ISO 27001:2022

ACCESS MANAGEMENT POLICY

INLINE WITH ISO 27001:2022 & SOC 2 TYPE 2

PREPARED BY :

MINISTRY OF MOS SECURITY

Document Name	**Access Management Policy**
Classification	**Internal Use Only**

Document Management Information

Document Title:	Access Management Policy
Document Number:	ORGANISATION-ACS-MNM-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	Access Management Policy
Classification	Internal Use Only

CONTENTS

1. PURPOSE 4
2. SCOPE 4
3. TERMS AND DEFINITIONS 4
4. ROLES AND RESPONSIBILITIES 4
5. ACCESS CONTROL PRINCIPLES 5
6. USER ACCESS MANAGEMENT 6
7. PRIVILEGED ACCESS MANAGEMENT 7
8. REMOTE AND THIRD-PARTY ACCESS 9
9. AUTHENTICATION AND PASSWORD MANAGEMENT 10
10. ACCESS MONITORING AND REVIEW 12
11. ENFORCEMENT 13
12. POLICY EXCEPTIONS 14
13. ESCALATION MATRIX 16

Document Name	Access Management Policy
Classification	Internal Use Only

1. PURPOSE

The purpose of this policy is to establish standardized access control requirements for all information systems, networks, and data assets owned or managed by [ORG NAME]. This policy ensures that access to these resources is granted only on the basis of legitimate business requirements and in a manner that upholds the confidentiality, integrity, and availability of organizational information, in alignment with ISO/IEC 27001 and SOC 2 Type 2 requirements.

2. SCOPE

This policy applies to all employees, contractors, consultants, interns, vendors, and third-party users who are granted access to [ORG NAME]'s information systems and data. The scope includes all forms of access—local, remote, administrative, and third party—whether through on-premises infrastructure, cloud environments, or integrated external systems.

3. TERMS AND DEFINITIONS

- **Access Control**: The selective restriction of access to information or systems based on predefined rules and criteria.
- **Authentication**: A process used to confirm the identity of a user or system prior to granting access.
- **Authorization**: The process of validating whether an authenticated user is permitted to perform an action or access specific data.
- **Least Privilege**: The practice of limiting access rights to the minimum necessary to perform job functions.
- **Need-to-Know**: Access is restricted to only those resources necessary for a user to perform their specific duties.
- **Privileged Access**: Elevated permissions typically granted to administrators or technical support personnel for managing systems.
- **De-Provisioning**: The revocation of access rights when no longer required due to role change, termination, or other status change.

4. ROLES AND RESPONSIBILITIES

Role	Responsibility
Chief Information Security Officer (CISO)	Policy ownership, approval of privileged access, and exception management.
Information Security Team	Oversight, monitoring, and compliance enforcement. Conducts periodic audits and access reviews.

IT Operations Team	Executes provisioning and de-provisioning activities. Maintains identity and access management tools.
Line Managers	Initiates access requests based on job responsibilities. Validates business need.
HR Department	Coordinates with IT to initiate and terminate user access during onboarding/offboarding.
System Owners	Defines system-specific access roles and participates in periodic reviews.

5. ACCESS CONTROL PRINCIPLES

1. All access granted to users shall be based on the need-to-know, need-to-have, and least privilege principles. Access must only be provided to information and assets that are required for the user to perform their defined roles and responsibilities.
2. A unique user ID shall be assigned to each individual requiring access to the organization's systems, networks, or information assets. This unique ID must be directly linked to the individual and their job function to ensure accountability and traceability of actions.
3. Use of shared user accounts shall be strictly prohibited and restricted to the maximum extent possible. In exceptional circumstances where technical or operational limitations necessitate shared access:
    - A formal justification must be documented.
    - Approvals must be obtained from both the Application Owner/Asset Owner and the CISO.
    - Shared account usage must be tightly controlled, time-bound, and monitored.
4. Access to information systems and resources shall be governed by Role-Based Access Control (RBAC) mechanisms, wherein users are mapped to roles and assigned access privileges aligned to those roles. Roles shall be reviewed periodically.
5. Access rights shall be designed and reviewed to ensure segregation of duties. No individual shall have access to execute conflicting functions unless explicitly approved and mitigated through compensating controls.

6. USER ACCESS MANAGEMENT

1. User Registration and Unique Identification

- All users shall be uniquely identified using a centrally managed identity system before any access is granted.
- A unique user ID shall be assigned to each individual and must be linked to their specific job responsibilities to ensure accountability and traceability.
- Group or generic accounts are prohibited unless explicitly approved and justified in accordance with the Shared Account Usage policy.

