Acceptable Use of Technology Policy

Purpose

The purpose of this policy is to outline BOWEN's expectations regarding the acceptable use of computer technology and systems. This policy is in place to protect employees and contractors and ensures that company and client technology resources are used appropriately for business purposes, in the course of normal operations.

Guidelines

Computer-based technology and internet systems at BOWEN and our clients' worksites are to be used for company business only. All business information and correspondence, including email, transmitted or received using computer-based technology is considered to be the business property of the company that our employees and contractors work at and is to be managed accordingly for business-related matters.

Client Policies

Internet access is administered under the client technology policies. Employees and contractors working at our clients' worksites must make sure that they are familiar with these policies.

Systems Security

Internet and network accounts are to be accessed only by assigned users for legitimate business purposes. Passwords may not be shared with other users or third parties. Employees and contractors are not permitted to obtain anyone else's account password. If a user has reason to believe that his/her password has been compromised, the user must inform the Information Systems (IS) department at his/her worksite immediately.

Internet and organizational network users must comply with the following security guidelines, rules, and regulations:

1. Personal files or data downloaded from the internet may not be stored on corporate hard drives or network servers.
2. Video and sound files must not be downloaded from the internet unless their use has been authorized for the purposes of conducting business.
3. Users must refrain from any online practices or procedures that would expose the network or resources to virus attacks, spyware, adware, malware, or hackers.
4. Employees and contractors using the internet must conduct themselves in a professional manner at all times, especially while participating in collaborative activities, and must not disclose BOWEN or our clients' confidential information or intellectual capital to unauthorized third parties.
5. Business information should not be sent to personal accounts. This includes, but is not limited to, email, online storage or social media accounts, without the prior written consent of BOWEN or the client.
6. Business information should not be stored on personal devices without prior authorization by BOWEN or the client. Any such authorized information must be kept secure and confidential at all times. Upon completion of employment/contract the information must be returned or destroyed as per BOWEN or client requirements.

Internet Use

Employees and BOWEN contractors may use the internet only to complete their job duties, under the purview of BOWEN or our clients' business objectives.

Unacceptable Use of the Internet

Inappropriate and unacceptable network and internet use includes, but is not limited to:

1. Usage for illegal purposes, such as theft, fraud, slander, libel, defamation of character, harassment (sexual and non-sexual), stalking, identity theft, online gambling, spreading viruses, spamming, impersonation, intimidation, and plagiarism/copyright infringement.
2. Any usage that conflicts with existing policies at BOWEN or our clients (e.g. bandwidth limitations, network storage, etc.) and/or any usage that conflicts with the mission, goals, and reputation of BOWEN and our clients.

3. Copying, destroying, altering any data, documentation, or other information that belongs to BOWEN, our clients, or any other business entity without authorization.
4. Engaging in any other activity which would in any way bring discredit, disrepute, or litigation upon BOWEN and our clients.
5. Engaging in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.
6. Engaging in any activity that could compromise the security of host servers or computers at BOWEN or our clients' worksites.
7. Engaging in any fundraising activity, endorsing any products or services, or participating in any political activity, unless authorized to do so as part of completing one's assigned job duties and responsibilities.
8. Allowing unauthorized or third parties to access BOWEN or our clients' network and resources.

Email

Email communications at BOWEN and our clients must be conducted with respect and should be created with professionalism and attention to detail.

Social Networking Sites and Blogs

Unless in direct support of the employee/contractor's assigned duties, the use of social networking sites (e.g. Facebook, My Space, Friendster, etc.) and personal Blogs / Twitter have been deemed an unacceptable use of personal internet at BOWEN. The use of these sites during paid work hours is prohibited.

The use of social networking sites via client networks is dictated by the client's technology policy.

The abuse of personal internet use on these sites using either corporate-owned and operated equipment or personal internet access devices during paid working hours is subject to disciplinary action. Employees and contractors that use these sites during their personal time are prohibited from disseminating any BOWEN or client private organizational information therein, or any negative comments regarding the organizations.

