# NovaTech Systems Acceptable Use Policy (AUP)

* Effective Date: 2025-04-15
* Policy Version: 2.0

## **1. Introduction and Purpose**

NovaTech Systems ("Company") provides various technology resources, including computers, network access, internet connectivity, email, software, and data ("Company Resources"), to its employees and other authorized users ("Users") to support business operations and facilitate job performance. These resources are valuable assets and represent a significant investment by the Company. Their use is a privilege granted to Users and is subject to the conditions outlined in this Acceptable Use Policy (AUP).

This policy establishes the rules and guidelines for the responsible, ethical, secure, and legal use of Company Resources. For many small and medium-sized businesses, clearly communicating expectations around technology use is fundamental not only for setting rules but also for educating users on basic security practices, which is vital given potentially limited resources for dedicated security training. Adherence to this AUP is essential for protecting the Company, its Users, its customers, and its partners.

The primary goals of this policy are to:

* Ensure the security, integrity, confidentiality, and availability of the Company's information systems, data, and network resources.
* Protect the Company's proprietary information, intellectual property, and sensitive data (including customer and employee data) from unauthorized access, disclosure, or loss.
* Prevent misuse of Company Resources that could lead to security breaches, legal liability, financial loss, or damage to the Company's reputation.
* Ensure compliance with all applicable laws, regulations, and contractual obligations.
* Maintain a productive and professional work environment free from harassment and inappropriate content.

All Users share the responsibility for understanding and adhering to this policy and for using Company Resources in a manner that reflects ethical and professional conduct.

## **2. Scope**

This policy applies to **all individuals** granted access to or using Company Resources, regardless of their location or role. This includes, but is not limited to:

* Full-time and part-time employees
* Temporary employees
* Contractors, consultants, and freelancers
* Volunteers and interns
* Volunteers and interns

This policy governs the use of **all Company Resources**, including, but not limited to:

* Company-issued hardware: Desktops, laptops, tablets, mobile phones, servers, printers, scanners, network equipment, peripherals.
* Personal devices used for work purposes (Bring Your Own Device - BYOD): \*\*\*\* *Note: Permitting BYOD introduces significant security and privacy complexities, especially regarding monitoring personal devices. A detailed, legally reviewed BYOD policy is strongly recommended if allowed.*
* Company network infrastructure: Wired and wireless networks (Wi-Fi), VPNs, remote access systems.
* Internet access provided by or through the Company.
* Communication systems: Company email, instant messaging platforms (e.g., Slack, Slack), video conferencing tools, phone systems.
* Software and applications: Company-licensed software (installed or cloud-based), operating systems, business applications (e.g., CRM, ERP), cloud services (e.g., Microsoft 365, Google Workspace, ``).
* Company data: All data created, stored, accessed, or transmitted using Company Resources, including customer information, financial records, intellectual property, trade secrets, employee data, operational data, and any data classified as confidential.
* Company accounts and credentials used to access any of the above resources.

## **3. Definitions**

To ensure clarity, the following terms are defined for the purpose of this policy :

* Company Resources: All technology, information, and communication systems owned, leased, managed by, or operated on behalf of NovaTech Systems. This includes hardware, software, networks, internet access, email, data, intellectual property, and related equipment and services.
* **User:** Any individual identified in the Scope section of this policy who is granted access to or uses Company Resources.
* **Confidential Information:** Any non-public information belonging to the Company, its customers, partners, or employees, the unauthorized disclosure of which could cause harm. Examples include, but are not limited to: financial data, customer lists and details, Personally Identifiable Information (PII), Protected Health Information (PHI) (if applicable), business strategies, product designs, source code, pricing information, employee records, passwords, security configurations, and ``.
* **Malware:** Malicious software designed to damage, disrupt, steal, or inflict illegitimate action on data, hosts, or networks. Includes viruses, worms, Trojan horses, ransomware, spyware, adware, and other harmful code.
* **Phishing:** Fraudulent attempts, typically via email, text message, or website, to deceive individuals into revealing sensitive information such as login credentials, credit card numbers, or personal identifiers, often by impersonating a legitimate entity.
* **Personal Use:** Any use of Company Resources for activities not directly related to the User's assigned job responsibilities or the Company's business objectives.
* **Intellectual Property (IP):** Intangible creations protected by law, such as patents, copyrights, trademarks, and trade secrets. This includes software developed by the Company, documentation, designs, branding, marketing materials, and proprietary processes.

