Document 2

Southstar Tech Solutions

Access Control Policy

Version: 1.0
Effective Date: January 2026
Owner: IT Operations & Security Team

---

1. Purpose

This policy defines how access to systems, applications, and data is granted, reviewed, and revoked at Southstar Tech Solutions to ensure security and compliance.

---

2. Scope

Applies to:

- All employees, contractors, and vendors
- All company systems, networks, and cloud services

---

3. Access Principles

Southstar Tech follows the principles of:

- Least Privilege — users receive only the access required for their role
- Role-Based Access Control (RBAC)
- Separation of Duties — critical tasks require multiple approvals

---

4. Account Provisioning Process

Step 1: Access Request

- Employee submits request through ServiceNow.

- Must specify system, role, and business justification.

Step 2: Approval

- Direct manager approval required.
- System owner approval required for privileged access.

Step 3: Account Creation

- IT Operations creates account in system.
- Access linked to Okta identity.

Step 4: Notification

- User receives confirmation email with login instructions.

---

5. Privileged Access

Privileged accounts include:

- System administrators
- Database administrators
- Security engineers

Requirements:

- MFA mandatory
- Approval from SOC Manager
- Access reviewed quarterly

---

6. Password Requirements

- Minimum 12 characters
- Combination of upper, lower, numbers, symbols
- Changed every 90 days

- Managed via corporate password manager

---

7. Access Review

- Quarterly access review by managers
- Inactive accounts disabled after 30 days
- Access revoked immediately upon termination

---

8. Emergency Access

Break-glass accounts:

- Stored securely
- Logged and monitored
- Post-use review required

---

9. Compliance Alignment

This policy aligns with:

- NIST Identity & Access Management controls
- ISO 27001 Access Control standards

---

10. Tools Used

Tool	Purpose
Okta	Identity & access management
ServiceNow	Access requests
Splunk	Monitoring login activity

---

11. Review Cycle

Reviewed annually or after major security events.