Acceptable Use Policy

Document ID: IT-SEC-015 **Last Updated:** 2024-02-01 **Owner:** IT Security
Classification: Internal **Applies To:** All Employees, Contractors, Vendors

---

Purpose

This policy defines acceptable use of NovaTech's information technology resources to protect our systems, data, and people while enabling productive work.

Scope

This policy covers: - Company-provided computers and devices - Company networks and internet access - Company email and communication tools - Company software and applications - Personal devices used for work (BYOD) - Cloud services and accounts

---

General Principles

Authorized Use

NovaTech IT resources are provided for business purposes. Limited personal use is permitted if it: - Does not interfere with work responsibilities - Does not violate any policy - Does not consume excessive resources - Does not expose the company to risk

User Responsibility

You are responsible for: - All activity under your accounts - Protecting your credentials - Following security policies - Reporting security concerns - Using resources appropriately

No Expectation of Privacy

NovaTech reserves the right to monitor and access: - Company-owned devices - Company email and communications - Network traffic - System logs and usage data

Monitoring is conducted for security, compliance, and operational purposes.

Acceptable Use

Permitted Activities

Work-related activities: - Business communications - Research and development - Training and learning - Collaboration with colleagues - Customer interactions

Limited personal use: - Brief personal communications - Personal email (web-based) - News and informational sites - Brief online shopping/banking

Prohibited Activities

Illegal activities: - Downloading pirated software/media - Hacking or unauthorized access - Harassment or threats - Child exploitation material - Fraud or identity theft

Security violations: - Sharing credentials - Bypassing security controls - Installing unauthorized software - Connecting unauthorized devices - Disabling security tools

Inappropriate content: - Pornography or explicit material - Hate speech or discriminatory content - Violent or disturbing content - Gambling (unless legally permitted)

Resource abuse: - Cryptocurrency mining - Excessive streaming/downloading - Running personal businesses - Mass personal file storage

Communication violations: - Spam or mass mailings - Impersonation - Defamatory statements - Unauthorized external communications

---

Email and Communication

Appropriate Use

- Professional tone in business communications
- Appropriate use of reply-all and distribution lists
- Prompt response to business communications
- Clear subject lines and signatures

Prohibited

- Sending confidential information externally without encryption
- Forwarding chain letters or hoaxes
- Using company email for personal business
- Sending messages that could embarrass the company
- Auto-forwarding to personal email

Retention

- Business emails are retained per retention policy
- Do not delete emails subject to legal hold
- Personal emails are not backed up

Internet Use

Acceptable

- Work-related research
- Professional development
- Limited personal browsing during breaks
- Streaming for work purposes (meetings, training)

Blocked or Restricted

The following categories are blocked or monitored: - Adult content - Malware/phishing sites - Anonymizing proxies - Peer-to-peer file sharing - Known security threats

Bandwidth Considerations

- Avoid large downloads during business hours
- Use streaming sparingly
- Report slow network issues to IT

Device Use

Company Devices

- Use for authorized purposes only
- Keep physically secure
- Enable encryption and screen lock
- Install updates promptly
- Do not modify hardware
- Return when leaving company

Personal Devices (BYOD)

If approved for BYOD: - Enroll in MDM solution - Keep device updated and secure - Allow remote wipe of work data - Report lost/stolen immediately - Separate work and personal data

Mobile Devices

- Use screen lock (PIN/biometric)
- Enable device encryption
- Install only approved apps for work
- Do not jailbreak/root devices
- Use VPN on public networks

Software and Applications

Approved Software

- Install only approved software
- Request new software through IT
- Keep software updated
- Use software per license terms

Prohibited Software

- Pirated or cracked software
- Hacking tools
- Unauthorized remote access tools
- Cryptocurrency miners
- Peer-to-peer sharing apps

Cloud Services

- Use only approved cloud services for work
- Do not store company data in personal cloud
- Follow data classification for cloud storage
- Enable MFA on all cloud accounts

Data Handling

Classification

Handle data according to its classification: - **Public:** No restrictions - **Internal:** Keep within company - **Confidential:** Need-to-know, encrypted - **Restricted:** Strict controls, encrypted

Prohibited Data Handling

- Storing company data on personal devices (unless approved)
- Sharing confidential data externally without authorization
- Copying customer data without business need
- Posting company information on social media

Social Media

Business Use

- Only authorized employees post as NovaTech
- Follow social media guidelines
- Protect confidential information

Personal Use

- Clearly distinguish personal from company views
- Do not disclose confidential information
- Do not speak on behalf of NovaTech
- Be professional even on personal accounts

Remote Work

Security Requirements

- Secure home network (change default passwords)
- Use VPN for sensitive work
- Keep work devices physically secure
- Do not allow others to use work devices
- Be aware of surroundings on video calls

Public Spaces

- Use VPN on public WiFi
- Use privacy screen
- Do not discuss confidential matters audibly
- Keep devices with you at all times

Reporting

What to Report

Report to IT Security immediately: - Lost or stolen devices - Suspected security incidents - Phishing attempts - Unauthorized access - Policy violations by others

How to Report

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

Non-Retaliation

Employees who report concerns in good faith are protected from retaliation.

Enforcement

Monitoring

IT may monitor: - Network traffic - Email communications - Website access - Device activity - Cloud application usage

Violations

Violations may result in: - Verbal or written warning - Temporary suspension of access - Termination of employment - Legal action if warranted

Severity Factors

- Nature of violation
- Intent (accidental vs. deliberate)
- Impact on security/operations
- Previous violations
- Cooperation in investigation

Acknowledgment

All users must acknowledge this policy: - During onboarding - Annually during compliance certification - When policy is significantly updated

---

Questions

For questions about this policy: - IT Security: security@novatech.com - IT Help: #it-help - HR: hr@novatech.com

---

Related Documents: Information Security Policy (IT-SEC-001), Data Classification Policy (IT-SEC-005), Remote Work Policy (HR-WRK-001)