloud accounts.
- Manual, ad-hoc, or unmanaged backups **shall be prohibited** for production workloads.
- Backups **shall not be stored on the same instance or ephemeral disks** as the primary workload.
- Unapproved DR tools or non-validated backup solutions **shall not be used** in any environment.

14. CLOUD SECURITY REVIEW & ASSESSMENTS

[ORG NAME] shall conduct periodic security reviews, assessments, and audits of all cloud platforms, resources, and services to ensure ongoing compliance with organizational security policies, regulatory requirements, and industry best practices.

All cloud environments must undergo continuous improvement based on assessment outcomes.

14.1 Periodic Cloud Security Reviews

- All cloud accounts, subscriptions, and resource groups **shall undergo formal security review** at least quarterly.
- Reviews **shall evaluate adherence to cloud configuration baselines**, including IAM, networking, encryption, monitoring, and workload security.
- Review findings **shall be documented**, assigned to responsible teams, and tracked to closure.
- Recurrent or severe non-compliance **shall trigger corrective action plans**, including escalation to senior management.

14.2 Cloud Security Posture Management (CSPM)

- Cloud Security Posture Management tools **shall be used** to continuously monitor cloud environments for misconfigurations and compliance violations.
- CSPM alerts **shall be reviewed and remediated** according to severity-based SLA timelines.
- Disabling CSPM or bypassing its controls **shall be prohibited** without exception approval.
- CSPM baselines **shall align with CIS benchmarks, NIST standards, and organizational policies**.

14.3 Vulnerability Assessment of Cloud Workloads

- All cloud workloads (VMs, containers, serverless, PaaS components) **shall undergo periodic vulnerability scanning**.
- Critical and high-severity vulnerabilities **shall be remediated within defined SLA timelines**.
- Vulnerability scanning **shall be integrated into CI/CD pipelines**, IaC workflows, and runtime environments.
- Scans must include operating systems, runtime libraries, third-party dependencies, and container layers.

14.4 Penetration Testing of Cloud Environments

- Penetration testing **shall be performed annually** for external-facing cloud workloads and high-risk systems.
- Internal penetration testing **shall be conducted** as required to validate segmentation, privilege boundaries, and configuration security.
- Testing of cloud environments **shall comply with cloud provider rules of engagement** and legal requirements.
- All findings from penetration tests **shall be remediated** and verified through re-testing.

14.5 Misconfiguration and Hardening Assessments

- Cloud resources **shall be evaluated regularly** to detect insecure configurations, exposed services, or deviations from best practices.
- Hardening assessments **shall include networking, IAM, storage, API security, encryption, and logging**.
- Identified misconfigurations **shall be corrected immediately** or mitigated using compensating controls.
- Persistent misconfigurations **shall be escalated** to the Information Security Team and management.

14.6 Compliance Assessments

- Cloud environments handling regulated or sensitive data **shall undergo periodic compliance assessments**, including GDPR, DPDP Act, PCI, HIPAA, and contractual requirements.
- Compliance control gaps **shall be documented**, analyzed, and remediated within required timelines.
- Evidence for compliance **shall be maintained**, including logs, audit trails, configuration screenshots, and assessment reports.

14.7 SaaS Security Reviews

- SaaS platforms used by [ORG NAME] **shall undergo annual security assessment**, including configuration review, access controls, sharing policies,

and tenant security settings.

- SaaS instances **shall be reviewed for DLP, logging, encryption, external sharing restrictions, and identity integration**.
- Unauthorized or misconfigured SaaS applications **shall be disabled**, remediated, or removed as necessary.

14.8 Third-Party Cloud Vendor Assessments

- Third-party cloud providers and SaaS vendors **shall be reassessed annually** to confirm ongoing compliance with security expectations.
- Vendors experiencing security breaches, compliance violations, or critical vulnerabilities **shall undergo immediate re-evaluation**.
- Vendor certifications such as ISO 27001, SOC 2, and CSA STAR **shall be validated annually** for authenticity and scope.

14.9 Cloud Cost & Resource Optimization Reviews (Security Impact)

- Resource reviews **shall evaluate unused, underutilized, or abandoned cloud resources** that may introduce unnecessary security risks.
- Dormant accounts, stale access keys, unused VMs, and inactive storage **shall be removed or secured**.
- Cost optimization activities **shall not reduce or weaken required security controls**.

14.10 Documentation, Reporting & Corrective Actions

- All assessment activities **shall be documented**, including scope, findings, impact ratings, and remediation plans.
- Reports **shall be reviewed by the Cloud Security Architect and CISO**, with action items assigned to responsible teams.
- All remediation activities **shall be tracked** until verified as complete.
- Significant risks or systemic weaknesses **shall be escalated to senior leadership**.

