For all employees of [Company Name] (ie: the “Company”) who have been approved for telecommuting (ie: “Remote Work From Home”), the following policies, which must be understood, acknowledged, agreed upon and adhered to, specify the conditions for performing work on a regular basis from a site other than our primary physical office location of [Company Office Address] (ie: the “office”).

**Telecommuting**

1. Work hours, meal and rest breaks, overtime compensation, and vacation schedules, shall conform to the Company’s personnel policies and wage and hour law. Requests to work overtime (non-exempt employees only), sick leave, vacation, or other leave must be approved by your manager in the same manner as when working at your regular work site.
2. Your duties and responsibilities remain the same as when working at the regular work site. Your manager, as always, reserves the right to assign work, as needed, including any assigned work that would be required to be completed at the office.
3. Employees who are working from home are expected to give notice to the facilitator of any scheduled in-person meeting if they intend to call into the meeting instead of attending it in the office. There is no such requirement for on-line meetings, and you are expected to attend meetings as invited, using conference calls, Microsoft Teams, Zoom, GoToMeeting or any other identified and approved virtual meeting service.
4. Recognizing that effective communication is essential for this arrangement to be successful, the following methods and times of communicating are agreed upon:
5. You are expected to provide an honest and accurate accounting of your time either by email to your supervisor or via the established Company software.
6. You are required to maintain regular communication by phone calls and e-mails at the same level as if you were in the office. Depending on your position, this may include periodic check-ins including at the start and end of each day as well as start and end of required lunches and breaks.
7. You are expected to respond timely to interoffice communications with the same level of responsiveness and professionalism as though you were working in the office.

5) You agree to remain accessible during designated work hours as if you were in the office.

6) Regarding space, equipment, furniture and/or supplies purchases, set-up and maintenance, the following is agreed upon, subject to potential reimbursement as set forth below:

1. Employees will provide their own office furniture and home office space. If the Company does not provide you a cellphone, laptop or desktop computer, you may use your own subject to the electronic use policy below. The Company’s IT group will provide you with technical support and maintenance of these items. If you need to purchase equipment (for example: connecting cables, a computer or a printer), those purchases must be necessary for you to perform your work from home and be pre-approved by your supervisor.
2. Personal equipment that is used to connect to the Company’s network and/or hosted computer systems must meet the technical requirements of company-owned equipment for remote access.
3. Personal equipment that is used to connect to the Company’s network and/or hosted computer systems must meet the cybersecurity control requirements of company-owned equipment used in the office.
4. It is expected that you will provide your own Internet service and phone service with sufficient internet speed to be able to perform your regular duties as though you were in the Company’s office.
5. It is expected that you will provide network security controls for your home Internet connection meeting the technical requirements of company-owned equipment for remote access.

7) You agree to maintain a safe and secure work environment. You further agree to hold the Company harmless for injury to others at your alternate work site. The Company will need, and you agree to provide, electronic and/or physical access to your telecommuting work site for purposes of assessing security requirements, proper operation and maintenance of Company-owned equipment and job performance.

You are solely responsible for ensuring the safety of your alternative work environment. However, because the Company is obligated to provide its employees with a workplace that is free from hazards that might cause serious harm or injury, the Company reserves the right to periodically inspect your remote-work space. Any such inspection will be preceded by advance notice and an appointment will be scheduled. Should you suffer an injury at home while engaging in Company business, you may be covered by the Company’s Workers’ Compensation insurance. As such, you are required to immediately report any work-related injuries that occur during working hours, regardless of location. You shall be liable for any injuries that occur to third parties at or around your alternative work environment and, of course, injuries that occur on your property or home while not engaged in Company work will not be a work injury, but may be covered under your homeowner’s or medical insurance policies.

1. You agree to use Company-owned equipment, records, and materials for purposes of Company business only, and to protect it against unauthorized or accidental access, use, modification, destruction, or disclosure. Further, you agree that no company information will be saved to unsecured personal devices. You must immediately, or as soon thereafter as practical, report to your manager instances of loss, damage, or unauthorized access at the earliest reasonable opportunity.
2. All equipment, records, and materials provided by the Company shall remain the property of the Company. All Company equipment will be returned to the Company for inspection, repair, replacement, or repossession as requested. This must happen as soon as practical upon request.
3. You understand that you are responsible for tax consequences, if any, of this arrangement, and for conformance to any local zoning regulations.
4. You understand that all your obligations, responsibilities, terms and conditions of employment with the Company remain unchanged, except those obligations and responsibilities specifically addressed in these policies.

**Computer, E-mail and Internet Usage**

When telecommuting, it is essential that you adhere to proper computer, e-mail and Internet usage in an appropriate, ethical and professional manner. In this regard, you must ensure that your home computer is safe and secure, and preferably used only by you, using our Company log-in. This policy outlines the guidelines for acceptable use of Employer’s technology systems.

1. *Confidentiality and Monitoring*

All technology provided to you by the Company, whether in your home or via the Company’s servers, including computer systems, communication networks, company-related work records and other information stored electronically, is the property of Company. In general, use of the Company’s technology systems and electronic communications should be job-related and not for personal convenience. The Company reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite. Internal and external e-mail, voice mail, text messages and other electronic communications are considered business records and may be subject to discovery in the event of litigation. All employees must be aware of this possibility when communicating electronically within and outside the Company.

1. *Appropriate Use*

You are expected to use technology responsibly and productively, as necessary, to perform your job. As if you were in the office, Internet access and e-mail use via the Company’s server is for job-related activities; however, minimal personal use is acceptable.

1. You may not use the Company Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual’s race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted.
2. Harassment of any kind is prohibited. Disparaging, abusive, profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail—are forbidden.
3. Copyrighted materials belonging to entities other than the Company may not be transmitted by you on the Company network without permission of the copyright holder.
4. You may not use the Company’s computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and spamming (sending unsolicited e-mail to thousands of users).
5. You are prohibited from downloading software or other program files or online services from the Internet without prior approval from your manager or IT. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into Company systems and networks.
6. You are responsible for the content of all text, audio, video or image files that you place or send over the Company’s Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Company's corporate identity is attached to all outgoing e-mail communications, which should reflect corporate values and appropriate workplace language and conduct.
7. While general access to the internet for recreational use by immediate household family on personal computers that have access to the Company’s computer systems is permitted, the employee is responsible to ensure the family member does not violate any policies, does not perform illegal activities, and does not access the Company’s computer systems in any way. The employee bears the responsibility for the consequences should the access be misused.

Note that violations of the foregoing rules will be grounds for disciplinary action, up to, and including, termination.

**Acknowledgement and Acceptance**

I have read, understand, and agree to this policy and its terms.

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

Employee Signature Date

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

Employee Name

**Appendix: A**

Technical Requirements for Remote Connectivity

1. An “always-on” internet connection of at least 10Mbps.
2. A physical firewall protecting your home network from the internet. MS-Windows Firewall is acceptable.
3. For all personal computers connecting to the Company’s on-premise and/or hosted computer systems:
   1. Minimum of MS-Windows 8.1
   2. MS-Windows patching that’s kept current and up-to-date.
   3. Business class Anti-virus protection that’s kept current and up-to-date.
   4. SSL-VPN connection into the Company’s on-premise computer systems.
   5. Dual-Factor Authentication setup for all remote connections into the Company’s on-premise and hosted computer systems.
   6. Installation of Company’s remote support agent.
4. All Wireless Access Points are configured to communicate using encryption only.

*Note that the Company reserves the right to change, adjust, or add to these requirements at any time.*