## Communication and Software Systems

### Electronic Communications Systems

**[Organization Name]** provides electronic communication systems to maintain superior communications both within the organization and with outside clients and vendors. You are encouraged to learn about these tools and how to use them. This policy provides directions for you regarding access and disclosure of information when using these communication systems. All employees and others outside the organization who may use the systems are expected to be aware of and support this policy.

Our electronic communication systems include computers, software, electronic mail (e-mail), copiers, fax machines, telephones, cell phones, voice mail, messengers, and various online services. All of these systems are operated and managed based upon this policy.

These systems and any other informational, storage, or retrieval services that the organization provides are organization tools and are to be used for business purposes only during business hours. Use of company systems during business hours for other than work-related purposes should be minimal and must not impact business operations.

The use of these systems is not private or confidential. Within the bounds of current and future laws, the organization reserves and intends to exercise the right to review, audit, intercept, access, and search these business systems at will, monitor data and messages within them at any time and for any reason, and disclose selected contents without notice or other restrictions. Messages sent through these systems remain the property of the organization.

As an employee, you must not permit any proprietary or confidential information of **[Organization Name]** to enter the public domain through electronic transmissions. Examples of the organization’s proprietary and confidential information are provided in the Confidentiality Policy. Also, these systems shall not be used to receive or distribute copyrighted materials, trade secrets, proprietary information, or similar materials from/to outside the organization without prior authorization.

Any messages or communications used through this system are subject to our anti-harassment, anti-discrimination, and non-solicitation policies. You are expected to carefully compose and review the wording, tone, and content of your communications before transmission.

You should check with your supervisor if you have any questions about the proper use of communication or software systems. All system users who discover violations of this policy are expected to notify their supervisors or managers immediately. Improper use or violation of this policy can result in corrective action, up to and including termination.

### Electronic Mail System

You are reminded to be courteous to other users of the e-mail system and to always conduct yourself in a professional manner. E-mail messages are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. You should write e-mail communications with no less care, judgment, and responsibility than you would use for letters or internal memoranda written on organizational letterhead.

You should know that even when a message is erased through e-mail, it is still possible to retrieve and read that message. Even though the organization reserves the right to retrieve and read any e-mail messages, those messages are to be treated as confidential by other employees and accessed only by the intended recipient. We expect employees to respect others’ privacy and not retrieve or read electronic messages for which they are not the intended recipient unless authorized. The use of passwords for security does not guarantee confidentiality; all passwords to company systems must be disclosed to the organization's **[Designated Position]**.

### Organization-owned Personal Computers

To protect the integrity of our systems, all software used on our computers must be registered with the **[Designated Position]**. Personal or downloaded software may only be installed after written authorization from that individual. A virus check of all such software must be made immediately before it is installed on any organization computer. A virus check must also be conducted on any electronic devices originating from or used on any computer outside of the organization prior to its use with an organization-owned computer. The copy or transfer of organization-owned software may occur only with the written authorization of **[Designated Position]**.

### Laptop Security

All staff that are issued laptops and other computer-related equipment will be given a copy of **[Organization Name]**’s computer-related equipment guidelines. These guidelines include security precautions and procedures as recommended by **[Organization Name]**.

Laptops and other applicable equipment will only be replaced by the company if the laptop and other equipment were secured by two anti-theft devices at the time they were stolen. For example, a computer camera stored in a locked cabinet within a locked office; a laptop locked in a safe in a locked motel room; a laptop secured in a locked drawer within a locked residence. An exception applies for a laptop or equipment taken during an assault situation.

In other situations, a deductible will apply to lost or stolen laptops and computer equipment. Employees should always follow company guidelines in safeguarding equipment. If an employee has followed these recommendations, the laptop and other equipment will be replaced. If the employee has not, however, the **[Designated Position]** has the option of paying the deductible or, for example, having the laptop replaced with a personal computer.