15.CLOUD EXIT & SERVICE TERMINATION MANAGEMENT

[ORG NAME] shall ensure that cloud services can be securely and efficiently terminated, offboarded, or migrated without data loss, unauthorized access, vendor lock-in, or disruption to business operations. All exit activities must follow documented procedures and ensure compliance with legal, regulatory, and contractual obligations.

15.1 Exit Planning Requirements

- Every cloud service used by [ORG NAME] **shall have a documented exit plan** prior to onboarding or production use.
- Exit plans **shall define data extraction methods, supported formats, service dependencies, and expected timelines**.
- All exit plans **shall be reviewed and approved** by the Information Security Team and the respective service owner.
- Cloud service contracts **shall be evaluated** to ensure exit rights, data deletion guarantees, and portability commitments are included.
- Any cloud adoption lacking an exit strategy **shall not proceed** until the required documentation is completed.

15.2 Exit Triggers

- A cloud exit process **shall be initiated** under circumstances including, but not limited to:
    - Contract non-renewal or expiration
    - Migration to a different cloud provider or service
    - Vendor performance degradation or breach of contract
    - Security, compliance, or legal requirements
    - Organizational restructuring or service decommissioning
- The decision to exit a cloud service **shall require approval** from the business owner and the CISO.

15.3 Secure Data Extraction and Migration

- All data stored within a cloud service **shall be exported in a structured, machine-readable, and industry-standard format**, wherever possible.
- Data extraction **shall be encrypted in transit** using approved protocols.
- Data completeness and integrity **shall be verified** as part of the migration process.
- All associated metadata, logs, configuration files, and encryption keys **shall be exported** where possible and applicable.
- Manual data extraction methods **shall not be used** unless unavoidable and approved.

15.4 Data Retention and Deletion by Provider

- Upon service termination, cloud providers **shall delete all organizational data**, including replicas, snapshots, cached copies, and backups.
- Providers **shall issue a formal certificate or written confirmation of secure data deletion**.
- Data deletion **shall follow NIST 800-88 or cloud-native secure wipe standards**, ensuring irretrievable destruction.
- Any delay or refusal by the provider to delete data **shall be escalated** to Legal and the CISO for resolution.
- Providers **shall not retain organizational data** for analytics, model training, or operational purposes post-termination.

15.5 Access and Identity Decommissioning

- All cloud identities, accounts, API keys, tokens, service accounts, and federated identities **shall be revoked immediately** during service exit.
- Cross-account roles, trust relationships, and SSO integrations **shall be removed**.
- Administrator and privileged roles associated with the exiting service **shall be disabled and deleted**.

- No residual access to the cloud service **shall remain** after decommissioning is complete.

- Access decommissioning activities **shall be documented** and verified by the Information Security Team.

15.6 Asset Recovery and Configuration Preservation

- All cloud configurations, templates, IaC artifacts, scripts, container images, VM images, and infrastructure diagrams **shall be exported and archived** before termination.

- Logs, audit trails, and system events **shall be collected and preserved** for compliance and forensic needs.

- Keys, certificates, and security configurations **shall be securely rotated or deactivated** once no longer required.

- Service-specific operational playbooks **shall be updated** to reflect any changes caused by the exit.

15.7 Log, Evidence, and Artifact Retention

- Logs associated with the cloud service **shall be retained** according to the organization's Logging & Monitoring Policy and legal requirements.

- Evidence related to data extraction, deletion, and configuration shutdown **shall be archived**.

- Retained logs **shall be protected from unauthorized access** and must be stored in approved secure locations.

- Any artifact required for future audits or investigations **shall be preserved** for the mandated retention duration.

15.8 Validation and Assurance Before Final Exit

- The Information Security Team **shall verify** that:
    - All data has been extracted successfully
    - All cloud resources, services, and accounts have been decommissioned
    - All provider-held data has been deleted

    - No security controls, logs, or identities remain active

- A formal validation checklist **shall be completed** and approved prior to closing the exit activity.

- Final sign-off **shall be obtained** from the business owner, IT Owner, and the CISO.

15.9 Vendor Responsibilities During Exit

- Vendors **shall cooperate fully** with exit activities, including data extraction, deletion, and configuration review.

- Vendors **shall not impose unreasonable delays, proprietary barriers, or fees** that hinder data migration or termination.

- Vendor non-compliance with exit obligations **shall be escalated** to Legal, Information Security, and senior management.

- Vendors **shall support post-termination inquiries** where required for compliance or investigation purposes.

