**IT AND ELECTRONIC COMMUNICATIONS POLICY**

**PURPOSE**

[EMPLOYER'S NAME] provides computers, networks, communication systems, and other IT resources primarily for business use. Limited personal use is permitted, as outlined below, but these resources must be used responsibly and ethically at all times, both during and outside working hours. This policy outlines the expectations and restrictions on the use of these systems to protect [EMPLOYER'S NAME] and its employees.

Each individual is responsible for ensuring that their use of IT resources aligns with professional, ethical, and legal standards. Misuse or inappropriate activity will not be tolerated.

This policy is designed to comply with applicable New York and federal laws and regulations.

**ANTI-HARASSMENT AND RESPECTFUL USE**

All employees must comply with [EMPLOYER'S NAME]'s anti-harassment policies, such as [POLICY NAMES], when using IT resources or communication systems. These systems must not be used to engage in behavior that could be perceived as harassing or offensive based on race, national origin, gender, sexual orientation, age, disability, religion, or any other characteristic protected by law.

**AGREEMENT TO POLICY TERMS**

By using [EMPLOYER'S NAME]'s IT resources and communication systems, employees acknowledge their understanding of and agreement to the terms of this policy as a condition of their employment.

**SECURITY, ACCESS AND PASSWORD MANAGEMENT**

The Information Technology (IT) Department is responsible for maintaining the security of [EMPLOYER'S NAME]'s IT resources and communication systems. This includes approving and managing user access, as well as suspending or terminating access in cases of misuse or when an individual is no longer authorized to use the systems.

Employee responsibilities

Employees must follow IT security protocols, including guidelines for creating, formatting, and regularly updating passwords. All user credentials (e.g., usernames, passcodes, passwords) and data stored on [EMPLOYER'S NAME]'s systems are the property of the company. Employees may only use credentials assigned to them or authorized in advance by the company.

Employees are prohibited from sharing usernames, passcodes, or passwords with others [except for an administrative assistant specifically assigned to assist them].

If an employee knows or suspects that a username, passcode, or password has been improperly shared or used, or if any security violation has occurred, they must report it immediately to the IT Department.

**SCOPE OF RESOURCES AND SYSTEMS**

This policy applies to all IT resources and communication systems owned, operated, or made available by [EMPLOYER'S NAME], as well as any use of these resources when accessed through an employee's personal devices. The following resources and systems are covered under this policy:

* Email systems: All email accounts provided by [EMPLOYER'S NAME].
* Internet and intranet: Access to the internet and internal networks.
* Telecommunications: Telephones, voicemail systems, wired and mobile phones, smartphones, and pagers.
* Office equipment: Printers, photocopiers, scanners, and related peripherals.
* Fax systems: Physical fax machines, e-fax services, and modems.
* Computer hardware and software: All computers, networks, peripherals, key fobs, and associated software provided by [EMPLOYER'S NAME].
* Physical security systems: Closed-circuit television (CCTV), access control systems, key cards, and fobs.

This policy governs all usage of these resources and systems to ensure their appropriate and secure use.

**PRIVACY EXPECTATIONS**

All data, communications and content transmitted, received, stored, or recorded on [EMPLOYER'S NAME]'s IT resources and communication systems are the property of the company. Employees should not expect privacy regarding any information, message, file, data, document, facsimile, telephone conversation, social media activity, or any other communication created, transmitted, or stored using company systems.

Monitoring and oversight

To safeguard against misuse, [EMPLOYER'S NAME] reserves the right to monitor, intercept, and review employees' use of IT resources and communication systems without prior notice. This includes, but is not limited to:

* Monitoring email (both incoming and outgoing), telephone conversations, voicemail, instant messaging, internet activity, and social media posts.
* Utilizing tools such as keystroke capture and network monitoring technologies to inspect and review system usage.
* By using [EMPLOYER'S NAME]'s systems, employees acknowledge and consent to such monitoring.

Data retention

[EMPLOYER'S NAME] may retain copies of communications and other data for a specified period and reserves the right to delete these copies without prior notice.

Confidentiality reminder

Employees should avoid using company IT resources and communication systems for any personal matters they wish to remain private or confidential, as privacy cannot be guaranteed.

**NETWORK SYSTEMS**

[EMPLOYER'S NAME] maintains an integrated network to support its business operations. Employees must adhere to the following guidelines when using the network:

* Never log in to network equipment using another employee's username or password.
* Do not access, modify, or delete any network document unless it is part of your authorized work for [EMPLOYER'S NAME].