Mobile Devices

Allowing Remote Wipe Provisions/Data Liability

If you are connected to the organization’s server, understand that making this connection via a mobile device may compromise the privacy of certain sensitive information. Confidential electronic information, including personally identifiable information**,** must be protected to prevent it from being exposed if the device on which the information was accessed is lost or stolen. In order to protect this information, the organization retains the right to delete data and applications from any device that contains the organization’s information. ***This right to delete such information may be exercised remotely or on-site if the organization determines such action is necessary to protect confidential, sensitive, or proprietary information. Please understand that in downloading any such information to a personal mobile device, you are consenting to the organization’s ability to delete this information at any time*.** This policy covers mobile devices such as smart phones, tablets, laptops, and any similar devices. Please ensure that you regularly sync any personal data [*e.g.*, applications, information, photos] to another device/computer for safekeeping, as the wipe command does not differentiate between business and personal information.

Mobile devices should be set to lock after every **[two [2], five [5], ten [10], or other designation]** minutes for security reasons. A PIN-based lockout is required, and the PIN must be given to the Information Technology department.

Obviously, it is critical that any loss or theft of a mobile device, including laptops, be immediately reported to **[Designated Position]**. Security of these devices should always include two (2) levels (*i.e.*, locked in a trunk if kept in a car; locked in a hotel safe, not left out in a hotel room; etc.) of safeguarding. Failure to ensure this minimum level of protection may leave an employee responsible for the cost of the device or loss of company-related information addressed in this policy, and further corrective action, up to and including termination.

### Use of Internet, Virtual Private Network, and Commercial Online Systems

Although **[Organization Name]** recognizes that the Internet may have useful applications to our business, you may not engage in Internet use without prior written approval from **[Designated Position]** and unless a specific business purpose requires such use. Absent such approval, you may not access the Internet using our computer systems at any time or for any reason.

Also, management approval is required before anyone can post any information on commercial online systems, the VPN, or the Internet. Any material not owned by **[Organization Name]** that will be posted must have received all proper copyright and trademark permissions from its originators prior to approval. For newly generated material, an employee should obtain copyright and trademark designations, as appropriate, prior to posting any content; the posted content should include copyright and trademark notices. Absent prior approval to act as our official representative from **[Organization Name]**, you must include the following disclaimer with any information you post: “Views expressed by the author do not necessarily represent those of **[Organization Name]**.”

### Social Media and Networking

Social networking websites and online communities, such as Twitter, LinkedIn, Facebook, and Flickr are increasingly used and can be accessed by individuals not only from computer systems, but also from smart phones. These tools have value because they can be used to market **[Organization Name]** products and share information; employees may also use these systems as a quick communications and networking tool to complete projects. It is not the intent of this policy to unduly limit employees’ access to these conduits, however, guidelines and expectations surrounding their use are necessary as there are liabilities inherent in such use. When any employee is using organization-provided computers or cell phones or is representing the organization via social networking activity, that individual is expected to represent the organization in a professional and positive light. **[Organization Name]** wishes to use social networking exclusively to its advantage, preventing and minimizing any negative outcomes. This includes ensuring that all employees will be free from harassment and unprofessional behavior when utilizing or consuming social media; therefore, employees authorized for its use must abide by all applicable laws [including copyright] and ethical considerations.

### Business Use

Employees may use social networking websites to conduct organizational business, as long as such use is authorized and complies with the organization’s policies. Company logos or other organizational information must conform to pre-approved marketing concepts and standards. We do not endorse making business references on behalf of others on sites such as LinkedIn.

### Ownership of Social Media Accounts

***NOTE: While many employers do not have an interest in “owning” the social media accounts of employees, there may be situations where such ownership/control may be important in protecting the information and reputation of the organization. In such cases, language such as the following should be utilized to evidence such ownership intent.***

In the case that a social media account is set up for business purposes, the organization has the right to review, edit, and delete content associated with the account. The organization will have access to information associated with the account such as the username and password, and any content associated with the account will be considered the property of the organization. If an employee separates from **[Organization Name]**, the organization has the right to assume control of this account.

