# E 220 - INFORMATION SYSTEMS POLICY

Employee Quick Reference:

Passwords must be protected and remain confidential to other employees and those outside the company.

If you have been granted access from home or remote locations, you must protect access of the company systems from access by others who may have access to the computer(s) from which you access the company Systems.

You must protect all company owned Software and Data from all unauthorized use.

Do not download any applications or data to a company computer or system without obtaining prior authorization from the IT Manager (no exceptions).

Personally owned equipment such as smart phones, tablets, and computers may only be used for company business with prior authorization from IT Manager (no exceptions).

Only use company email for business use.

Only use the company's internet connection for appropriate use. The company allows employees to check their personal email via the company internet connection and using a company computer and internet browser during the business day, but this privilege is not to be abused.

All employees who have access or use the company's computer systems, must sign the INFORMATION SYSTEMS POLICY.

INFORMATION SYSTEMS POLICY

**Policy:**

It is the policy of the Company Inc. that all computer equipment, software, data, and generated output produced or stored are valuable assets of the Company and that all verbal and written procedures safeguarding these assets be followed. Furthermore, it is the Company's policy to strictly comply with all laws, including all software license agreements and copyright privileges of software developers. A license is generally required for all computer software programs obtained from third parties. The unlicensed or unauthorized duplication or use of any software program or company data is illegal and will not be tolerated.

Computer equipment, is defined as any piece of equipment designed to input, display, store, calculate or output information. This includes all computer hardware, tablets, smart phones, local area network devices and data cabling. Also included is the company's telephone system including its ancillary tools such as voice mail and messaging. Computer software, for the purposes of this policy, refers to all applications and data, including electronic mail (E-mail) stored on any piece of computer equipment including personal computers, tablets, smart phones, network servers, fixed disk drives, CD's , DVD's, flash drives, third party 'cloud' services (including apple i-cloud), company owned or managed websites, or other media. Also included under this policy is any company correspondence and company related data that may be stored on personally owned devices.

It is the objective of management to ensure that efficient, secure and cost-effective approaches are employed by all personnel in addressing the company's information processing needs. These approaches shall be coordinated within the Company to ensure that overall long range information processing needs are met, that redundant efforts are avoided, and to the extent possible, hardware and software approaches are compatible and in adherence with applicable and ever evolving standards.

**Procedure:**

Employees are not to remove desktop computers, printers, or other associated hardware, software, from the company facilities, equipment, or storage resources without knowledge and explicit permission of the designated IT Administrator.

Data, including email, is not to be removed or copied from any company provided or controlled storage source and placed on any non-company controlled storage media, including personally owned computers, tablets, telephones, smart phones, storage media, or internet locations without the knowledge and approval of the designated IT

Administrator. Employees are not authorized to establish any outside data storage resources, including "cloud" storage sites, intended to host company data without the knowledge and approval of the designated IT Administrator. Examples can include but are not limited to; iCloud, Facebook, Dropbox, Google Drive, and One Drive.

Employees are not to make copies of any licensed program except for backup purposes. This includes copies for other employees in the same department, in another department, in another part of the Company, or for personal use. All software purchased by or developed by the Company will remain the property of the Company. It is strictly forbidden for any employee to install software from any source onto Company provided equipment, network, or website without approval of the designated IT Administrator. This includes any application, utility, game or other program including screen savers not included with the operating system. All files must be scanned for computer viruses by an authorized method before being transferred to Company computers or networks. The intentional introduction of a computer virus, Trojan horse or other such malicious code is prohibited. Any such actions described above, or other "hacking" methods used on Bryant Group equipment, is subject to legal action.

Employees may be allowed to access the company network and systems from their home or other remote (non-company controlled) location using personally owned equipment. Such access is granted on a case by case basis and subject to all specifications of this policy as well as all safeguards and controls as may additionally be specified by the IT Administrator. No programs or data is to be stored on a non-company device without knowledge and approval off the designated IT Administrator. This restriction specifically applies to remote access of all email flowing through the company email systems, including both the "bryantgroupinc.net" or "bryant-group.com" domains.

As it is the policy of the Company that all computer equipment, software and data are valuable assets, the company maintains the right to access data maintained on all company owned computer equipment and data storage environments. This includes data stored on the company network, on local fixed disk drives, tablets, phones, smartphones, CD's, DVD's, flash drives, i-cloud, web sites, cloud services, or other media. The company reserves the right to monitor/audit use of its computer & communications equipment, applications, files, data and services to ensure that its policies are being followed and that resources are being used appropriately. Under no circumstances may an employee open or modify any computer equipment without the approval of the designated IT Administrator. Any damages to company computer equipment by an employee attempting such unauthorized modifications are the financial responsibility of the employee.

Use of E-mail, the Internet and the Intranet are privileges and are to be used only for business purposes of the Company. E-mail messages are not private and employees should gauge their usage accordingly. The Company will take reasonable action to prevent the unauthorized interception or alteration of E-mail messages, however, the

complete reliability or privacy of E-mail traffic cannot be guaranteed. The Company reserves the right to monitor E-mail messages to assure compliance with all of its policies. Sending or receiving messages, or downloading files that are of a nature that potentially could be construed as discriminatory, racist, sexist, solicitous, defamatory, insulting, romantic, pornographic, breaches of confidentiality or in violation of the Company's harassment policies are strictly forbidden. Subscription to any mailing lists is not permitted without advance approval from the designated IT Administrator.

Employees are required to maintain all systems security measures as are implemented at any time by the Company. Passwords for all company controlled systems, web-sites, or applications are not to be shared with anyone other than an employees' direct supervisor or a member of the designated IT staff / IT support contractor. If there is a question as to the appropriateness of sharing any system or data access instructions or information, including a password, employees shall immediately contact the designated IT Administrator for clarification.

Any violation of this policy may result in disciplinary action and be subject to discharge.

_____

Print Employee's Name

_____

Employee's Signature Date