## **4. Acceptable Use Guidelines**

Company Resources are provided to facilitate business activities and support Users in performing their job duties effectively. Acceptable use includes:

* Performing tasks directly related to your job description and responsibilities.
* Communicating with colleagues, clients, suppliers, and business partners for work-related purposes using approved Company communication systems (e.g., company email, Slack).
* Accessing, creating, storing, and sharing work-related documents, data, and information using authorized Company systems and platforms.
* Conducting research and accessing information on the internet necessary for completing work assignments.
* Using company-licensed software and applications for their intended business functions.
* *Placeholder:* Utilizing Company-approved Artificial Intelligence (AI) tools (e.g., ) strictly for while adhering to the data input restrictions outlined in the Prohibited Activities section.

**Incidental Personal Use:**

* **[Option 1: Permitted]** Limited, occasional personal use of Company Resources is permitted provided it meets **all** the following conditions :
  + It is brief and occurs during personal time (e.g., breaks, lunch) or does not interfere with work duties and productivity.
  + It does not consume significant Company resources (e.g., excessive bandwidth for streaming, large downloads/uploads, excessive storage).
  + It does not violate any other provisions of this AUP, particularly the Prohibited Activities section.
  + It does not result in any direct cost to the Company.
  + It does not expose the Company to unnecessary security risks.
  + Examples of potentially acceptable incidental use: brief checks of personal email (non-work accounts), quick access to news or weather sites, brief personal phone calls using company phone if permitted.
* **[Option 2: Prohibited]** Personal use of Company Resources is strictly prohibited. All use must be directly related to Company business.

*Note: Permitting incidental use requires careful definition and consistent enforcement to avoid ambiguity and potential abuse. SMBs should consider if they have the means to monitor and enforce these distinctions effectively. A stricter policy may be simpler to manage.*

## **5. Prohibited Activities**

Any use of Company Resources that violates laws, regulations, contractual obligations, ethical standards, or other Company policies is strictly prohibited. Engaging in prohibited activities may lead to disciplinary action, including termination, and potential legal consequences. The following activities are explicitly prohibited :