15.10 Prohibited Exit-related Practices

- Cloud service termination **shall not occur without a validated and approved exit plan**.

- Data shall not be migrated or deleted **without proper authorization** and verification.

- Unverified or incomplete data deletion **shall be prohibited**.

- Retaining provider access beyond contract termination **shall be strictly prohibited**.

- Termination steps **shall not be skipped or accelerated** without completing formal validation.

16. CLOUD SECURITY VIOLATIONS & ENFORCEMENT

[ORG NAME] shall strictly enforce this Cloud Security Policy. Any violation, deviation, or unauthorized activity related to cloud environments, data, or access shall be treated as a security breach and subject to disciplinary action, investigation, and corrective measures.

16.1 Definition of Cloud Security Violations

- Any unauthorized creation, modification, or deletion of cloud resources **shall be considered a violation**.
- Bypassing or disabling required cloud security controls (MFA, logging, encryption, monitoring) **shall constitute a violation**.
- Storing data in unapproved cloud services or regions **shall be treated as a data handling violation**.
- Unauthorized public exposure of cloud resources, APIs, or storage **shall be treated as a major security incident**.
- Misconfigurations leading to security risks (e.g., open security groups, public buckets) **shall be treated as non-compliance**.
- Unauthorized vendor or third-party integration with cloud systems **shall be treated as a policy breach**.
- Using personal cloud accounts to store, process, or transmit organizational data **shall be strictly prohibited**.
- Attempting to conceal or alter cloud logs, alerts, or evidence **shall be treated as a severe violation**.

16.2 Reporting Cloud Security Violations

- All suspected or confirmed violations **shall be reported immediately** to the Information Security Team or the Incident Handling Team.
- Employees and contractors **shall not attempt to investigate or fix violations themselves** unless authorized.
- Reports may be submitted via service desk, hotline, or direct escalation channels defined in the Incident Management Policy.
- Failure to report known violations **shall itself be considered a violation**.

16.3 Investigation and Assessment

- The Information Security Team **shall initiate an investigation** promptly upon receiving a violation report.

- Investigations **shall include evidence collection**, log review, configuration analysis, and interviews where required.
- Violations **shall be classified by severity**, based on potential impact, data exposure, and risk to the organization.
- High-severity violations **shall be escalated** to the CISO and senior management.
- Investigations **shall be documented**, including findings, root cause, and remediation recommendations.

16.4 Disciplinary Actions

Depending on severity and intent, disciplinary actions **may include**, but are not limited to:

- Formal warning or written reprimand
- Temporary or permanent loss of cloud access privileges
- Suspension of system or administrative rights
- Mandatory security awareness or corrective training
- Revocation of project responsibilities or reassignment
- Termination of employment or contract
- Legal action or regulatory reporting when required

Disciplinary actions **shall comply with HR policies, employment contracts, and legal frameworks**.

16.5 Remediation and Corrective Actions

- All violations **shall require a corrective action plan (CAPA)** with defined responsibilities and timelines.
- Technical remediation (e.g., closing open ports, restoring logging, re-enabling encryption) **shall be completed immediately** based on risk.
- Long-term corrective actions **may include process changes**, improved controls, automation, or re-training.

- The Information Security Team **shall verify remediation** and close the violation only after full compliance is restored.

16.6 Repeat or Systemic Violations

- Repeat offenders **shall face escalated disciplinary actions**, potentially including termination.
- Systemic issues identified through repeated violations **shall trigger process reviews** and security architecture re-evaluation.
- Patterns of violations **shall be reported to senior management and governance committees**.

16.7 Vendor & Third-Party Violations

- Vendors or third parties violating cloud security requirements **shall be subject to contractual penalties**, access revocation, or service termination.
- Security breaches involving vendors **shall be escalated immediately**, and the vendor shall be required to provide incident reports and remediation.
- Third-party violations **may result in blocking vendor access**, suspension of integrations, or legal action.

16.8 Enforcement Authority

- The CISO, Information Security Team, and senior management **retain authority to enforce this policy** across all cloud environments.
- Enforcement decisions **shall be fair, consistent, and proportionate** to the severity of the violation.
- HR, Legal, IT, and Business Owners **shall collaborate** during enforcement actions as required.

17.POLICY EXCEPTIONS

[ORG NAME] recognizes that exceptional circumstances may require temporary deviations from this Cloud Security Policy. All exceptions must follow a formal approval workflow, be time-bound, and include appropriate compensating controls to minimize risk.

17.1 Requesting an Exception

- Any request for deviation from this policy **shall be formally submitted** using the standard IT/Security Exception Request Form.
- Exception requests **shall include clear justification**, scope, risk assessment, impacted systems, compensating controls, and proposed duration.
- Verbal or informal exception requests **shall not be accepted** under any circumstances.

