

**Access Management Policy**

**Document Statistics**

|  |  |
| --- | --- |
| **Type Of Information** | **Document Data** |
| Document Title | Access Management Policy |
| Document Code | PO/AMP/V02 |
| Date of Release | 27th Dec 2023 |
| Document Revision No | 2nd release of document |
| Document Owner | IT Executive |
| Documents Author(s) | IT Head |
| Document Change Reviewer | IT Head |
| Security Classification | Confidential |
| Document Status | Approved |

**Document approvers.**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Approver** | **Approver Contact(Email)** |
| 1 | Vice President Strategy & BIS | Rashmin Vyawahare <r.vyawahare@cloudextel.com> |

**Document Change Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Revision Date** | **Nature of Change** | **Date Approved** |
| 1 | 26th July 2022 | Initial Release | 28th July 2022 |
| 2 | 25th Dec 2023 | Revised Release | 27th Dec 2023 |

**Document Contact Point**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Document/Process** | **Document Author** | **Document Primary Focal Point** |
| 1 | Access Management Policy | IT Head | IT Policies Folder |

**Document Reference List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No** | **Reference No.** | **Document Name** | **Effective date** |
| 1 | PO/AMP/V01 | Access Management Policy\_Ver.1 | 29th July 2022 |
| 2 | PO/AMP/V02 | Access Management Policy\_Ver.2 | 27th Dec 2023 |

Contents

[1. Policy Statement 5](#_Toc163744863)

[2. Objectives 5](#_Toc163744864)

[3. Scope 5](#_Toc163744865)

[4. Access Control Principles 5](#_Toc163744866)

[4.1 Least Privilege 5](#_Toc163744867)

[4.2 Need-to-Know 5](#_Toc163744868)

[4.3 Separation of Duties 5](#_Toc163744869)

[5. User Authentication 5](#_Toc163744870)

[5.1 Password Policies 5](#_Toc163744871)

[5.2 Role-Based Access Control (RBAC) 5](#_Toc163744872)

[5.3 Attribute-Based Access Control (ABAC) 5](#_Toc163744873)

[6. Access Request and Approval Process 5](#_Toc163744874)

[7. Monitoring and Auditing 5](#_Toc163744875)

[8. Account Management 5](#_Toc163744876)

[9. Incident Response 6](#_Toc163744877)

[10. Compliance 6](#_Toc163744878)

[11. Training and Awareness 6](#_Toc163744879)

[12. Documentation 6](#_Toc163744880)

[13. Responsibilities 6](#_Toc163744881)

[14. Review and Revision 6](#_Toc163744882)

[15. Enforcement 6](#_Toc163744883)

# 1. Policy Statement

This Access Management Policy outlines the principles, procedures, and guidelines for controlling access to the organization's information systems, data, and resources.

# 2. Objectives

The primary objectives of this policy are:

• Ensure the confidentiality, integrity, and availability of organizational information.

• Implement the principle of least privilege.

• Facilitate compliance with applicable laws, regulations, and industry standards.

• Enable efficient and secure user access to resources based on job responsibilities.

# 3. Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals or entities with access to the organization's information systems.

# 4. Access Control Principles

## 4.1 Least Privilege

Access will be granted based on the principle of least privilege, providing users with the minimum level of access necessary for their job functions.

## 4.2 Need-to-Know

Access to information will be granted only to individuals who have a legitimate need-to-know for their job responsibilities.

## 4.3 Separation of Duties

Critical functions will be divided among multiple individuals to prevent unauthorized access and misuse.

# 5. User Authentication

## 5.1 Password Policies

• Users must create strong passwords following established guidelines.

• Passwords must be changed regularly.

• Multi-factor authentication (MFA) is mandatory for accessing sensitive systems.

## 5.2 Role-Based Access Control (RBAC)

Access permissions will be assigned based on predefined roles, reflecting job responsibilities.

## 5.3 Attribute-Based Access Control (ABAC)

Access decisions will take into account user attributes, resource attributes, and environmental factors.

# 6. Access Request and Approval Process

• Users must submit access requests through the designated system.

• Access requests will undergo an approval workflow.

• Managers or designated approvers will review and authorize access requests.

# 7. Monitoring and Auditing

• Logging of user activities and access attempts will be implemented.

• Regular audits of access logs will be conducted to identify and respond to suspicious activities.

# 8. Account Management

• Procedures for creating, modifying, and deactivating user accounts will be documented.

• Regular reviews of user accounts will be conducted to ensure alignment with business needs.

# 9. Incident Response

• Incident response procedures will be in place to address unauthorized access or security incidents promptly.

# 10. Compliance

• The access management practices will be designed to comply with applicable legal and regulatory requirements.

# 11. Training and Awareness

• User training programs will be conducted during onboarding for new joiners and regularly twice a year to educate employees on security policies and best practices.

# 12. Documentation

• This policy will be documented and regularly reviewed for updates.

# 13. Responsibilities

• Define roles and responsibilities for individuals involved in access management.

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| Access Manager/Coordinator:  Mahesh Addagatla <m.addagatla@cloudextel.com> | * Oversees access management. * Develops policies. * Manages requests and approvals. |
| System Administrators:  Mahesh Addagatla <m.addagatla@cloudextel.com> | * Implements and maintains access controls. * Manages user accounts. * Monitors system access. |
| Data Owners:  Respective Owners | * Identify sensitive data. * Define access requirements. * Approve access requests. |
| End Users:  All Users | * Follow policies. * Submit access requests. * Adhere to security protocols. |

# 14. Review and Revision

• Regularly review and update the Access Management Policy to address changing security threats and business needs.

# 15. Enforcement

• Violations of this policy may result in disciplinary action, including revocation of access privileges, suspension, or termination.