CloudServe Access Control Policy

Effective Date: 9/09/2024
Last Updated: 9/09/2024
Version: 1.0

---

1. Purpose

The purpose of this Access Control Policy is to ensure that only authorized individuals have access to CloudServe's systems, data, and resources. This policy establishes controls for managing user access and maintaining the security, availability, and confidentiality of sensitive information.

---

2. Scope

This policy applies to all CloudServe employees, contractors, and third-party vendors who require access to CloudServe's systems, networks, and data. It covers all systems, including cloud infrastructure, web applications, internal networks, and any storage where sensitive data resides.

---

3. Access Control Principles

CloudServe adopts the following key access control principles:

- **Need to Know**: Access to information is limited to those whose roles require it.
- **Least Privilege**: Users are granted the minimum level of access necessary to perform their job functions.
- **Role-Based Access Control (RBAC)**: Access is assigned based on defined roles to streamline user management.
- **Separation of Duties**: Critical tasks are divided among multiple personnel to reduce the risk of unauthorized actions.

---

4. User Authentication

CloudServe enforces the following user authentication mechanisms:

- **Multi-Factor Authentication (MFA)**: All users must use MFA for accessing critical systems, including the cloud infrastructure and internal networks.
- **Strong Password Policy**:
    - Passwords must be a minimum of 12 characters and include a mix of upper and lower-case letters, numbers, and special characters.
    - Passwords must be changed every 90 days.
    - Password history must prevent the reuse of the last 5 passwords.

---

5. Access Requests and Approval

Access to systems and data must be requested and approved as follows:

- **Access Requests**:
    - Users must submit access requests through the designated internal portal.
    - Each request must include the specific system, the level of access needed, and the business justification.
- **Access Approval**:
    - Access requests must be approved by the user's manager and the IT security team.
    - Any elevated privileges (e.g., admin rights) require additional approval from the department head.

---

6. Access Reviews and Audits

- **Quarterly Access Reviews**: Managers and the IT security team will conduct quarterly reviews of all user accounts to ensure access levels are appropriate and up to date.
- **Termination of Access**: Upon termination or role change, a user's access must be revoked or adjusted immediately.
- **Logging and Monitoring**: All access attempts, successful or failed, must be logged. Logs will be monitored for suspicious activities.

---

7. Privileged Access Management

Special precautions are in place for privileged (administrative) access:

- **Admin Account Restrictions**: Admin accounts must only be used for administrative tasks. Day-to-day operations should be conducted using standard user accounts.
- **Admin Access Logging**: All privileged access and actions taken using admin accounts must be logged and reviewed monthly by the IT security team.

---

8. Remote Access

- **VPN and Encryption**: Remote access to CloudServe's systems must be done through a secure VPN connection, and all communications must be encrypted.
- **Authentication**: MFA is mandatory for all remote connections.

---

9. Third-Party Access

- **Third-Party Contracts**: Third-party vendors must sign security agreements and undergo risk assessments before accessing CloudServe systems.
- **Limited Access**: Vendors are granted temporary, least-privilege access for the duration of their contract.
- **Monitoring**: Vendor activities will be monitored, and access logs will be reviewed regularly.

---

10. Policy Compliance

- **Training**: All employees and third parties with system access must undergo access control training.
- **Non-Compliance**: Violations of this policy may result in disciplinary actions, including termination or legal action.

---

11. Review and Updates

This policy will be reviewed and updated annually or as needed to address changes in security requirements or regulations.

---

12. Contact Information

For questions or further information regarding this Access Control Policy, contact the IT Security Team at CloudserverIT@CS.com.