**Access Control Policy**

**Policy ID:** SEC-ACP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Information Security Officer (CISO)  
**Applies To:** All employees, contractors, vendors, and authorized third-party users

**1. Purpose**

This policy establishes standards for managing user access to [COMPANY NAME] systems and data to prevent unauthorized access, ensure accountability, and protect sensitive information.

**2. Scope**

This policy applies to all information systems, applications, devices, and facilities owned, operated, or managed by [COMPANY NAME] where access control is required. It includes all users with physical or logical access.

**3. Policy Statements**

**3.1 User Access Management**

* Access to systems and data must be granted based on the principle of least privilege and business need. *(NIST AC-6; ISO 27001 A.5.18)*
* All users must have unique credentials; shared or generic accounts are prohibited. *(NIST IA-2; ISO 27001 A.5.18)*
* Access must be formally requested, reviewed, and approved by authorized personnel. *(NIST AC-2; ISO 27001 A.5.15)*
* Access provisioning and deprovisioning must follow documented procedures and occur promptly. *(NIST AC-2, AC-3; ISO 27001 A.5.17)*

**3.2 Authentication and Login Controls**

* Strong authentication controls must be implemented, including complex passwords and Multi-Factor Authentication (MFA) for high-risk access. *(NIST IA-5, IA-7; ISO 27001 A.5.15)*
* Default credentials must be changed before use and never reused across systems. *(NIST CM-6; ISO 27001 A.5.14)*
* Failed login attempts must trigger account lockout after a defined threshold. *(NIST AC-7; ISO 27001 A.5.18)*

**3.3 Privileged Access Management**

* Elevated access (e.g., administrator or root) must be tightly controlled, logged, and used only when necessary. *(NIST AC-5, AU-2; ISO 27001 A.5.19)*
* Privileged account use must be limited to specific tasks and regularly reviewed. *(NIST AC-2, AC-6; ISO 27001 A.5.15)*
* Session logging and monitoring are required for all privileged access activities. *(NIST AU-6; ISO 27001 A.5.20)*

**3.4 Access Review and Recertification**

* All access rights must be reviewed at least quarterly to ensure alignment with job roles. *(NIST AC-2(7); ISO 27001 A.5.15)*
* Access to systems or data must be revoked immediately upon employee termination or role change. *(NIST AC-2(5); ISO 27001 A.5.17)*

**3.5 Physical Access Control**

* Physical access to critical systems or secure areas must be restricted using badge systems, biometrics, or equivalent mechanisms. *(NIST PE-2, PE-3; ISO 27001 A.7.1)*
* Visitor access must be documented, supervised, and limited to authorized areas only. *(NIST PE-8; ISO 27001 A.7.2)*
* Physical access logs must be retained and reviewed periodically. *(NIST PE-6; ISO 27001 A.5.20)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| All Users | Use credentials responsibly, report access issues, and comply with this policy. |
| Managers | Approve access requests and validate user access regularly. |
| IT/Security Team | Implement and monitor access controls; maintain logs and audit trails. |
| HR | Notify IT of changes in employment status for access adjustment. |

**5. Compliance and Enforcement**

Noncompliance may result in disciplinary action, revocation of access privileges, or legal penalties. System access is monitored and audited to ensure adherence to this policy.

**6. Review and Maintenance**

The CISO shall review this policy annually or following any major system, role, or regulatory change. Updates must be approved and distributed accordingly.

**7. Acknowledgment and Agreement**

I acknowledge that I have read, understand, and agree to comply with the Access Control Policy. I understand the importance of securing access to systems and the consequences of policy violations.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Manager/HR (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |