Password Requirements

Document Number: IT-ACC-006 **Effective Date:** January 1, 2020 **Last Updated:** June 1, 2023 **Owner:** IT Security **Applies To:** All employees, contractors, and system users

Overview

Strong passwords are essential for protecting NovaTech systems and data. This document outlines password requirements for all company accounts.

Password Standards

Minimum Requirements

Requirement	Standard
Minimum length	12 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 (annual rotation)
Lockout	10 failed attempts = 30-minute lockout

Strong Password Guidance

DO: - Use a passphrase (4+ random words) - Make it memorable but unique - Use a password manager - Make each account password unique

DON'T: - Use dictionary words alone - Include personal information (name, birthday, etc.) - Use keyboard patterns (qwerty, 12345) - Reuse passwords from other sites - Share passwords with anyone

Example Strong Passwords

- `correct-horse-battery-staple` (passphrase)
- `Mnt@inSunr1se2024!` (mixed characters)
- `3Blue#Elephants&Dance` (memorable phrase)

Password Manager

Recommended: 1Password

NovaTech provides 1Password licenses for all employees: - Securely stores all passwords - Generates strong passwords - Works across devices - Family plan included (personal use)

Getting Started with 1Password

1. Accept invitation email from 1Password
2. Set up your master password (make it VERY strong)
3. Install browser extension
4. Install mobile app

See 1Password Setup Guide (IT-SW-010) for detailed instructions.

System-Specific Requirements

Okta (SSO)

- Primary authentication for most systems
- Enforces standard requirements
- MFA required for all logins

Service Accounts

- Minimum 20 characters
- Random generation required
- Stored in SecureVault (not 1Password)
- See Service Account Management (IT-ACC-015)

API Keys and Tokens

- Treat as passwords
- Store in SecureVault
- Never commit to code repositories
- Rotate regularly (90 days recommended)

Multi-Factor Authentication (MFA)

Requirement

MFA is **required** for all NovaTech accounts that support it.

Supported Methods (in order of preference)

1. **Hardware security key** (YubiKey) - Strongest
2. **Authenticator app** (Okta Verify, Google Authenticator)
3. **Push notification** (Okta Verify)
4. **SMS** (least secure, avoid if possible)

Setting Up MFA

1. Log into Okta
2. Go to Settings > Security Methods
3. Add at least 2 methods (backup)
4. Store backup codes securely

See MFA Setup Guide (IT-ACC-003) for detailed instructions.

Password Rotation

Standard Rotation

- Passwords expire annually (365 days)
- 14-day warning before expiration
- Grace period for updates
- No penalty for early rotation

Forced Rotation

Immediate password change required when: - Suspected compromise - Security incident - Shared with unauthorized person - Exposed in data breach

How to Change Your Password

1. Go to app.novatech.com/apps
2. Click your profile icon
3. Select “Settings” > “Password”
4. Follow prompts to create new password

Compromised Passwords

If You Suspect Compromise

1. Change password immediately
2. Report to security@novatech.com
3. Review account activity for unauthorized access
4. Check if password was used elsewhere (change those too)

Breach Monitoring

IT Security monitors for NovaTech credentials in known breaches. If your credentials appear: - You'll be notified automatically - Password reset will be required - Additional verification may be needed

Password Recovery

Self-Service Recovery

Most password resets can be done via: 1. "Forgot Password" link on login page 2. Verification via MFA or email 3. Create new password

IT-Assisted Recovery

If self-service fails: 1. Contact IT Support 2. Verify identity (ID verification process) 3. IT issues temporary password 4. Change immediately upon login

Manager-Approved Recovery

For sensitive systems, manager verification may be required before password reset.

Prohibited Practices

Never Do These

- **Share passwords** - Each person must have their own credentials
- **Write passwords down** - Use password manager instead
- **Send via unencrypted channels** - Never email or Slack passwords
- **Store in plain text** - No passwords in documents, code, or notes
- **Use "password" variations** - password1, P@ssw0rd, etc.
- **Bypass MFA** - Required on all supported systems

Consequences

Password policy violations may result in: - Required security training - Account lockout pending investigation - Disciplinary action for serious violations

Special Circumstances

Shared Accounts

- Shared accounts are discouraged
- When necessary, use SecureVault for credential sharing
- Each person should still have individual auditable access

Temporary Passwords

- Expire after first use
- Maximum 24-hour validity
- Must be changed immediately

Emergency Access

- Break-glass procedures exist for emergencies
- Documented and audited
- See Emergency Access Procedures (IT-ACC-030)

FAQ

Q: Why can't I use my pet's name? A: Personal information is easily guessable. Attackers research targets.

Q: Do I really need different passwords for everything? A: Yes. If one is compromised, others remain safe. Use a password manager.

Q: My password manager generated a 50-character password. Is that okay? A: Yes! Longer is better. Password managers remove the need to remember it.

Q: What if I forget my master password for 1Password? A: This is critical - write it down and store securely (safe, safe deposit box). 1Password cannot recover it.

Q: How often should I actually change my password? A: Annually is required, but change immediately if you suspect any compromise.

Q: Can IT see my password? A: No. Passwords are stored hashed. IT can reset passwords but cannot view them.

Support

For password-related issues: - **Self-service:** app.novatech.com/account - **Slack:** #it-help - **Email:** it-support@novatech.com

---

Related Documents: MFA Setup Guide (IT-ACC-003), 1Password Setup Guide (IT-SW-010), SSO Login Procedures (IT-ACC-002), Security Awareness Training (IT-SEC-001)