# AethelGuard Solutions

## Access Control Policy v1.0

**1. Context & Objective**
This Access Control Policy ("the Policy") establishes the principles, rules, and responsibilities for managing access to AethelGuard Solutions' information systems, data, and physical assets. The primary objective is to protect the confidentiality, integrity, and availability of all critical resources, ensuring that only authorized individuals and systems have appropriate access. This Policy is a foundational component of AethelGuard Solutions' overall Information Security Management System (ISMS).

**2. Scope**
This Policy applies to all AethelGuard Solutions employees, contractors, third-party vendors, and any external entities requiring access to AethelGuard's IT infrastructure, internal and client-related data, and physical premises. It covers all information systems, applications, data classifications, cloud and on-premise resources, and endpoint devices used within AethelGuard Solutions.

**3. Core Principles**
Access controls within AethelGuard Solutions are governed by the following core principles:

- **Principle of Least Privilege:** Users are granted the minimum level of access permissions necessary to perform their assigned job functions, and no more.
- **Need-to-Know Basis:** Access to sensitive information and systems is restricted to individuals whose legitimate duties require such access.
- **Separation of Duties (SoD):** Critical functions are separated among different individuals to prevent a single person from completing a fraudulent or malicious act without collusion.
- **Defense-in-Depth:** Multiple layers of security controls are implemented to protect assets, ensuring that if one control fails, others remain to provide protection.
- **Accountability:** All access activities are logged and auditable, ensuring that individuals can be held accountable for their actions.

**4. Provisioning & Deprovisioning**
This section outlines the lifecycle management of user access.

- **Access Provisioning:**
    - All access requests must be initiated via a formal request process (e.g., HR request, IT Service Desk ticket) and approved by the appropriate manager/asset owner.
    - Access will be granted based on job role and the Principle of Least Privilege.
    - New user accounts and access permissions must be provisioned within [e.g., 1 business day] of approved requests.
- **Access Review:**
    - User access permissions will be formally reviewed by asset owners/managers at least [e.g., quarterly for privileged accounts, semi-annually for standard accounts] to ensure continued necessity and appropriateness.
- **Access Deprovisioning:**

- Upon employee termination, resignation, or role change, all associated system access must be revoked or adjusted within [e.g., 2 hours for critical systems, 24 hours for all others] of notification from HR.
- Offboarding checklists will be utilized to ensure all access points are addressed.

**5. Authentication & Credentials**

This section defines requirements for verifying user identities.

- **Multi-Factor Authentication (MFA):** MFA is mandatory for all administrative access to critical systems (e.g., cloud platforms, production environments, code repositories), remote access (e.g., VPN, client portals), and privileged internal applications.
- **Password Policy:**
  - Minimum length of [e.g., 14 characters].
  - Must include a combination of uppercase, lowercase, numbers, and special characters.
  - Passwords must not be reused across different systems.
  - Password changes enforced at least every [e.g., 90 days] for administrative accounts.
- **Credential Hygiene:** Users must protect their credentials, avoid sharing, and report any compromise immediately. Service accounts will be managed separately with unique, complex credentials and minimal privileges.

**6. Privileged Access Management (PAM)**

This section outlines the controls for managing highly sensitive accounts.

- **Identification of Privileged Accounts:** All administrative, root, or service accounts with elevated permissions across critical systems (e.g., cloud environments, production servers, network devices, client configuration tools) are designated as privileged.
- **PAM Solution:** A dedicated Privileged Access Management solution [e.g., name a tool if applicable, otherwise state "will be implemented"] will be used to manage, store, and rotate privileged credentials.
- **Session Monitoring & Auditing:** All privileged sessions will be logged, monitored, and regularly reviewed for suspicious activity.
- **Just-In-Time Access (JIT):** Where feasible, privileged access will be granted on a just-in-time basis, limiting its duration and scope to only what is required for specific tasks.

**7. Audit & Compliance**

This section details the logging, monitoring, and review activities related to access controls.

- **Logging Requirements:** All access attempts (successful and failed), privilege changes, and critical system modifications will be logged.
- **Audit Trails:** Audit logs will be securely stored for a minimum of [e.g., 1 year] and protected from unauthorized alteration.
- **Monitoring:** Logs will be continuously monitored for anomalous activity, unauthorized access attempts, and policy violations, integrating with security monitoring systems (SIEM).
- **Compliance Reporting:** Regular reports on access control compliance will be generated for management review.

**8. Governance & Responsibilities**

Clear ownership and accountability are essential for effective access control.

- **Policy Ownership:** The Security Lead is responsible for the overall maintenance and review of this Policy.
- **Control Implementation:** IT Operations and Cloud Operations are responsible for implementing and maintaining technical access controls.
- **Compliance Oversight:** The Compliance team ensures access controls adhere to regulatory requirements and internal policies.
- **User Responsibility:** All users are responsible for adhering to this Policy and protecting their access credentials.

- **Escalation:** Any suspected unauthorized access or policy violation must be reported immediately to the Security Operations Center (SOC) or Security Lead.

**9. Compliance Requirements**

This Policy supports compliance with relevant legal, regulatory, and contractual obligations, including:

- **ISO 27001:** Specifically addressing Annex A.9 (Access Control) requirements.
- **GDPR (General Data Protection Regulation):** Ensuring protection of Personal Identifiable Information (PII) through appropriate access restrictions.
- **Client Contracts:** Adherence to security clauses in service agreements with clients.

**10. Appendices**

- **Related Internal Processes:**
    - Incident Response Plan (for handling unauthorized access incidents)
    - Change Management Policy (for changes to access control systems)
    - Information Classification Policy (for defining data sensitivity and access tiers)
- **Tools Utilized:**
    - Azure AD for IAM
    - CyberArk for PAM
    - Splunk for logging/monitoring