* **Illegal or Unlawful Activities:**
  + Using Company Resources for any activity that violates federal, state, local, or international laws or regulations.
  + Infringing upon intellectual property rights, including copyright, trademark, and patent laws (e.g., downloading, installing, or distributing pirated software, music, videos, or other copyrighted materials).
  + Engaging in fraud, theft, embezzlement, or deceptive practices.
  + Accessing or distributing child pornography or other illegal content.
  + Making threats of violence.
  + Illegal gambling.
* **Security Violations:**
  + Sharing account passwords, access tokens, smartcards, keys, or other authentication credentials with anyone, including colleagues, family, or friends.
  + Attempting to bypass or disable security controls, firewalls, access restrictions, monitoring tools, or authentication mechanisms.
  + Knowingly or negligently introducing Malware (viruses, worms, ransomware, spyware, etc.) onto Company systems or networks.
  + Attempting to gain unauthorized access to any Company or third-party system, data, account, or network (hacking).
  + Performing unauthorized security scanning, vulnerability assessments, or penetration testing on Company or external networks.
  + Intercepting network traffic or communications not intended for the User.
  + Connecting unauthorized devices (e.g., personal USB drives containing unknown software, unapproved routers, personal laptops without authorization) to the Company network or Company-issued devices.
* **Data Misuse and Disclosure:**
  + Accessing, copying, modifying, deleting, sharing, or transmitting Confidential Information or personal data (customer, employee, or partner) without proper authorization and a legitimate business need-to-know.
  + Storing Company data, especially Confidential Information, on personal devices, personal cloud storage accounts (e.g., personal Dropbox, Google Drive), or any unauthorized location.
  + Improperly disposing of data or equipment containing data (e.g., failing to shred documents, not securely wiping devices before disposal).
  + Inputting Confidential Information, proprietary code, customer data, PII/PHI, or any non-public Company information into public or unapproved AI tools or platforms (e.g., public versions of ChatGPT, Google Gemini, [List specific unapproved tools]).
* **Inappropriate Content and Communication:**
  + Creating, accessing, storing, transmitting, downloading, or distributing content that is obscene, pornographic, sexually explicit, profane, harassing, abusive, threatening, defamatory, libelous, discriminatory (based on race, religion, gender, sexual orientation, disability, age, etc.), hateful, violent, or otherwise offensive or inappropriate for a professional workplace.
  + Engaging in cyberbullying, harassment, or creating a hostile work environment through electronic communications.
  + Sending unsolicited bulk email (spam), chain letters, pyramid schemes, or other disruptive mass communications.
  + Forging email headers, IP addresses, or otherwise misrepresenting the origin of communications (impersonation).
* **Network Abuse and Resource Misuse:**
  + Engaging in activities that intentionally degrade or disrupt network performance, system availability, or access for other Users (e.g., excessive personal streaming, large file sharing for non-business purposes, running unauthorized servers or services, cryptocurrency mining).
  + Launching denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks against any system or network.
* **Unauthorized Software/Hardware:**
  + Downloading, installing, or using any software, applications, browser extensions, hardware, or peripherals that have not been explicitly approved by the Company's IT department or ``.
* **Misrepresentation and Unauthorized Actions:**
  + Impersonating another individual or entity in communications.
  + Representing personal opinions as those of the Company without explicit authorization.
  + Entering into contracts or agreements on behalf of the Company without proper authority.
* **Personal Gain:**
  + Using Company Resources to operate a personal business, for commercial solicitation, or for significant political activity or lobbying (unless expressly authorized).
* **Other Prohibited Activities:**
  + *Placeholder:* `` *Note: Tailoring this section with specific, relevant examples significantly increases the policy's effectiveness for the client's environment.*

## **6. User Security Responsibilities**

All Users play a critical role in maintaining the security of Company Resources. Adherence to the following security practices is mandatory :

