LINKEDIN SERVICES PORTFOLIO / IT & COMPLIANCE DOCUMENTATION

Access Control & Account Security Policy

Example deliverable: an auditable policy framework that requires organization-specific review and approval.

Document control	Details
Document ID	SEC-POL-006
Policy owner	Information Security
Classification	Internal / Demonstration
Review cycle	At least annually or upon material change

1. Policy objective

Protect organizational systems and information through role-based access, individual accountability, appropriate authentication, and timely access reviews. This example describes a fictional midsize professional-services organization.

2. Core requirements

- Identity: Every user receives a uniquely attributable account. Shared interactive accounts are prohibited unless formally excepted and monitored.
- Least privilege: Access is assigned by approved role and limited to documented business needs.
- Multi-factor authentication: MFA is required for remote access, privileged accounts, and supported business-critical applications.
- Account lifecycle: New access requires managerial approval; access changes follow role transitions; access is disabled promptly on separation.
- Privileged access: Administrative permissions are separate from standard user permissions and reviewed more frequently.
- Logging: Security-relevant authentication, administrative actions, and access changes are logged in line with the approved retention schedule.

3. Access request workflow

Step	Required evidence
Request	Business justification, requested system and role, ticket ID.
Approve	Manager and system owner approval; security approval for privileged access.
Provision	IT confirms access matches approvals and records completion.
Review	Owner periodically recertifies access; exceptions are documented.
Revoke	IT records removal at end of business need or separation.

4. Access-review cadence

System owners review privileged access at least quarterly and standard business-system access at least semiannually. Reviews document reviewer identity, date, disposition, and remediation owner.

5. Exceptions and enforcement

Exceptions must be time-limited, risk-assessed, documented, and approved by the policy owner. Violations may result in access suspension or other action consistent with organizational policy.

6. Evidence and control mapping

Evidence artifact	Control intent
Approved access tickets	Authorization and traceability
Role entitlement matrix	Least privilege and separation of duties
MFA configuration exports	Strong authentication
Termination checklist	Timely deprovisioning
Access review attestations	Periodic validation of entitlement

Illustrative policy, not legal advice or a claim of NIST, ISO 27001, SOC 2, or HIPAA compliance. Map to applicable requirements and validate through qualified reviewers.