2. Access Request and Approval Workflow

- Access requests must be formally initiated by the user's Reporting Manager through a designated Access Request Form or ticketing system.
- All requests must include:
  - Justification of business need
  - Role/function the user is performing
  - Duration of access, if temporary
- The request shall be approved by both the Line Manager and the Application/System Owner. No access will be granted without documented approval.

3. Access Provisioning

- Upon receiving all necessary approvals, the IT Operations team shall provision access based on the role-based access matrix (RBAC).
- Provisioning must be logged with details such as requestor, approver, access granted, and time/date of provisioning.
- Temporary access should be clearly marked and configured with automated expiry dates.

4. Access De-Provisioning

- The HR department and Line Managers must notify IT Operations immediately upon employee resignation, termination, role change, or internal transfer.
- De-provisioning must occur within 24 hours of the triggering event.
- Residual user accounts and credentials must be permanently removed within 5 business days unless an extension is formally approved.
- All de-provisioning actions must be recorded in the De-Provisioning Register.

5. **Access Review and Recertification**
    - System Owners shall perform formal access reviews:
        - Quarterly for critical systems and privileged accounts
        - Semi-annually for general business systems
    - Review must validate whether current access aligns with role requirements.
    - Any access found to be excessive or obsolete shall be revoked within 7 working days.
    - Results of the review must be documented and retained for at least 12 months.
6. **Temporary and Emergency Access**
    - Requests for temporary access must follow the standard approval process and specify a start and end date.
    - Emergency or break-glass access shall only be granted in critical scenarios, with prior CISO approval and continuous monitoring.
    - All emergency access activity must be logged and subject to post-event review within 48 hours.
7. **Dormant Account Management**
    - User accounts that remain unused for 30 consecutive days shall be automatically disabled by the IAM system.
    - Accounts inactive for more than 90 days shall be permanently deactivated and archived in accordance with the Retention Policy.
    - The IT Operations team must review dormant accounts monthly and take appropriate cleanup actions.

7. PRIVILEGED ACCESS MANAGEMENT

1. **Definition and Scope**

    Privileged access refers to elevated system or application-level permissions that allow users to perform administrative tasks, configure security controls, access sensitive information, or override standard system restrictions. This includes, but is not limited to, domain admins, system administrators, database administrators, and superuser roles.

2. **Eligibility and Business Justification**
    - Privileged access shall be granted only to users with job responsibilities that explicitly require such elevated rights.

- Every request must be accompanied by a documented business justification and reviewed by the Application/System Owner.
- Final approval must be obtained from the Chief Information Security Officer (CISO).

3. Approval and Access Provisioning

- All privileged access requests must follow a formal approval workflow via the designated access management system.
- Privileged accounts shall be provisioned with the minimum necessary access to perform required tasks and shall, wherever possible, be time-bound and task-specific.

4. Multi-Factor Authentication (MFA)

- All privileged accounts must be protected using MFA irrespective of the access method (local or remote).
- MFA mechanisms must comply with the organization's Authentication and Password Management Policy.

5. Privileged Session Monitoring

- Activities performed through privileged accounts must be fully logged, monitored, and reviewed on a monthly basis by the Information Security Team.
- Session recordings or audit trails must be enabled for systems where technical feasibility exists.
- Any anomalies or policy violations must be reported as security incidents.

6. Review and Certification

- Privileged access rights shall be reviewed monthly by System Owners in collaboration with the Information Security Team.
- Any unauthorized or redundant access must be revoked within 48 hours and documented as part of the access review process.

7. Service and Non-Human Accounts

- Service accounts with elevated privileges must be uniquely identified, have strong credentials, and be monitored for misuse.
- Use of service accounts for interactive login is prohibited unless explicitly approved and time-boxed.

8. Privileged Access Revocation

- Privileged access must be revoked immediately upon role change, transfer, or termination.

- Emergency removal procedures must be in place for revoking access in critical incidents.
- De-provisioning activities shall be logged and subject to periodic audit.

8. REMOTE AND THIRD-PARTY ACCESS

1. Remote Access Requirements

- Remote access to [ORG NAME] systems shall only be permitted through secure, organization-approved Virtual Private Network (VPN) solutions.
- Multi-Factor Authentication (MFA) is mandatory for all remote users, including internal staff and third parties.
- Remote access requests must undergo documented risk assessment and be approved by the respective Application Owner and the CISO.
- Access must be time-bound, and restricted to specific systems relevant to the user's role or engagement.

