Computer/Network Usage Policy

The Company's computer systems (including VPN, internet and networks), electronic mail system and voicemail system are made available to employees for use in connection with Company business and in the course and scope of the performance of employee job duties. The internet, network, servers, hub, electronic mail, voicemail systems, computers, laptops, cameras, headsets, monitors, hardware and software are all Company property ("Computer Systems").

Employees do not have a personal privacy right in any matter created, sent or received from the Company's Computer Systems. The Company expressly reserves the right to access, inspect, monitor, copy, remove, delete and/or disclose any and all hardware, software, applications, documents, data, messages or other files generated, used or stored on the Company Computer Systems in its absolute discretion and without the employees' prior knowledge, consent or authorization.

While incidental personal use is permitted during non-working time, the Company's Computer Systems shall not be used for illegal or outside business activities or result in a violation of any Company policy. As noted, no right to privacy in such use exists and the Company reserves the right to monitor or record even such personal use.

The Company also reserves the right to service the systems as necessary. All system passwords and security codes must be made available to the Company upon request by the IT Manager.

The Company assumes no liability for the loss, damage, destruction, alteration, disclosure or misuse of any data or communication transmitted over or stored on Company Computer Systems. The Company accepts no responsibility or liability for the loss or non-delivery of any voicemails, emails, or other data stored on Company Computer Systems.

Use of the Computer Systems must comply with the law and Company policy. Use should not involve words, images or references that would arguably violate any policies contained in this Handbook. Moreover, the Company's Computer Systems may NOT be used to post or transmit any disparaging messages or content about the Company or to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. For example, eliciting or requesting emails be received on Company email accounts (for example, by using your Company email to sign up for e-mail updates or "alerts" for an online retailer you use for personal shopping) is strictly prohibited. Notwithstanding, the foregoing is not intended to restrict statutory employee rights under the National Labor Relations Act to discuss with others terms and conditions of employment.

For security reasons, employees shall always log off of the network prior to leaving Company premises and shall never share their passwords with anyone other than authorized members of the Company's IT Department.

Potential dangers exist in accepting or opening data or files from unknown internet or email sources. Be alert to the potential dangers of accepting programs from public sources such as bulletin boards and conferences, or unsolicited emails. Do not open or execute a file or attachment if you are uncertain of expected results or do not know the source of the file or attachment.

Employee-users are prohibited from downloading any-non work productivity content from the internet or from external drives without prior written approval of the Company's IT Manager. Downloading of games or other applications is prohibited. Downloading of any executable files or programs, which change the configuration of the computer system, is prohibited. The employee-user should take extreme caution when downloading files from the internet. 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 and/or unauthorized entry into the Company's network.

If the employee finds that any damage occurred as a result of downloading files, the incident must be reported immediately to your supervisor. The intentional introduction of any virus-containing program or code is grounds for immediate termination, and may be grounds for criminal action. Any employee receiving a prompt or message stating that the Company software system has detected a potential virus must contact the IT Department immediately.

When downloading materials from the internet, most information is subject to copyright or other intellectual property right protection. Therefore, nothing may be copied or downloaded from the internet for use within the Company unless express permission to do so is stated by the material owner. Similarly, the Company's electronic mail system may not be used to send (upload) or receive (download) copyrighted materials or Company confidential information (as defined in this handbook) without prior written authorization from the Company's IT Department.

The Company purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Employees may only use software on local area networks or on multiple machines according to the software license agreement. The Company prohibits the illegal duplication of software and its related documentation to personal laptops or devices. Downloading of music, movies, images, etc. from the internet is not allowed.

When uploading materials to the internet, ensure that any Company copyrighted documents transferred via the internet clearly indicate our Company as holder of the copyright.

Materials distributed over the internet in the form of shareware or freeware, often come with express requirements or limitations attached (for example, not to be used for commercial purposes; cannot charge others for use or distribution; subject to a copyright or attribution notice being affixed to each copy, must distribute source code, etc.) If there are such terms applied, you must read and understand them before downloading the software, and make a copy of the terms if possible. If you think that the Company will not be able to comply with any part of the terms, do not download the material. Any time you are unsure about the meaning of the restrictive language or have questions about it, you should contact your supervisor to review it before downloading or using the material.

Employees must seek assistance and approval from their supervisor before incorporating anything downloaded from the internet (or any external online service) into material the Company intends to distribute externally.

Prior to or upon separation of employment, no employee shall print, forward, transmit or remove any information whatsoever from the Company's Computer Systems, without written permission from management. Also, upon separation of employment, all Company-provided phones, computers and other equipment must be returned. Once the device is returned to IT, all data on the device will be erased. Employees are not permitted to forward to themselves or otherwise save or print any the Company data, including emails, business contacts, customer lists, or other information. If you do not return the device to the IT Department prior to leaving on your last day, the Company reserves the right to electronically "cleanse" your mobile device, which will remove all data from the phone. Failure to return the device when required to do so may have additional legal consequences.

Employees who violate this policy may be subject to disciplinary action, up to and including, termination of employment. If you have any questions about this policy, please contact your supervisor or the IT Manager.