**DOWNLOADING AND INSTALLING SOFTWARE**

Downloading files or software from the internet poses significant risks, including the potential introduction of malware or viruses. To mitigate these risks:

* Do not download or install any software or shareware onto a company device without explicit authorization from the IT Department.
* Employees must not accept terms or conditions of website agreements without prior approval from [MANAGER NAME] or [DEPARTMENT NAME].

**OPEN SOURCE SOFTWARE**

For questions about open source software, refer to [EMPLOYER'S NAME]'s specific open source software policy, which addresses related use and restrictions.

**CONFIDENTIALITY AND PROPRIETARY RIGHTS**

[EMPLOYER'S NAME]'s confidential information and intellectual property, including trade secrets, are valuable assets. Employees must handle them with care and ensure their protection during any use of electronic communication systems, such as email, text messaging, internet access, social media, and phone conversations or voicemail.

Disclosure of [EMPLOYER'S NAME]'s confidential information or use of its intellectual property is governed by the company's confidentiality and proprietary rights [agreement/policy]. If you are unsure about sharing confidential information with specific individuals or need guidance on protecting proprietary rights, consult your manager.

Use of [EMPLOYER’S NAME]’s trademarks

Do not use [EMPLOYER'S NAME]'s name, brand names, logos, taglines, slogans, or trademarks without prior written approval from the [EMPLOYER'S NAME] Legal Department.

Third-party proprietary rights

This policy also prohibits using [EMPLOYER'S NAME]'s IT resources and communication systems in ways that infringe or violate third-party proprietary rights. Digital tools can access vast amounts of protected information, including materials covered by copyright, trademark, patent, or trade secret laws.

Do not knowingly use, share, or distribute such materials—whether downloaded from the internet or received via email—without prior written authorization from the [EMPLOYER'S NAME] Legal Department.

**EMAIL AND TEXT MESSAGING GUIDELINES**

[EMPLOYER'S NAME] provides certain employees with access to email and text messaging systems, including SMS and internet-based instant messaging, to support their job responsibilities. These systems are designed to promote efficient and secure business communication while minimizing unnecessary costs and unproductive messaging. The following guidelines outline acceptable use and etiquette for these systems.

Spam and suspicious messages

* Avoid interaction: Do not open, reply to, or interact with unsolicited commercial or bulk messages (spam). This includes messages offering to remove you from a distribution list.
* Report and block: Report suspicious messages to the email administrator, who can take steps to block incoming messages from the sender. Delete all spam immediately.
* Email address protection: Be cautious about using your company email address on websites, discussion forums, or other public platforms to avoid spam. For information-gathering purposes, use a separate email account from a free service, such as Gmail or Yahoo Mail.

Business email etiquette

* Professional tone: Email and text communications should be clear, concise, and professional. Avoid sarcasm, humor, inappropriate language, or comments that might be misinterpreted.
* Respectful correspondence: As emails lack visual and tonal cues, focus on precise and respectful language to minimize misunderstandings.

Personal use of company-provided email

[Choose one option based on company policy:]

* [Limited personal use: Personal use of company-provided email is allowed during non-working hours, provided it does not involve unprofessional or inappropriate content or interfere with your responsibilities.
* Occasional use permitted: Occasional personal use of company email is allowed during working hours, as long as it remains professional and does not affect your productivity or job responsibilities.
* No personal use: Personal use of company-provided email is strictly prohibited.]

**INTERNET AND SOCIAL MEDIA**

[EMPLOYER'S NAME] provides internet access to [certain] employees to support their job responsibilities. This section outlines the expectations and acceptable use of the internet and social media while using the company's IT resources.

Personal use of the internet

[Select the appropriate option based on company policy:]

* [Prohibited use: Personal internet use, including social media, is strictly prohibited during working hours or when using the company's computers, networks, and IT resources.
* Occasional use permitted: Employees may occasionally access the internet or social media for personal use while at work, provided such use remains professional, appropriate, and does not interfere with job responsibilities or productivity.]

Prohibited internet activities

Using the internet to access the following types of content or websites is strictly forbidden:

* Pornographic or sexually explicit material.
* "Hate" sites or any content promoting discrimination, harassment, or violence.
* Any site or activity that violates the law or [EMPLOYER'S NAME]'s policies against harassment and discrimination.

Monitoring and review

[EMPLOYER'S NAME] reserves the right to monitor and review all internet activities conducted on company systems without prior notice. This includes:

* Records of websites visited.
* Postings, downloads, and other internet activity.
* By using company-provided internet access, employees acknowledge and consent to such monitoring and review.

