Service Account Policy

Document ID: IT-ACC-005 **Last Updated:** 2024-01-20 **Owner:** IT Security Team **Classification:** Internal

---

Purpose

This policy governs the creation, management, and security of service accounts at NovaTech. Service accounts are non-human accounts used by applications, scripts, and automated processes.

Definitions

- **Service Account:** A non-interactive account used for automated processes
- **API Key:** A unique identifier for authenticating API requests
- **Service Principal:** An identity for cloud resources (AWS IAM, Azure AD)

Account Naming Convention

Service accounts must follow this naming pattern:

```
svc-<team>-<application>-<environment>
```

Examples: `- svc-platform-deployment-prod - svc-data-etl-staging - svc-security-scanner-dev`

Request Process

Step 1: Submit Request

1. Create ticket in ServiceNow under "Service Account Request"
2. Provide:
    - Account purpose and business justification
    - Required permissions (principle of least privilege)
    - Owner and backup owner
    - Environment (dev/staging/prod)

Step 2: Approval

- Development accounts: Team lead approval
- Staging accounts: Team lead + Security review
- Production accounts: Director + Security review + Change Advisory Board

Step 3: Provisioning

IT Security will provision the account within: - Development: 1 business day - Staging: 2 business days - Production: 5 business days (includes CAB review)

Security Requirements

Password/Secret Management

- Passwords must be at least **32 characters**
- Store secrets in HashiCorp Vault (never in code or config files)
- Rotate secrets every **90 days** (automated via Vault)

Permissions

- Follow principle of least privilege
- Document all permissions granted
- Review permissions quarterly

Monitoring

- All service account activity is logged
- Anomalous activity triggers alerts
- Failed authentication alerts after 3 attempts

Owner Responsibilities

Service account owners must: 1. Maintain accurate documentation 2. Respond to security inquiries within 24 hours 3. Initiate quarterly access reviews 4. Request decommission when account is no longer needed 5. Ensure secrets are properly rotated

---

Lifecycle Management

Quarterly Review

- Owners receive automated review reminders
- Confirm account is still needed
- Verify permissions are appropriate
- Update documentation if changed

Decommissioning

When a service account is no longer needed: 1. Submit decommission request in ServiceNow 2. Revoke all secrets and API keys 3. Remove from all systems 4. Archive audit logs for 7 years

---

Prohibited Actions

- Sharing service account credentials via email or Slack
- Using service accounts for interactive logins
- Granting admin/root access without explicit approval
- Storing credentials in source code repositories

Incident Response

If a service account is compromised: 1. Immediately rotate all associated secrets 2. Report to security@novatech.com 3. Review audit logs for unauthorized activity 4. Complete incident report within 48 hours

---

Compliance

This policy supports compliance with: - SOC 2 Type II - ISO 27001 - GDPR (where applicable)

Exceptions

Exceptions require written approval from the CISO. Submit exception requests to security@novatech.com with business justification.

Related Documents: Password Requirements (IT-ACC-001), Secret Management Guide (IT-SEC-015), Change Management Policy (IT-OPS-003)