Employee/Contractor-Owned Property

BOWEN and our clients recognize the importance of having convenient access to corporate data (emails, calendar, contacts, etc.) on personal devices such as smart phones and tablets. In the event that a BOWEN employee or contractor creates, stores or transmits business information on personally-owned property (including, but not limited to: laptop computers, desk-top computers, mobile telephones, BlackBerry devices, memory cards, notebooks, PDAs, or loose-leaf paper, etc.), the business information remains the express property of BOWEN or our clients.

BOWEN and our clients do not accept responsibility for any loss or damage suffered by employees or contractors as a result of employees or contractors using BOWEN or our clients' internet connection for personal use.

BOWEN and our clients reserve the right to inspect and/or audit the property of employees and contractors on BOWEN or our clients' premises, where it is either known that they use personally-owned property for the purposes of conducting business, or where it is reasonably suspected that such properties contain business information. BOWEN or our clients also retain the right to remotely reset (wipe) your device to factory default settings in order to remove confidential and/or proprietary information from your device. These inspections, audits and practices are not intended as a punitive measure, and are employed only for the protection of the business interests of BOWEN or our clients.

Should one of the following events occur with your personal device containing corporate data, notify the IS team:

- Lost or stolen – you must report this to the IS team immediately
- You plan to discard or recycle your device
- Another individual will become the primary user of your device
- You are leaving your position
- Any other event that would put BOWEN or our clients' confidential information at risk

Cellular Phones at Work

- Employees and contractors are encouraged to use their non-paid time to make or receive personal calls and should keep personal calls to a minimum during paid work time.
- BOWEN and our clients strictly prohibits the use of cellular phones or similar devices while at any work site at which the operation of such device would be a distraction to the user and/or could create an unsafe work environment. Such work sites must be secured or the device used only by an employee who is out of harm's way at such work environments.

- BOWEN and our clients strictly prohibit the use of mobile phones, and PDA's while operating company-owned and operated vehicles, or while operating a vehicle on business. The use of hands-free mobile phones is also discouraged during work hours. Employees and contractors are solely responsible for any fines and/or charges laid by the authorities for illegal use of a phone or PDA while operating a vehicle at any time.
- BOWEN and our clients are not liable for the loss of personal cellular phones brought into the workplace.

Client, Visitor and Employee Privacy

The following measures have been adopted to ensure the ongoing privacy of our clients, visitors, employees and contractors:

- BOWEN employees and contractors are strictly prohibited from posting sensitive, libelous, incendiary or personal information regarding our clients, visitors and employees/contractors on the company intranet, social networking sites and/or the internet in general.
- BOWEN employees and contractors are strictly prohibited from taking photographs of clients, visitors, employees or contractors on BOWEN or our clients' premises for either personal or professional reasons, unless they have received prior authorization to do so.
- BOWEN employees and contractors are strictly prohibited from posting photographs of other employees, contractors, clients or visitors on the internet, unless authorized to do so.

Accessing & Monitoring Usage Records

BOWEN and our clients reserve the right to monitor, access, retrieve, read, and disclose, at any time, any electronic communication, data or other similar material related to the use of company email and internet systems by staff working at their sites. BOWEN and our clients also have the right to monitor and log any and all aspects of its electronic systems including, but not limited to, monitoring internet sites visited, chat and newsgroups, file downloads, and call communications sent and received by staff working at their sites via company systems.

BOWEN and our clients will do their best to accommodate employee privacy while being diligent and thorough when conducting investigations regarding company email and internet usage.

Upon Resignation, Layoff or Termination

Upon resignation, layoff or termination of employment or contract with BOWEN or our clients, employees and contractors are required to promptly return any and all equipment and material pertaining to BOWEN or our clients' business in their possession.

In the event that a device containing business information is password-protected, the employee will be required to provide the correct user name and password for the device.

Any personal computing device which has been set up to connect to BOWEN or client networks may be remotely reset.

Disciplinary Action

Any violation of this policy will be treated like violations of other BOWEN or our clients' policies. Any and all misconduct will be addressed according to established procedures. Violations of this policy may result in one or more of the following:

1. Temporary or permanent revoking of access to corporate internet resources and/or other IS resources;
2. Temporary or permanent revoking of corporate devices; and/or
3. Disciplinary action according to applicable corporate policies, up to and including suspension or termination of contract or employment.

Published Oct. 1, 2016