

PURPOSE AND SCOPE

This policy defines the baseline controls that protect the ACME Horizon platform and ACME corporate systems. It applies to all workforce members, contractors, and service providers with access to ACME-managed resources.

PRINCIPLES

- Least privilege for all identities and services
- Defense in depth with layered controls
- Secure by default configurations
- Continuous verification and monitoring

ACCESS CONTROL

- All administrative access requires MFA
- Role-based access aligned to job function
- Service accounts use scoped tokens and short-lived credentials

CRYPTOGRAPHY

- Encryption in transit and at rest using industry-standard protocols
- Managed keys with rotation and strict separation of duties

VULNERABILITY AND PATCH MANAGEMENT

- Track vulnerabilities to remediation and verify closure
- Risk-based prioritization informed by exploitability and exposure

SECURE DEVELOPMENT

- Static and dynamic analysis in CI
- Dependency scanning and signed artifacts
- Threat modeling for changes with material impact

LOGGING AND MONITORING

- Centralized, immutable logs with time synchronization
- Alerting for anomalous access and configuration drift

THIRD-PARTY MANAGEMENT

- Security review for new vendors
- Contractual obligations for data protection and breach notification

DATA CLASSIFICATION

- Public, Internal, Confidential, Restricted

- Controls scale with classification level

EXCEPTIONS AND GOVERNANCE

Exceptions require documented risk acceptance and time-bound remediation plans. Policy governance lives with the security leadership function.