**The Risks Associated With Social Media**

In the past, forums for public communication were mostly controlled, like television or radio. Social media now allows individuals to broadcast their messages to the public at no cost, with no special equipment, and with no oversight. This ability can have a serious impact on our company and its reputation. Employees that have insider knowledge have the potential to cause a lot of damage.

There are also legal and employment risks. Social media usage by employees can cause a decrease in employee productivity. When hiring employees, organizations might choose to check a candidate's profile on social media sites. Employees might also use media sites to share information that could lead to their termination, which may cause legal issues.

Social media also introduces information security risks. Oversharing by employees could lead to leaked information about the company which will affect the company's strategy or reduce our competitive advantage. Social engineering attacks can also be used to gain access to the company's assets by coercing an employee to provide user credentials or act negatively. Viruses and other malware can also be transferred through social media sites.

**Social Networking Policy**

The role of Social Networking and Social Media websites is growing within companies and at the same time, poses an increasing risk to company activities. The following Social Networking Policy will assist employees in determining appropriate use of these sites, while they are both on and off duty.

Scope of Policy

The policies related to personal accounts apply to all full-time, part-time, and temporary employees, or any consultants hired. The policies related to company accounts apply to all accounts that are used for official business purposes of the company. Examples of social networking and media websites include, but are not limited to, Facebook, Twitter, LinkedIn, Flickr, and Youtube.

Policies

1. The IT department, under the direction of the CIO, will oversee and administer this policy.
2. All officially recognized accounts must be approved by IT and the CIO.
3. All official accounts must have at minimum two employees as administrators.
   1. If an administrator is no longer employed by the company for any reason, they must immediately be removed from being an administrator on that account, and a replacement will be appointed.
4. Employees are expected to adhere to same standards of conduct online as they would in the workplace. Laws and policies respecting contracting and conflict of interest, as well as applicable policies and guidelines for interacting with current, past, potential employees, associates, and clients apply online and in the social media context just as they do in personal interactions. Employees are fully responsible for what they post to social media sites.
5. Use good judgement about content and respect privacy laws. Do not post any private ro confidential employee or company information.
6. Post only content that is not threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise illegal.
7. Representation of your personal opinions as being endorsed by the company is strictly prohibited. The company’s name or marks may not be used to endorse any opinion, product, private business, cause, or political candidate.
8. Employees should not use any social networking and media site for personal use, including but not limited to those mentioned above.
   1. Exception to this policy if the social or networking and media site is used for a job function, such as for HR or marketing purposes.