* **Password and Authentication Security:**
  + Create strong, unique passwords for all Company accounts, following the guidelines specified in the Company's Password Policy (if applicable) or meeting minimum requirements (e.g., ``).
  + Keep all passwords and authentication credentials strictly confidential. Do not share them with anyone, write them down in easily accessible locations, or store them insecurely.
  + Change passwords immediately if compromise is suspected and follow any scheduled password change requirements.
  + Utilize Multi-Factor Authentication (MFA) whenever it is required or offered for Company accounts and systems.
* **Device Security:**
  + Always lock your computer screen (e.g., using Ctrl+Alt+Del on Windows, or Cmd+Control+Q on Mac) or log off when leaving your workstation unattended, even for short periods. Configure automatic screen locking after [e.g., 10-15] minutes of inactivity.
  + Physically secure all Company-issued devices (laptops, tablets, phones) against theft, loss, or unauthorized access, especially when working remotely, traveling, or in public spaces. Do not leave devices unattended in vehicles or public areas.
  + Report any lost or stolen Company device immediately to ``.
  + When working remotely or in public, connect only to trusted and secure Wi-Fi networks. Use the Company-provided Virtual Private Network (VPN) when accessing Company Resources remotely, as required by policy. Avoid using public Wi-Fi for sensitive tasks.
* **Data Handling and Protection:**
  + Access, use, store, and transmit Confidential Information only as authorized and necessary for your job duties. Handle all Company data with appropriate care and according to its classification (if applicable).
  + Do not store Confidential Information or sensitive Company data on personal devices, personal cloud storage services, or removable media (like USB drives) unless explicitly authorized and secured according to Company policy.
  + Securely dispose of sensitive information when no longer needed, following Company procedures (e.g., using approved shredders for paper documents, securely deleting electronic files).
  + Use encryption for sensitive data in transit (e.g., email attachments) and at rest (e.g., on laptops, removable media) where required by policy or regulation.
* **Email and Internet Security:**
  + Exercise extreme caution with emails, messages, links, and attachments from unknown or suspicious sources. Be vigilant for signs of phishing attempts. Do not click links or open attachments unless you are confident of the sender's identity and the content's legitimacy.
  + Do not download or install software, browser extensions, or files from untrusted websites or sources.
  + Report any suspicious emails, websites, or potential security threats immediately to ``.
* **Software and System Maintenance:**
  + Use only software that is licensed to the Company and approved for use by the IT department or ``. Do not install unauthorized software.
  + Ensure your operating system and applications are kept up-to-date with the latest security patches and updates. Cooperate with IT/`` regarding scheduled updates and patch management. Do not disable or interfere with update processes.
* **Incident Reporting:**
  + Immediately report any suspected or actual security incidents, policy violations, data breaches, malware infections, lost/stolen devices, or system vulnerabilities to ``. Early reporting is crucial for minimizing damage.
* **Physical Security:**
  + Keep physical documents containing Confidential Information secure (e.g., locked drawers, secure disposal). Maintain a clear desk and clear screen when away from your workspace.
  + Be aware of your surroundings. Prevent unauthorized individuals from viewing sensitive information on your screen ("shoulder surfing").
  + Do not allow unauthorized individuals to follow you into secure Company areas ("tailgating"). Challenge or report unfamiliar persons in restricted areas.

## **7. Monitoring and Privacy**

To ensure the security, integrity, and effective operation of its technology resources, and to enforce this policy, NovaTech Systems reserves the right to monitor, access, retrieve, read, and disclose any and all information created, sent, received, or stored on Company Resources. This includes, but is not limited to, monitoring of internet usage, email communications, file access, application usage, network traffic, and system logs.

Monitoring is conducted for legitimate business purposes only, including :

* Ensuring compliance with this AUP, other Company policies, and applicable laws and regulations.
* Protecting the Company's network, systems, and data from security threats, unauthorized access, malware, and other risks.
* Investigating suspected policy violations, misconduct, or illegal activities.
* Maintaining system performance, troubleshooting issues, and ensuring operational continuity.
* Meeting legal, regulatory, or auditing requirements.

Users should have no reasonable expectation of privacy regarding their use of Company Resources or any data created, stored, or transmitted on them. All such data and communications are considered the property of NovaTech Systems. While the Company respects employee privacy, the need to protect its resources and operations necessitates monitoring. Personal information encountered during monitoring will be handled appropriately, but privacy cannot be guaranteed on Company systems.

All monitoring activities will be conducted in accordance with applicable laws and regulations.

Optional Clause: Monitoring activities may be performed directly by NovaTech Systems personnel or by its authorized third-party IT service provider, ``.

*Note: Transparency about the purpose of monitoring (security, compliance, operations) is crucial for maintaining employee trust, even while explicitly stating the lack of privacy expectation on company systems. Avoid language suggesting arbitrary surveillance.*

## **8. Consequences of Violation**

Violation of this Acceptable Use Policy may lead to disciplinary action, up to and including immediate termination of employment or contract, and may also result in civil or criminal liability.

