Password Policy

Document ID: IT-SEC-020 **Effective Date:** January 1, 2024 **Last Updated:** February 2024 **Owner:** Information Security **Applies To:** All Employees, Contractors, Systems

---

Purpose

This policy establishes requirements for creating, managing, and protecting passwords to ensure the security of NovaTech systems and data.

Scope

This policy applies to: - All NovaTech employees and contractors - All systems, applications, and services - All accounts (user, service, admin) - Both NovaTech-managed and third-party systems

---

Password Requirements

Standard User Accounts

Requirement	Value
Minimum length	16 characters
Maximum length	128 characters
Character types	3 of 4: uppercase, lowercase, numbers, symbols
Password history	Cannot reuse last 12 passwords
Maximum age	365 days
Minimum age	1 day

Privileged Accounts

Privileged accounts (admin, root, service) have stricter requirements:

Requirement	Value
Minimum length	20 characters
Character types	All 4: uppercase, lowercase, numbers, symbols
Password history	Cannot reuse last 24 passwords
Maximum age	90 days
Minimum age	1 day

Service Accounts

Requirement	Value
Minimum length	32 characters
Generation	Random (system-generated)
Storage	SecureVault only
Rotation	90 days (automated)

Password Creation Guidelines

Do's

Create strong passwords by: - Using passphrases (e.g., "correct-horse-battery-staple") - Using a password manager to generate passwords - Making passwords memorable but unique - Using different passwords for each account

Example strong passwords: - `MyDog$Loves2RunInThe*Park!` (passphrase) - `j8K#mP2$vL9@nQ4x` (random) - `Coffee-Mountain-Laptop-73!` (random words)

Don'ts

Avoid: - Dictionary words alone (password, admin) - Personal information (birthdate, pet names) - Sequential patterns (12345, abcde) - Keyboard patterns (qwerty, asdfgh) - Previously used passwords - Same password across accounts - Sharing passwords

Weak password examples: - `Password123!` (common pattern) - `NovaTech2024` (company + year) - `John$mith1985` (name + birthyear)

Multi-Factor Authentication (MFA)

Requirements

MFA is **required** for: - All user accounts (no exceptions) - VPN access - Cloud provider consoles (AWS, GCP, Azure) - Production system access - Administrative interfaces - Email access - SecureVault access

Approved MFA Methods

Method	Priority	Use Case
Hardware security key (YubiKey)	Preferred	High-security, phishing-resistant
Authenticator app (Okta Verify)	Standard	Most users
Push notification	Standard	Mobile-enabled users
TOTP (Google Authenticator)	Acceptable	Backup method
SMS	Not allowed	Vulnerable to SIM swapping

Enrolling in MFA

1. Log in to Okta (okta.novatech.com)
2. Go to **Settings → Security Methods**
3. Click **Set up** next to your preferred method
4. Follow enrollment instructions
5. Set up a backup method

Hardware Security Keys

NovaTech provides YubiKey security keys: - Request via IT Service Desk - 2 keys provided (primary + backup) - Register both keys in Okta - Store backup securely

---

Password Storage

Approved Storage

Storage Method	Allowed	Notes
1Password (company-provided)	Yes	Primary password manager
SecureVault	Yes	For service accounts and automation
Okta Secure Notes	Yes	For personal passwords
Brain (memory)	Yes	Limited to a few critical passwords

Prohibited Storage

Storage Method	Allowed	Risk
Plain text files	No	Easily compromised
Spreadsheets	No	No encryption
Email	No	Stored in plaintext
Sticky notes	No	Physically visible
Browser auto-save	No	Less secure than password manager
Shared documents	No	Uncontrolled access

1Password Guidelines

All employees receive 1Password access: - **Personal vault:** Your accounts - **Team vault:** Shared team credentials (limited) - **Emergency kit:** Store securely at home

Setting up 1Password: 1. Install browser extension and desktop app 2. Create master password (follow guidelines above) 3. Save emergency kit PDF 4. Enable biometric unlock (optional)

Password Sharing

Never Share

- Your personal account password
- Your MFA codes (except during enrollment)
- Your master password

Shared Credentials (When Necessary)

Some shared credentials are unavoidable (shared service accounts):

Approved method: 1. Store in SecureVault 2. Use access policies to control who can view 3. Rotate after team changes 4. Audit access regularly

Request access: 1. Submit access request via IT Service Desk 2. Manager approval required 3. Access granted via SecureVault policy

---

Password Reset

Self-Service Reset

For Okta and most integrated apps: 1. Go to okta.novatech.com 2. Click **Forgot Password** 3. Verify identity via email + MFA 4. Create new password 5. Update in password manager

IT-Assisted Reset

If self-service unavailable: 1. Contact IT Service Desk 2. Verify identity (employee ID, manager verification) 3. IT generates temporary password 4. Change password immediately upon login

Compromised Password

If you suspect your password is compromised: 1. **Immediately** change the password 2. Report to security@novatech.com 3. Review account activity 4. IT Security will investigate

---

Account Lockout

Lockout Policy

Threshold	Action
5 failed attempts	Account locked for 15 minutes
10 failed attempts	Account locked for 1 hour
15 failed attempts	Account locked until IT reset

Unlock Procedure

Auto-unlock: Wait for lockout period to expire

Manual unlock: Contact IT Service Desk with: - Your full name - Employee ID - Reason for lockout

---

Privileged Access

Definition

Privileged accounts include: - System administrators - Database administrators - Cloud infrastructure admins - Security team accounts - Break-glass/emergency accounts

Additional Requirements

1. **Separate accounts:** Use privileged account only for admin tasks
2. **Just-in-time access:** Request access when needed, auto-revoke
3. **Session recording:** Admin sessions may be recorded
4. **Enhanced monitoring:** All privileged actions logged
5. **Regular review:** Quarterly access review

Break-Glass Accounts

Emergency access accounts for outage recovery: - Stored in secure physical location - Password in sealed envelope - Requires 2-person access - All usage triggers immediate alert - Post-incident password rotation required

---

Compliance

Monitoring

Security team monitors for: - Weak passwords (via controlled assessment) - Password reuse across accounts - Failed login attempts - Unusual access patterns

Enforcement

Violation	First Offense	Repeat
Weak password	Forced reset	Training
Shared password	Warning + reset	Disciplinary
Stored insecurely	Warning + training	Disciplinary
Compromised password (negligence)	Training	Disciplinary

Exceptions

Exceptions to this policy require: 1. Written request to security@novatech.com 2. Business justification 3. Risk assessment 4. CISO approval 5. Documented compensating controls 6. Time-limited exception

---

Special Systems

Legacy Systems

Some legacy systems have limitations: - Document in exception register - Implement compensating controls - Plan for upgrade/replacement

Third-Party Systems

For systems not supporting our password requirements: - Use maximum allowed length and complexity - Enable MFA if available - Document in risk register

---

Training

Required Training

All employees must complete: - Password security awareness (onboarding) - Annual security refresher - Phishing awareness training

Resources

- Security awareness portal: security.novatech.com/training
- Password manager guide: docs.novatech.com/1password
- MFA enrollment: docs.novatech.com/mfa

Incident Response

Report Security Incidents

Report to security@novatech.com: - Suspected password compromise - Phishing attempts - Unauthorized access attempts - Lost MFA devices

Response Process

1. Immediate password reset
2. Session termination
3. MFA re-enrollment if needed
4. Investigation
5. Follow-up actions

Policy Review

This policy is reviewed: - Annually (minimum) - After security incidents - When industry standards change - When technology changes

---

Questions

- **Policy questions:** security@novatech.com
- **Technical help:** IT Service Desk
- **Password manager:** 1password@novatech.com

Related Documents: Security Best Practices (IT-SEC-001), Acceptable Use Policy (IT-SEC-015), MFA Guide (IT-SEC-025)