*NOTE:* *This policy is not mandated by New York City/State or Federal law, and reflects the operational preferences of the author only.*

**ELECTRONIC COMMUNICATIONS SYSTEMS**

Electronic communications systems include all computer networks, IT resources, access to the Internet, and all forms of electronic communications (including, but not limited to, email, phone and voice mail systems, facsimile machines including e-fax systems, printers, photocopiers, scanners, video conferencing, and social media posts) using computers, servers, phone systems and other data processing equipment owned by [Organization Name]. This policy also applies to electronic communications including but not limited to email, phone and voice mail systems, facsimile machines including e-fax systems, printer, photocopiers, scanners, video conferencing and social media posts made for or relating to [Organization Name] business usingemployee-owned equipment.

No Expectation of Privacy:

Electronic communications systems are [Organization Name] property and their purpose is to facilitate [Organization Name] business. Employees should have no expectation of privacy in any emails, files, data, documents, facsimiles, telephone conversations, voice mails, social media posts or messages, instant messages, or other communications or content created on, transmitted through, received on or printed from, or stored or recorded on the [Organization Name]’s electronic communications systems, including via the Internet. Communications and all content transmitted or stored in these systems, including any back-up copies, are the exclusive property of the [Organization Name] and [Organization Name], **in its sole discretion, reserves the right to monitor, access, intercept, retrieve, read, disclose, and/or delete any material on its electronic communications systems, whether employees utilize [Organization Name] owned devices or personal devices to access the [Organization Name] network or systems**. This may include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems, including Internet access, as well as keystroke capturing and other network monitoring technologies. [Organization Name] may exercise this right, despite the use of passwords or other security measures and without any further notice to the employee.

Appropriate Usage:

The Electronic communications systems -- including access to the Internet -- should be used only for job-related purposes. Occasional or incidental personal use is permissible so long as, in the [Organization Name]’s opinion, (1) it does not consume more than an insignificant amount of [Organization Name] resources and employee time; (2) it does not interfere with the employee’s responsibilities and productivity; (3) it does not preempt, interfere or conflict with any business-related activity; and (4) it does not preempt, interfere or conflict with existing employee standards of conduct or other policies set forth by [Organization Name] in its employee handbook or otherwise. Because personal use of the Internet affects the speed and effectiveness of the [Organization Name]’s computer systems, employees are specifically counseled to access the Internet for job-related purposes only.

The electronic communications systems should never be used for inappropriate purposes, or in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by Federal, state or local law (e.g., to send or receive sexually explicit or racially insensitive messages or to visit websites with sexually explicit content). All forms of electronic communications are subject to [Organization Name] policy against harassment. Anything that would be inappropriate to send in a non-electronic communication (e.g., by memo or letter) is similarly inappropriate if sent electronically (e.g., by email, telephone, text, instant message). Since electronic communications can be copied, forwarded, saved, intercepted and archived, employees should be careful about the words they use and the documents they transmit, as well as the Internet sites they access. Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, employees should exercise caution when forwarding electronic communications and must at all times comply with the confidentiality policy.

User Accountability:

Each employee is responsible for all actions performed on [Organization Name] electronic communications systems and other resources with the employee’s login credentials. To prevent unauthorized parties from obtaining access to electronic communications, employees should choose passwords that are difficult to guess (not a personal detail or reflection of work activities) and these should be changed regularly. Upon request, passwords must be disclosed to the employee's supervisor and the [Insert Title]. Employees should not reveal their individual passwords to other employees or anyone outside [Organization Name].

Remote Access:

[Organization Name] may provide equipment for remotely accessing the electronic communications systems, including computer hardware, software, phone lines and mobile devices, voicemail systems, connectivity to the network and other applicable equipment as deemed necessary. All [Organization Name] owned equipment provided for the purpose of remotely accessing the electronic communications systems should be used only for the purpose of facilitating [Organization Name] business and the employee assumes all responsibility for their appropriate use in accordance with this and other applicable [Organization Name] policies. Disabling a virus scanner or firewall on [Organization Name] provided equipment may be cause for discipline under this policy.

Security Breach Reporting:

It is the responsibility of every employee to report the loss or compromise of any confidential or proprietary information (e.g., confidential information has been improperly accessed or disclosed to an unauthorized recipient, or a device containing such information has been lost), any system disruptions (e.g., email outages), actual or suspected security breaches (e.g., unauthorized access of the email system, servers or networks), and unusual system behavior (e.g., missing files, frequent system crashes) that arise with [Organization Name] electronic communications systems. Any such incidents should promptly be reported to your supervisor and to [Insert Title].