The specific disciplinary action taken will depend on the nature, severity, frequency, and impact of the violation, as well as any prior history of violations. Actions will be applied consistently and fairly. Potential consequences include, but are not limited to:

* Verbal warning.
* Written warning placed in the personnel file.
* Mandatory retraining on security awareness or policy compliance.
* Temporary or permanent suspension of access privileges to specific systems, applications, or the entire network.
* Recovery of costs incurred by the Company due to the violation (e.g., remediation costs, legal fees).
* Termination of employment, contract, or relationship with the Company.
* Reporting to law enforcement authorities if illegal activity is suspected, potentially leading to criminal prosecution or civil lawsuits.

*Note: Outlining a range of consequences emphasizes proportionality and suggests a fair process, which can encourage compliance and reporting of minor issues rather than immediate fear of termination for any mistake.*

Users are reminded of their responsibility to report any known or suspected violations of this policy immediately to ``.

## **9. Policy Review and Updates**

This Acceptable Use Policy will be reviewed at least annually, or more frequently as needed, by NovaTech Systems management`] to ensure its continued relevance, effectiveness, and compliance with changing technologies, business needs, and legal/regulatory requirements.

The Company reserves the right to amend or update this policy at any time. Users will be notified of any significant changes to the policy, and the updated version will be made available through Slack and internal HR portal. Continued use of Company Resources after notification of changes constitutes acceptance of the revised policy.

## **10. Contact Information**

* **For questions** regarding the interpretation or application of this policy, please contact:
  + ``
  + Email: security@novatech.com
  + Phone: 800-555-0123
* **To report suspected policy violations** or security incidents, please contact:
  + ``
  + Email: ``
  + Phone: ``

## **11. User Acknowledgment**

By signing below, or by accessing or using Company Resources after being provided with this policy, I acknowledge that I have received, read, and understood the NovaTech Systems Acceptable Use Policy, Version 2.0, dated 2025-04-15.

I agree to fully comply with all the rules, guidelines, and responsibilities outlined in this policy as a condition of my access to and use of Company Resources.

I understand that my use of Company Resources may be monitored and that I have no reasonable expectation of privacy regarding such use.

I further understand that any violation of this policy may result in disciplinary action, up to and including the termination of my employment or contract with NovaTech Systems, and may also lead to legal action if applicable laws are violated.

*Note: Obtaining this signed acknowledgment is crucial for demonstrating employee awareness and enforcing the policy effectively. This should be part of the onboarding process for new hires and done periodically for existing staff when the policy is updated.*

User Signature

User Printed Name

Date

## **12. Legal Disclaimer**

IMPORTANT NOTICE FOR NovaTech Systems:

This document is a general Acceptable Use Policy (AUP) template provided by `` for informational purposes only. It is intended to serve as a starting point and must be customized to meet the specific needs, risks, industry requirements, and legal obligations of NovaTech Systems.

* Customization Required: This template may not cover all situations or address all applicable laws and regulations relevant to your specific business operations and jurisdiction(s). You are solely responsible for reviewing, modifying, and adapting this policy to accurately reflect your company's environment, technology use, risk tolerance, and compliance requirements. Placeholders such as NovaTech Systems, , `2025-04-15`, , and `` must be replaced with appropriate information specific to Acme Tech Solutions.
* **Not Legal Advice:** This template does not constitute legal advice. Laws regarding employee monitoring, data privacy, intellectual property, and technology use vary significantly by jurisdiction and are subject to change.
* Legal Review Mandatory: NovaTech Systems MUST consult with its own independent legal counsel to review and approve the final version of this policy before implementation. This review is essential to ensure the policy complies with all applicable federal, state, local, and international laws, regulations, industry standards (e.g., HIPAA, PCI-DSS if applicable), and any relevant contractual obligations. Failure to obtain legal review may result in an unenforceable or non-compliant policy.
* Disclaimer of Liability: provides this template "as is" without any warranty, express or implied. disclaims any and all liability arising from the use, modification, or implementation of this template or the resulting policy by NovaTech Systems. The responsibility for the final policy content and its enforcement rests solely with Acme Tech Solutions.