Security Best Practices for Employees

Document ID: IT-SEC-010 **Last Updated:** 2024-02-15 **Owner:** Security Team **Classification:** Internal

Overview

Security is everyone's responsibility at NovaTech. This guide outlines essential security practices for all employees to protect our company, customers, and data.

Password Security

Requirements

- Minimum **16 characters**
- Mix of uppercase, lowercase, numbers, symbols
- No dictionary words or personal information
- Unique password for each service

Best Practices

- Use **1Password** (company-provided) to generate and store passwords
- Never reuse passwords across services
- Never share passwords via Slack, email, or any channel
- Enable 2FA everywhere it's available

Password Manager Setup

1. Download 1Password from software center
2. Sign in with your NovaTech account
3. Install browser extension
4. Start saving passwords to vault

Multi-Factor Authentication (MFA)

Required MFA

MFA is mandatory for: - Okta (all NovaTech applications) - AWS Console - GitHub - VPN - Financial systems

Approved MFA Methods

Method	Security Level	Recommended
Hardware key (YubiKey)	Highest	Yes
Okta Verify (push)	High	Yes
Authenticator app (TOTP)	Medium	Yes
SMS	Low	Backup only

Hardware Security Keys

All employees receive a YubiKey. Set up for: - Okta primary MFA - GitHub 2FA - Personal accounts (optional)

Email Security

Recognizing Phishing

Red flags: - Urgency (“Act now!”, “Immediate action required”) - Suspicious sender address - Generic greetings - Requests for credentials or sensitive data - Unexpected attachments - Mismatched or suspicious links

When in Doubt

1. Don’t click links or download attachments
2. Report to security@novatech.com
3. Use the “Report Phishing” button in Gmail
4. Ask in #security-questions if unsure

Safe Email Practices

- Verify unexpected requests through a different channel
- Hover over links to preview URLs before clicking
- Never provide credentials via email
- Be cautious of calendar invites from unknown senders

Device Security

Laptop Security

- Enable FileVault (Mac) or BitLocker (Windows) - enforced by IT
- Set up screen lock: 5 minutes inactivity
- Lock screen when away: `Cmd+Ctrl+Q` (Mac) or `Win+L` (Windows)
- Keep software updated (automatic updates enabled)
- Never leave laptop unattended in public

Mobile Device Security

- Enable device PIN/biometric lock
- Enroll in MDM if using for work
- Don't install apps from untrusted sources
- Enable "Find My" feature

Public Spaces

- Use privacy screen in public
- Never leave devices unattended
- Be aware of shoulder surfing
- Avoid sensitive work in public

Network Security

VPN Usage

Required when: - Using public WiFi (coffee shops, airports) - Accessing production systems - Handling sensitive data

Optional but recommended: - Home network - Mobile hotspot

Public WiFi Risks

- Avoid accessing sensitive data on public WiFi without VPN
- Don't access banking or financial accounts
- Verify network names (avoid evil twin attacks)
- Prefer mobile hotspot when possible

Home Network

- Use strong WiFi password (WPA3 preferred)
- Keep router firmware updated
- Consider separate network for IoT devices
- VPN recommended for sensitive work

Data Protection

Data Classification

Level	Examples	Handling
Public	Marketing materials	No restrictions
Internal	Policies, procedures	Internal only
Confidential	Customer data, financials	Encrypted, need-to-know
Restricted	Security configs, keys	Strict access control

Handling Sensitive Data

- Never share via unencrypted channels
- Don't store on personal devices
- Use approved tools only (see Data Classification Policy)
- Delete when no longer needed

Customer Data

- Access only for legitimate business need
- Never copy to local devices
- Report any suspected breach immediately
- Follow GDPR and data privacy policies

Physical Security

Office Security

- Always badge in (no tailgating)
- Challenge unknown visitors politely
- Lock confidential documents
- Use shredders for sensitive papers
- Report lost badges immediately

Working Remotely

- Secure workspace from family/roommates for sensitive calls
- Use headphones for confidential discussions
- Lock screen when stepping away
- Be mindful of smart speakers/cameras

Incident Reporting

What to Report

- Suspected phishing attempts
- Lost or stolen devices
- Suspicious system activity
- Potential data breaches
- Unknown people in secure areas
- Anything that seems “off”

How to Report

- **Urgent:** #security-urgent Slack channel
- **Email:** security@novatech.com
- **Phone:** +1-512-555-0199 (24/7 hotline)

No Blame Culture

- Report incidents without fear of punishment
- Early reporting minimizes damage
- We learn from incidents to improve

Social Engineering Awareness

Common Tactics

- **Pretexting:** Fake scenarios to extract information
- **Baiting:** Offering something enticing
- **Quid pro quo:** Offering help in exchange for information
- **Tailgating:** Following someone into secure areas

Defense

- Verify identity through official channels
- Don't share information with unverified requesters
- Be skeptical of unsolicited offers
- Report suspicious approaches

Security Training

Required Training

- Annual security awareness training
- Phishing simulation exercises
- Role-specific security training

Resources

- Security wiki: wiki.novatech.com/security
- Monthly security newsletter
- #security-awareness Slack channel

Quick Reference

Emergency Contacts

- Security hotline: +1-512-555-0199
- Email: security@novatech.com
- Slack: #security-urgent

Key Actions

1. Use 1Password for all passwords
2. Set up YubiKey as primary MFA
3. Lock screen when away
4. Use VPN on public WiFi
5. Report suspicious emails
6. Report incidents immediately

Related Documents: Password Requirements (IT-ACC-001), VPN Setup Guide (IT-ACC-003), Data Classification Policy (COM-DP-001), Incident Response Plan (IT-SEC-020)