**SOCIAL MEDIA USE**

Social media platforms provide opportunities to engage in discussions, share information, and interact with others online through various formats, including text, video, audio, and photographs. While [EMPLOYER'S NAME] respects employees' rights to use social media, employees must do so responsibly to protect the company's interests and maintain focus on their job responsibilities.

Personal use of social media

[Choose the appropriate option based on company policy:]

* [Prohibited use: Personal use of social media is strictly forbidden during working hours or when using [EMPLOYER'S NAME]'s computers, networks, and IT resources.
* Limited use permitted: Occasional personal use of social media during working hours is allowed, provided it does not interfere with work responsibilities, involve inappropriate content, or violate this policy.]

Compliance with internet use guidelines

All social media activity must comply with the general internet use rules outlined in this policy, including avoiding:

* Sharing or accessing inappropriate, offensive, or discriminatory content.
* Activities that violate [EMPLOYER'S NAME]'s policies against harassment or discrimination.
* Using social media to share confidential, proprietary, or other protected company information.

Employees should exercise caution when posting about topics related to [EMPLOYER'S NAME] and ensure that their use of social media reflects professionalism and responsibility.

**TELEPHONE AND VOICEMAIL POLICY**

[EMPLOYER'S NAME] provides landline and/or mobile telephone access and voicemail systems to certain employees to facilitate their job duties. To ensure professional service and prevent misuse of company resources, telephone conversations and voicemail messages may be monitored, recorded, and reviewed without prior notice. Recorded messages may also be stored for a period of time and deleted periodically.

Personal use of telephones and emails

Employees are allowed occasional personal use of company telephones and voicemail systems, provided such use:

* Remains professional and appropriate.
* Does not interfere with work responsibilities or productivity.
* Does not involve commercial, religious, or political solicitation, or promotion of outside organizations.

Monitoring and consent

[EMPLOYER'S NAME] expressly reserves the right to monitor, record, and review all telephone conversations and voicemail messages—whether business-related or personal—without further notice. By using [EMPLOYER'S NAME]'s telephones or voicemail systems, employees acknowledge and consent to this monitoring and recording.

**INAPPROPRIATE USE OF IT RESOURCES AND COMMUNICATION SYSTEMS**

Employees are strictly prohibited from using [EMPLOYER'S NAME]'s IT resources and communication systems—including email, text messaging, internet access, social media, telephones, and voicemail—for any inappropriate or unlawful purposes. Examples of prohibited activities include, but are not limited to:

1. Misrepresentation: Impersonating another individual or entity.
2. Offensive content: Sending, posting, or encouraging messages or information containing sexual, racist, religious, or otherwise offensive material.
3. Unauthorized disclosure: Revealing [EMPLOYER'S NAME]'s proprietary, confidential, or intellectual property without proper authorization.
4. Illegal activities: Engaging in or soliciting activities that are unlawful.
5. Misrepresentation of opinions: Presenting personal opinions as those of [EMPLOYER'S NAME].
6. Disruption of work: Using resources in a way that interferes with your job performance or the work of others.
7. Policy violations: Engaging in any activity that conflicts with [EMPLOYER'S NAME]'s policies or practices.

Employees must ensure that their use of company resources aligns with professional, ethical, and lawful standards at all times.

**VIOLATION OF THIS POLICY**

Employees who fail to comply with any part of this policy will be subject to disciplinary action, which may include measures up to and including termination of employment.

**POLICY ADMINISTRATION**

The [DEPARTMENT NAME] department is responsible for overseeing and enforcing this policy. If you have any questions or require clarification regarding its contents, please reach out to the [Human Resources/Legal/DEPARTMENT NAME] department for assistance.

**APPLICABILITY TO COLLECTIVE BARGAINING AGREEMENTS**

The terms outlined in this policy are designed to complement, not replace, amend, or supplement, the terms and conditions of employment outlined in any collective bargaining agreement that applies to unionized employees at [EMPLOYER'S NAME].

Employees covered by a collective bargaining agreement should refer to its terms for guidance. Where this policy's terms differ from those in the applicable collective bargaining agreement, the agreement's terms will take precedence.

**ACKNOWLEDGEMENT OF RECEIPT AND REVIEW**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name), acknowledge that on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date), I received and reviewed a copy of [EMPLOYER'S NAME]’s [NAME OF POLICY]. I understand that it is my responsibility to familiarize myself with the policy and adhere to its terms.

I also acknowledge that this policy is not intended to create an employment contract or alter my at-will employment status, unless otherwise specified in a written agreement signed by an authorized representative of [EMPLOYER'S NAME]. Any delay or failure by [EMPLOYER'S NAME] to enforce the provisions of this policy does not constitute a waiver of its rights to enforce them in the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date