2. Endpoint Security and Compliance

- Devices used for remote access must meet corporate endpoint security requirements including up-to-date antivirus, disk encryption, and firewall controls.
- The use of personal devices (BYOD) must comply with the organization's BYOD Policy and must be explicitly authorized.

3. Third-Party Access Controls

- All third-party access (e.g., vendors, partners, consultants) must be governed by signed contractual agreements including confidentiality and acceptable use clauses.
- Access must be granted using named individual accounts, never shared credentials.
- Duration of access must be aligned with contract timelines or project delivery milestones and must be automatically revoked upon expiration.

4. Monitoring and Logging of Third-Party Access

- All remote and third-party sessions must be logged and subject to real-time monitoring for abnormal activity.
- Screen recordings or privileged session monitoring should be enabled where technically feasible for high-risk systems.
- Logs must be reviewed by the Information Security Team for policy compliance and potential misuse.

5. Third-Party Exit and Deprovisioning

- Upon project completion, contract expiry, or disengagement, all third-party access must be revoked within 24 hours.
- A formal exit checklist must be executed including account deactivation, return of assets (if applicable), and data handover.

6. Periodic Review

- All remote and third-party access must be reviewed monthly by the System Owner to verify continued need and appropriateness of access.
- Any access found to be redundant, inactive, or excessive must be removed immediately and documented.

9. AUTHENTICATION AND PASSWORD MANAGEMENT

1. Password Policy Enforcement

- All users must comply with the organization's Password Management Policy.
- Passwords must meet the following minimum complexity requirements:
  - Minimum of 12 characters in length
  - Must include uppercase, lowercase, numeric, and special characters
  - Must not be easily guessable (e.g., no reuse of username, DOB, common words)
  - Password history must be enforced to prevent reuse of the last 6 passwords
- Passwords must be changed at least once every 90 days or immediately if compromised.

2. Multi-Factor Authentication (MFA)

- MFA is mandatory for:
  - All privileged accounts
  - Remote access users
  - Users accessing sensitive or regulated systems
- MFA implementation must use two or more independent factors (e.g., password + token or biometric).

3. Temporary and Initial Passwords

- Default or temporary passwords must be system-generated and meet password complexity standards.
- These passwords must be changed upon the first login.

- Temporary credentials should have an expiry not exceeding 48 hours unless extended with approval.

4. Credential Confidentiality and Handling

- Users must not disclose passwords or store them in insecure mediums (e.g., documents, sticky notes).
- Credential sharing, password embedding in scripts, or use of hardcoded credentials is strictly prohibited.
- Where credential storage is necessary (e.g., for automated jobs), an approved secure credential vault must be used.

5. Service Account Password Management

- Service account credentials must:
  - Be strong and meet complexity requirements
  - Be rotated at least every 90 days
  - Be restricted in scope and non-interactive unless explicitly authorized
- All service account usage must be logged and monitored for misuse or anomalies.

6. Account Lockout and Alerting

- User accounts shall be locked after 5 consecutive failed login attempts.
- Lockout shall be either time-based or require helpdesk intervention.
- Repeated or distributed authentication failures shall trigger automated alerts to the Information Security Team.

7. Authentication Logging and Auditing

- All authentication attempts (successful and failed) must be logged.
- Logs must include user ID, timestamp, source IP, and system accessed.
- Authentication logs shall be retained for a minimum of 12 months for auditing and forensic purposes.

8. Review and Compliance

- The Information Security Team shall perform periodic reviews to ensure compliance with this policy.
- Any deviations or violations shall be addressed under the Enforcement section of this document.

10. ACCESS MONITORING AND REVIEW

1. Logging of Access Events

- All access to critical systems, sensitive applications, and high-risk data repositories must be logged in real time.
- Logs must include key details such as user ID, timestamp, source IP address, authentication status, accessed resources, and action performed (e.g., read, write, delete).
- Logging must capture both successful and failed access attempts.

2. Centralized Log Aggregation

- All access logs must be collected in a centralized Security Information and Event Management (SIEM) platform.
- The SIEM system shall be configured to perform correlation, alerting, and anomaly detection for access-related activities.
- Logs must be protected from unauthorized modification and be retained for a minimum of 12 months.