### Monitoring

While the organization does not routinely monitor social networking sites, other employers, organizations, and individuals do monitor and share information found on social networking websites. Again, posted information is public information.

### Protection

Social networking sites collect profile information for advertising opportunities and criminal reasons. Phishing (e-mail messages asking for username and passwords, etc.) and spamming are two downsides. Never click on links asking for personal or confidential information. Heed security warnings and pop-ups. Use of these sites may mean more SPAM sent to your e-mail account. If possible, disable the ability of others to post HTML comments to your home page. When accessing these sites, use caution when you see a posting or link that looks suspicious; when in doubt, delete it. Viruses and spyware may damage the organization’s operating system, compromise data, or expose your privacy and that of others you communicate with via e-mail and social media sites.

Be aware that others may piece together personal information for identity theft purposes. Be prudent in making comments or posts which reveal your or others’ travel plans or divulge other safety-sensitive and private information.

### Prohibited Conduct

Behavior and judgment in an electronic environment should mimic behavior in a physical setting. Employees are expressly prohibited from posting content that is malicious, abusive, threatening, intimidating, coercing, profane, disruptive, discriminatory, or harassing. Defamatory statements are prohibited and employees should be aware they are personally responsible for the legal consequences of such statements.

Nothing in this policy should be interpreted as limiting an employee’s right to engage in legally protected speech or other activity. Failure to adhere to these standards and to use appropriate protocols will lead to further corrective action, up to and including termination.

### Telephone Usage

**[Organization Name]** realizes that employees must occasionally make and receive personal telephone calls at work. Such calls must be kept to a minimum and should impact your work as little as possible. Unauthorized use of the telephone, including charging long distance calls to the organization, will result in corrective action, up to and including termination.

### Voice Mail System

The voice mail system at **[Organization Name]** is the property of the organization and is provided for use in conducting organization business. All communications and information transmitted by, received from, or stored in this system are organization records and property of **[Organization Name]**. The voice mail system is to be used for business only; use of the system for personal purposes is prohibited. You have no right to personal privacy in any matter stored in, created, received, or sent over the voice mail system. **[Organization Name],** in its discretion as owner of the voice mail system, reserves the right to monitor, access, retrieve, and delete any messages stored in, created with, received by, or sent over the system for any reason and without employee permission. You are not authorized to retrieve or listen to any voice mail messages that are not sent to you. Any exception to this policy must receive prior approval from **[management officials with authority to waive the policy]**.

### Cell Phones

Where job or business needs necessitate immediate access to an employee, the organization may provide/require a business cell phone for work-related communications. This phone is provided for business use only. Business cell phones are not to be used for purposes not related to work. Keep in mind that cell phone internet usage, phone records, voice mail, and text messages are not private and may be accessed. If an organization-provided phone is used for personal business, any phone charges incurred by an employee related to the personal usage will be the sole responsibility of the employee.

Personal calls during the workday using personal cell phones can be distracting to others and can interfere with employee productivity. Use of a personal phone for any reason should therefore be limited to breaks and lunches.

Any use of a cell phone while driving may present an unsafe condition for the driver, other employees, and the general public. The organization **[strongly discourages, prohibits]** the use of cell phones while driving, except when hands-free accessories are used. In cases where a cell phone call is necessary, employees must adhere to all federal, state, and local rules and regulations regarding such to help ensure the safe operation of both organization-owned and private vehicles. If an employee is using a cell phone while driving and has an accident, any costs, fees, and fines shall be solely the responsibility of the employee.

**[Optional:]** Employees should not use handheld cell phones for business purposes while driving. Should an employee need to make a business call while driving, a lawfully designated area to park should be located and the individual should pull over to make the call. Employees may use hands-free cell phones to make business calls, but only in emergency situations. Such calls should be kept short and should the circumstances warrant (e.g., heavy traffic, bad weather, unfamiliarity with area), the employee should locate an appropriate area to pull over to continue the call.