17.2 Review and Evaluation

- All exception requests **shall undergo a security review** conducted by the Information Security Team.
- The review **shall assess the security, operational, and compliance risks** associated with the requested deviation.
- The Information Security Team **may request additional information**, impose conditions, or recommend denial of the request.
- Exceptions that introduce unacceptable risk **shall not be approved**.

17.3 Exception Approval Workflow

All exceptions shall follow the approval hierarchy listed below (consistent with your other MOS policies):

1. **First Level – Unit Manager / Business Owner**
    - Reviews business necessity and validates justification.
2. **Second Level – Information Security Officer / Cloud Security Architect**
    - Reviews technical impact, risks, and compensating controls.
3. **Third Level – Chief Information Security Officer (CISO)**
    - Provides final approval or rejection of the exception.
    - High-risk exceptions require CISO's explicit written approval.

17.4 Validity Period and Renewal

- Approved exceptions **shall be valid only for the duration explicitly stated** in the approval (maximum 90 days unless otherwise approved).
- Expired exceptions **shall not be extended automatically** and must undergo full re-evaluation.
- Renewal requests **shall be treated as new exceptions**, requiring a fresh justification and risk review.

17.5 Compensating Controls

- All approved exceptions **shall require compensating controls** to minimize associated risks.
- Compensating controls **shall be documented** and validated prior to exception activation.
- If compensating controls cannot be implemented, the exception **shall be rejected**.

17.6 Documentation and Record Keeping

- All approved and rejected exceptions **shall be documented**, including:
    - Request details
    - Approval chain
    - Compensating controls
    - Expiration date
    - Risk assessment summary
- Exception records **shall be retained** as per the organization's retention requirements and made available for audits.

17.7 Monitoring and Compliance

- Approved exceptions **shall be continuously monitored** by the Information Security Team for compliance with compensating controls.

- If an exception leads to a security incident or repeated violations, **it may be revoked immediately**.
- Exceptions not adhering to defined conditions **shall be treated as policy violations**.

17.8 Prohibited Practices

- Exceptions **shall not be used** to bypass critical controls such as:
    - Encryption
    - MFA
    - Logging and monitoring
    - Access control
    - Data deletion requirements
- Temporary or emergency exceptions **shall not become permanent** without CISO review and formal approval.

18. ESCALATION MATRIX

In case of access management-related issues, violations, or delays in provisioning/de-provisioning, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Escalation Level	Role/Designation	Responsibility	Contact Mode
Level 1	Reporting Manager / Team Lead	First-level resolution and access validation	Email / Ticketing Tool
Level 2	System/Application Owner	Review of access alignment with business roles	Email / Phone
Level 3	IT Operations Manager	Resolution of system-level or technical delays	Internal escalation call
Level 4	Information Security Officer (ISO)	Security assurance and compliance validation	Email / Escalation Tool
Level 5	Chief Information Security Officer	Final authority on policy enforcement and risk mitigation	Direct escalation via email / formal report

- Escalations must be documented through the ITSM tool or equivalent service desk system.
- Each escalation must include clear description of the issue, impacted users/systems, time of initial request, and business impact.
- SLAs for resolution based on priority level shall be defined and tracked by the IT Service Management function.

19. POLICY REVIEW AND MAINTENANCE

To ensure continued relevance, accuracy, and compliance with evolving legal, regulatory, and operational requirements, this policy will be reviewed and updated on a defined schedule or as required by significant changes in the business environment.

13.1 Review Frequency

- This policy shall be formally reviewed **at least once every 12 months**
- Additional reviews may be initiated based on:
    - New regulatory or contractual requirements (e.g., updates to ISO 27001, DPDP Act, GDPR)
    - Major changes to IT systems, data flows, or organizational structure
    - Results of internal or external audits
    - Security incidents or classification breaches

13.2 Review and Update Responsibilities

Role	Responsibility
Policy Owner (CISO)	Owns the policy, coordinates the review process, and initiates updates
Privacy Officer / DPO	Ensures the policy aligns with data protection laws and retention obligations
Legal & Compliance	Validates alignment with legal holds, retention rules, and regulatory changes
IT / Data Stewards	Provide input on system capabilities, automation feasibility, and enforcement mechanisms

13.3 Version Control and Documentation

- Every change to this policy will be assigned a **version number**, **approval date**, and **summary of changes**
- The most recent version will be published on [ORG NAME]'s internal policy portal or document repository
- Archived versions will be retained for a minimum of **3 years** for audit purposes

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO