Sample Computer and Electronic Devices Usage Policy

_____ (the "Organization") provides a variety of electronic communications systems for use in carrying out its business. All communication and information transmitted by, received from or stored in these systems are the property of the Organization and, as such, are intended to be used for job-related purposes.

Employees are required to acknowledge this Policy before receiving access to the various systems in use at the Organization. The following summary guidelines regarding access to and disclosure of data on any Organization electronic communication system will help you better determine how to use these systems in light of your own and the Organization's privacy and security concerns.

Acceptable Use of Organization Systems and Monitoring: The Organization provides the electronic communication systems, Internet access, network access, personal computers, electronic mail, phones, voice-mail, software applications and other communications devices and methods for your use on Organization business. Whether accessed on-site or remotely, employees are expected to use these systems for Organization business in a productive and businesslike manner. Limited personal use is permitted to the extent that it does not interfere with the employee's job performance, Organization resources, and is consistent with the rules related to use of Organization systems and property. The Organization may access and disclose all data, messages, and information stored on or transmitted through its systems or sent or made over its electronic communications system. The Organization reserves the right to monitor communication and data at any time, with or without notice, to ensure that Organization property is being used for business purposes. The Organization also reserves the right to disclose the contents of messages for any purpose at its sole discretion.

Retrieval: Notwithstanding the Organization's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so.

Message Content: All e-mail must identify the sender. E-mails may not be sent anonymously. The e-mail and voice-mail systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. The systems are not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability. The Organization's overall employee manual or code of conduct shall apply in the event of possible misuse or misconduct.

Employees should note that any data and information on the Organization electronic systems is the property of the Organization. As a result, information saved, stored, or transmitted on or through the Organization's systems is not private and no employee should have an expectation of privacy in any information on the Organization systems. Accordingly, no employee should use the Organization electronic systems to send, receive, or store any messages or documents that they wish to keep private.

In addition, the e-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

Legal Proceedings: Information sent by employees via the electronic mail system may be used in legal proceedings. Electronic mail messages are considered written communications and are potentially the subject of subpoena in litigation. The Organization may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process and will fulfill any legal obligations to third parties.

Confidential Information and Data Security: The Organization's policies regarding use and disclosure or confidential and proprietary information apply to the use of any electronic communication system. The Organization does not permit the transfer of Organization data to employees' non-Organization personal accounts, electronic devices, USBs, thumb drives, portable hard drives, or any other data storage devices or media without authorization by the Organization. In the event that the Organization discovers such unauthorized transfers, the Organization will require that all Organization data be deleted from any non-Organization devices or accounts. The Organization may require third-party verification, acceptable to the Organization, that the Organization data has been properly deleted. Appropriate disciplinary action may occur as the result of unauthorized data transfers.

Physical Security: Access to computers and computer equipment, including, but not limited to, server rooms, will be limited to employees who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive should be secured in a locked room or office during non-business hours. Equipment that is to be removed from Organization property must be approved in advance with the IT department and an inventory of this equipment maintained by IT. All equipment removal from the premises by an individual must be documented, including the makes, manufacturers and serial numbers on an IT supplied form, and a copy of this form shall be filed in the employee's HR folder. If the employee leaves the organization, the employee must return the equipment to the Organization prior to the last day of employment.

Network Security: IT will monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected. IT will also implement and maintain procedures to provide adequate protection from intrusion into the Organization's computer systems from external sources. No computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network. Employees should not store personal, business, member or other credit card/account information, or passwords within word processing or other data documents.

Personal Computer Security: Only legally licensed software will be installed on the Organization computers. Users are expected to read, understand and conform to the license requirements of any software product(s) they use or install. Software cannot be copied or installed without the permission or involvement of the IT department. IT will configure all workstations with virus protection software, which should not be removed or disabled. Each employee is responsible for protecting their computer against virus attack by following IT guidelines for scanning all incoming communications and media, and by not disabling the anti-virus application installed on their workstation. All data disks and files entering or leaving the Organization should be scanned for viruses. All employees will log out of the

network and turn their computers off before leaving the office at night. Employees should log off of the network when they will be away from their desk for an extended period.

Backup Procedures: In the event a PC must be replaced or re-imaged. The IT department will only attempt to back up the My Documents folder of the PC. Data stored in any other folder will not be backed up. Employees working on especially crucial information is encouraged to backup these projects to external disks. Computer users will be responsible for ensuring that the data stored on their local machines is backed up as required by the owner.

Access to Organization Computers: The Organization will provide computer accounts to employees who require such access to perform the functions of their jobs. Employees are not permitted to access systems beyond their specific level of authorization.

Network Use: The Organization network is to be used for business purposes only. Employees with Internet access are expressly prohibited from accessing, viewing, downloading, or printing pornographic or other sexually explicit materials. In addition, Employees should be mindful that there is no assurance that e-mail texts and attachments sent within the Organization and on the Internet will not be seen, accessed or intercepted by unauthorized parties.

Software Usage: Employees are expected to use the standard software provided by IT, or identify applications they need in the course of their work. Employees are permitted to download applications, demos or upgrades at their own risk. Employees are strictly prohibited from downloading and installing file sharing programs. Employees will use the standard e-mail system provided by the Organization for official e-mail communications, and should not install their own e-mail systems.

Return of property upon termination**:** All Organization property, including the electronic systems, User IDs and passwords, must be returned to the Organization when your employment is terminated. Organization policy does not permit the transfer of Organization data to employees' non-Organization personal accounts or electronic devices. In the event that the Organization discovers such unauthorized transfers after employment ends, the Organization will require that all Organization data be deleted from any non-Organization devices or accounts. When a data transfer is discovered after employment has ended, the Organization will require third-party verification, acceptable to the Organization, that the Organization data has been properly deleted.

Failure to comply with the Computer and Electronic Systems Usage Policy may result in disciplinary action up to and including termination of employment. Any employee who does not understand any part of the policy is responsible for obtaining clarification from his or her manager or the IT department.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

COMPUTER AND ELECTRONIC DEVICES USAGE POLICY

ACKNOWLEDGMENT

Employee Name: _____

Employee Position: _____

Date of Receipt of Computer and Electronic Devices Usage Policy:

I acknowledge and agree that:

(1) I have received a copy of the Company Computer and Electronic Devices Usage Policy;

(2) I have read the Computer and Electronic Devices Usage Policy in its entirety and fully understand the provisions contained therein; and

(3) I agree to abide by the provisions contained in the Computer and Electronic Devices Usage Policy.

_____
Employee's Signature

_____
Employee's Name (Printed)

_____
Date