SAMPLE COMPUTER USAGE POLICY

If used properly, electronic communication services and devices like computers, voicemail, Internet, and e-mail can make a more efficient and productive work environment. The e-mail, computer, Internet and voice-mail systems are [Company] property. Personal use by an employee is prohibited while the employee is on working time. [Company] may intercept, monitor, copy, review and download any communications or files employees create or maintain on these systems. When using the Internet, do not send materials of a sensitive or confidential nature unless the information is properly coded to prevent interception by third parties.

An employee’s communications and use of the [Company] e-mail, computer, Internet and voice-mail systems will be held to the same standard as all other business communications, including compliance with the Company’s discrimination and harassment policies. Employees are expected to use good judgment in their use of [Company]’s system. Management should be notified of unsolicited, offensive materials received by any employee on any of these systems.

Furthermore, an employee’s consent and compliance with e-mail, computer, Internet and voice-mail policies is a term and condition of employment. Failure to abide by these rules or to consent to any interception, monitoring, copying, reviewing and downloading of any communications or files is grounds for discipline, up to and including discharge.

In order to ensure proper use, a few basic rules must be observed:

1. All electronic communication services and devices provided by [Company] must not be used for games, harassment, or offensive messages. Use of such services and devices by an employee on working time for solicitation and other non-business related reasons is not acceptable.

2. [Company] reserves the right to monitor and/or search any part of its computer or communications resources at any time and for any reason. For this reason, employees should not consider things like computer discs, computer programs, computer journal entries, e-mail, voicemail or any other electronic communication to be private.

3. Passwords for accessing the Company’s computer resources (the network login) must not be shared with any other person, including a supervisor or manager. Password changes will be required by the network server every 60 days. Password protecting documents or spreadsheets may only be done with management approval.

4. Because of the danger of computer viruses, employees may not use any personal removable media on computers and other such equipment without the consent of a supervisor or manager.

5. Information brought into such services and devices through the Internet or other communications networks is proprietary and confidential. Employees may not copy, transfer, transmit, or otherwise share such information without the consent of a supervisor or manager.
6. Information on individual PCs is not backed up. As a result, critical documents and spreadsheets must not be stored on individual PC hard drives. (Note: There may be some instances in which storing information locally is required by a software package. Special procedures will be taken in these cases.) Each person has a special, secure area on the network file server, designated as their \( U:\) drive or Users directory, where all information not needed by others should be stored. Shared information, which others may need to access, must be stored under shared areas of the network, such as the \( N:\) drive on the network file server.

7. Transmission of sexually explicit pictures, jokes, or material is strictly prohibited as is the visiting of inappropriate websites.