### 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.

*Posting*

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.