3. Real-Time Alerts and Monitoring

- Alerts must be generated for abnormal access activities, including but not limited to:
  - Privileged access outside approved business hours
  - Repeated failed login attempts
  - Access from unrecognized or blacklisted IP addresses
  - Concurrent logins from geographically inconsistent locations
- The Information Security Team shall monitor these alerts and initiate incident response procedures as necessary.

4. Periodic Access Reviews

- Access rights for all users must be reviewed on a quarterly basis for critical systems and semi-annually for non-critical systems.
- Access reviews must be performed by the System/Application Owners in coordination with the Information Security Team.
- All deviations, excess privileges, or orphaned accounts identified during the review must be remediated within 7 working days.

5. Dormant and Orphaned Account Management

- Dormant accounts (inactive for 30+ days) must be flagged and reviewed weekly.

- Orphaned accounts (accounts without active owners) must be disabled immediately and investigated by IT Operations.
- Automated controls must be implemented where feasible to disable dormant or orphaned accounts.

6. Audit Readiness and Record Retention

- All access logs, review certifications, and remediation actions must be stored securely and made available during internal or external audits.
- Access-related evidentiary records must be retained in compliance with the organization's data retention policy and applicable regulatory requirements.

11. ENFORCEMENT

1. Policy Compliance

- All users, contractors, and third parties with access to [ORG NAME]'s systems and data are required to adhere strictly to this Access Management Policy.
- Any deviation, negligence, or unauthorized behavior related to access controls shall be treated as a policy violation.

2. Violation Categories and Examples

- Violations include, but are not limited to:
  - Sharing or disclosing user credentials
  - Unauthorized access to systems or data
  - Failure to remove access during offboarding
  - Use of shared accounts without approval
  - Misuse of privileged access

3. Disciplinary Actions

- Depending on the severity, intent, and impact of the violation, disciplinary actions may include:
  - Verbal or written warning
  - Suspension of access rights
  - Formal HR disciplinary procedures
  - Termination of employment or contract
  - Legal action under applicable laws and regulations

4. Incident Management and Reporting

- All suspected or actual access violations must be reported immediately to the Information Security Team or Security & Compliance Office.
- The incident must be documented and managed as per the organization's Incident Management Policy.

5. Corrective and Preventive Actions (CAPA)

- Upon conclusion of an investigation, appropriate CAPA measures shall be taken to mitigate recurrence.
- These may include additional training, technical controls, updates to workflows, or enhanced monitoring.

6. Appeals and Review Process

- Individuals subject to disciplinary actions may appeal in writing to the CISO or the designated Appeals Review Committee within 5 working days of notice.
- The outcome of the appeal process shall be final and documented.

7. Retention of Records

- All enforcement records including investigation reports, logs, evidence, and communication must be retained securely for a minimum of 24 months, or longer if mandated by regulatory or legal requirements.

12. POLICY EXCEPTIONS

1. Request for Exception

- Any deviation from the defined standards in this Access Management Policy must be requested formally using the IT Policy Exception Request Form.
- Requests must contain:
  - Business justification and scope of the exception
  - Duration for which the exception is needed
  - Risk assessment and impact analysis
  - Any proposed compensating controls

2. Approval Workflow

- All exception requests must follow a structured multi-level approval process:

Level	Approver
Level 1	Department Head / Business Unit Owner

Level 2	Application/System Owner
Level 3	Information Security Officer (ISO)
Level 4	Chief Information Security Officer (CISO)

- The CISO holds final authority to approve, deny, or revoke an exception.

3. Documentation and Register Maintenance

- Approved exceptions must be recorded in the Exception Register maintained by the Security & Compliance Office.
- Each entry must include requester details, approval chain, expiry date, and applicable controls.

4. Time Bound Validity and Review

- Exceptions must be time-bound and reviewed periodically.
- Default maximum validity shall not exceed 90 days unless formally extended and reapproved.
- Active exceptions shall be reviewed monthly to ensure continued relevance and risk containment.

5. Compensating Controls

- If an exception introduces additional risk, mitigating or compensating controls must be enforced. Examples include:
  - Enhanced logging and monitoring
  - Restricting access scope or duration
  - Additional user validation or supervision

6. Revocation and Audit

- The CISO reserves the right to revoke an exception if:
  - The associated risk becomes unacceptable
  - The business justification no longer applies
  - Evidence of misuse or policy breach is found
- All exceptions shall be subject to review during internal and external audits.
- Non-compliance with the approved terms of the exception may lead to enforcement actions as defined in Section 11.

13. 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.

ISO 27001:2022

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

MINISTRY OF MOS SECURITY

WWW.MINISTRYOFSECURITY.CO