Security FAQs

Document Number: FAQ-SEC-001 **Last Updated:** February 2024 **Owner:** Information Security

---

Passwords & Authentication

Q: What are the password requirements?

A: Standard accounts require: - Minimum 16 characters - At least 3 of 4 character types (uppercase, lowercase, numbers, symbols) - Cannot reuse last 12 passwords - Must change every 365 days

Use a passphrase like "MyDog$Loves2RunInThe*Park!" for easy-to-remember but strong passwords.

Q: Is multi-factor authentication required?

A: **Yes**, MFA is required for all accounts with no exceptions. Approved methods: - Hardware security key (YubiKey) - Preferred - Okta Verify app - Push notification - TOTP authenticator apps

SMS is NOT allowed due to security vulnerabilities.

Q: How do I set up MFA?

A: 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. We recommend setting up a backup method

Q: I lost my MFA device. What do I do?

A: 1. Use your backup MFA method if you have one 2. If no backup: Contact IT Service Desk 3. IT will verify your identity and issue temporary access 4. Set up new MFA device immediately

Q: How do I get a YubiKey?

A: Request via IT Service Desk. All employees can receive 2 YubiKeys (primary and backup) at no cost.

Password Manager

Q: Does NovaTech provide a password manager?

A: Yes, all employees receive a **1Password** account. Features: - Personal vault for your accounts - Team vaults for shared credentials - Browser extension and desktop app - Mobile app

Q: How do I set up 1Password?

A: 1. Check email for 1Password invitation 2. Create your master password (strong!) 3. Download emergency kit PDF 4. Install browser extension 5. Install desktop and mobile apps

Q: Can I use 1Password for personal passwords?

A: Yes! Your 1Password account includes a personal vault for non-work passwords. Keep work and personal separate.

Q: What if I forget my 1Password master password?

A: Use your emergency kit to recover. If you've lost both: 1. Contact IT 2. Account will be reset 3. All saved passwords will be lost (you'll need to reset them)

This is why saving your emergency kit is critical!

Phishing & Suspicious Activity

Q: How do I identify a phishing email?

A: Red flags: - Unexpected or urgent requests - Sender email doesn't match claimed organization - Generic greetings ("Dear Customer") - Spelling and grammar errors - Suspicious links (hover to check URL) - Requests for credentials or sensitive info - Threats or extreme urgency

Q: What should I do if I receive a suspicious email?

A: 1. **Don't click any links or attachments** 2. Report it: Click the "Report Phishing" button in Gmail 3. Forward to: security@novatech.com 4. Delete the email

Q: I clicked on a suspicious link. What now?

A: 1. **Immediately** disconnect from the network if possible 2. Report to security@novatech.com 3. Change passwords for any accounts you might have exposed 4. Security team will guide you through next steps

Q: I gave out my password to a phishing site. What do I do?

A: 1. **Immediately** change your NovaTech password 2. Change passwords for any other accounts using that password 3. Report to security@novatech.com 4. Enable additional monitoring on your accounts 5. Security team will review and respond

---

Device Security

Q: What security software is required on my laptop?

A: All NovaTech laptops automatically have: - CrowdStrike Falcon (endpoint protection) - Disk encryption (FileVault/BitLocker) - MDM management - Automatic updates

Don't disable or remove these tools.

Q: Can I use my personal device for work?

A: Limited use allowed: - **Phone:** Can install Slack and Okta Verify - **Tablet:** Can access email via web - **Computer:** Not allowed for work purposes

All work should be done on your NovaTech laptop.

Q: My laptop was lost or stolen. What do I do?

A: 1. **Immediately** report to IT: it@novatech.com or #it-help 2. Report to security@novatech.com 3. IT will remotely wipe the device 4. Change passwords for any saved credentials 5. If stolen, file a police report

Time is critical - report immediately to minimize risk.

Q: What should I do when traveling with my laptop?

A: - Never leave your laptop unattended - Use a laptop lock in hotels - Use VPN on all public networks - Avoid public charging stations (use your own charger) - Don't let others use your device - Be aware of shoulder surfers

---

Data Security

Q: What is sensitive data?

A: Data classifications at NovaTech: - **Public:** Can be shared openly - **Internal:** NovaTech employees only - **Confidential:** Limited access, business sensitive - **Restricted:** Highest sensitivity (PII, financial, credentials)

Q: How should I handle customer data?

A: - Access only what you need - Don't download to personal devices - Don't share outside approved channels - Report any accidental exposure immediately - Follow data handling procedures in IT-SEC-005

Q: Can I use personal cloud storage (Google Drive, Dropbox)?

A: **No**. Use only NovaTech-approved storage: - Google Drive (NovaTech account) - Confluence - SecureVault (for secrets) - Approved project repositories

Q: How do I share files securely with external parties?

A: - Use NovaTech Google Drive with view-only links - Set expiration on shared links - Verify recipient before sharing sensitive data - Use password protection for highly sensitive files - Don't send sensitive attachments via email

---

Network Security

Q: Is VPN required?

A: VPN is required when: - Working from public WiFi - Accessing sensitive internal systems - On untrusted networks

VPN is recommended but not required on your secure home network.

Q: How do I connect to VPN?

A: 1. Open GlobalProtect app 2. Enter portal: vpn.novatech.com 3. Sign in with Okta credentials 4. Complete MFA 5. Click Connect

Q: Can I use public WiFi?

A: With precautions: - **Always use VPN** on public WiFi - Avoid accessing highly sensitive systems - Prefer mobile hotspot when possible - Don't access banking or enter passwords without VPN

Q: Is my home network secure enough?

A: Recommendations for home network security: - Use WPA3 or WPA2 encryption (not WEP) - Change default router password - Use a strong WiFi password - Keep router firmware updated - Consider a separate guest network

---

Reporting Security Issues

Q: How do I report a security concern?

A: Report to: **security@novatech.com**

What to report: - Suspicious emails (phishing) - Potential data breaches - Lost or stolen devices - Suspicious activity on accounts - Security vulnerabilities you discover - Policy violations you observe

Q: What happens when I report something?

A: 1. Security team receives your report 2. They assess severity 3. Investigation begins if needed 4. You may be contacted for more information 5. Incident is resolved and documented 6. You'll receive follow-up if appropriate

Q: Will I get in trouble for reporting?

A: **Never**. We encourage reporting and have a no-retaliation policy. Reporting issues helps keep everyone safe.

Q: Is there a bug bounty program?

A: Yes, we have a bug bounty program through HackerOne for external security researchers. Internal employees should report through normal channels.

Compliance & Training

Q: What security training is required?

A: - **Security Awareness Training:** Annual, all employees - **Phishing Simulations:** Quarterly - **Role-Specific Training:** As required by role

Complete training via the Knowbe4 platform.

Q: How often is training required?

A: Annual training is required by: - SOC 2 compliance - Customer contracts - NovaTech policy

Complete by the deadline to avoid access restrictions.

Q: What is SOC 2 and why does it matter?

A: SOC 2 is a security certification that: - Assures customers their data is protected - Required for enterprise sales - Demonstrates our security commitment

Your compliance with policies directly supports SOC 2.

Questions?

- **Security questions:** security@novatech.com
- **IT support:** #it-help
- **Password help:** IT Service Desk
- **Policy questions:** Your manager or HR

Related Documents: Security Best Practices (IT-SEC-001), Password Policy (IT-SEC-020), Data Classification (IT-SEC-005)