InformationShield

www.informationshield.com

# Information Security Policies

## Social Networking Acceptable Use Policy

| | | | | | |
|---|---|---|---|---|---|
| Policy # | 7.1.3 | Effective Date | MM/DD/YYYY | Email | contact@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888.123.4567 |

## About This Document

*This sample information security policy is taken from the samples within the PolicyShield Security Policy Subscription. This sample follows our "best practices" policy template and includes comments to illustrate the purpose of various sections. It is released for education purposes and is not for reuse. Please contact Information Shield for more information on this and other sample policies: www.informationshield.com*

### Table of Contents



## Overview

Company X provides internet access to all employees, both permanent and temporary, through our corporate network. Social networking and other interactive web sites provide a unique opportunity to interact with other individuals and have become extremely popular with internet users. However, the unique nature of these sites also exposes individuals and organizations to additional risks not found on traditional web sites.

## Purpose

This policy defines the requirements for properly and securely using social networking sites by employees who access the Internet.

## SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at Company X, including all personnel affiliated with third parties. This policy also applies to personal use of the internet outside of Company X networks.

## TERMS AND DEFINITIONS

**Social Networking Sites** – A class of web sites which allows users to interact with other users and post content that can be viewed and shared by other users. Examples of these sites include: MySpace, Facebook, LinkedIn, YouTube and Flickr.

**Friend Request** – A request by another user on a social networking site to become part of your trusted network. Accepting friend requests gives that user special access to the information on your own personal web page.

**Browser Cookies** – Cookies are small pieces of code stored on a machine by web sites in order to track user behavior. Cookies can be exploited from social networking sites to gain access to other sites and applications.

## POLICY STATEMENTS

### Personal Use of Social Networking Sites

*[Note: The following section provides three different levels of security with regard to employee access of social networking sites. Please choose the version appropriate for your organization.]*

**Use Social Networking Sites Prohibited** – Company X users are prohibited from accessing social networking sites via company computers and networks.

**Limited Use of Social Networking Sites** – Company X users are not allowed to access social networking sites during normal business hours. Limited personal use of social networking sites is permitted via Company X networks after hours and during personal time such as lunch breaks.

**Only Approved Sites** – Company X users must only access social networking sites approved by Company X management. Please refer to list the *Approved Social Networking Sites*. Company X reserves the right to block access to sites not on the list of approved sites.

### Training and Approval for using Social Networking Sites

**Training Required** - Company X users must not access social networking web sites without a proper understanding of the associated personal and business risks. In order to receive access privileges, all workers must complete the Company X computer-based training information security course then pass the accompanying test.

**Approval Required** - Access to social networking sites will be provided to only those workers who have a legitimate business need for such access.

### Secure Use of Social Networking Sites

**Secure Settings** – All users of social networking sites must configure their accounts according to the procedures defined by the Information Security department.

**Accepting Friend Requests** - Users must not accept friend requests from individuals that they do not know and cannot identify.

**Downloading Files** – Users must not download any files posted on social networking sites and store them on Company X computers or networks.

**Installing Applications** – Users are prohibited from installing social networking applications while they are accessing social networking sites from Company X computers.

**Posting Information** – Unless explicitly approved by management, users are prohibited from posting any information indicating their employment with Company X. Examples include photos wearing Company X apparel and posts revealing details of employment with the company.

**Defamation or Harassment** – Users must not use social networking sites to participate in harassment of other users, or to post content that would cause harm to others, such as incriminating photos or videos.

**Company Email Addresses** – Unless approved by management, users of social networking sites must never use their Company X-issued email addresses in their personal profile. Only personal email addresses from third-party providers should be listed in profiles.

*(Note: Botnet software uses cookies to look for other social networking sites to infect with the compromised user account.)*

**Regular Deleting of Browser Cookies** - Users of social networking sites must delete all browser cookies immediately after using these sites.

## ENFORCEMENT

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

## EXCEPTIONS

*[This optional section clearly defines the requirements for any exceptions to this policy. This assumes the organization has a documented exception and review process.]*

Exceptions to this policy must be made in writing by the manager of the employee that will be out of compliance with this policy and approved by a member of the Information Security Department.

## REFERENCES

*[This optional section contains references to supporting documents for this policy, including any reference to a "master" policy index for organizing policy documents for compliance.]*

ISO/IEC 27002 - Section 5.1.1 Information Security Policy
7.1.3 Acceptable use of assets
6.2.2 Addressing security when dealing with customers

## RELATED DOCUMENTS

*[This optional section contains references to other policy documents, procedures, standard operating procedures, or other information or documents that may help enforce or educate users on this policy.]*

Internet Acceptable Use Policy, Sample Corporate Use of Blogging Policy, Sample Corporate Use of Social Networking Sites.

## APPROVAL AND OWNERSHIP

| Owner | Title | Date | Signature |
|---|---|---|---|
| Policy Author | Title | MM/DD/YYYY | |
| **Approved By** | **Title** | **Date** | **Signature** |
| Executive Sponsor | Title | MM/DD/YYYY | |

## REVISION HISTORY

| Version | Description | Revision Date | Review Date | Reviewer/Approver Name |
|---|---|---|---|---|
| 1.0 | Initial Version | 10-15-2009 | 10-15-2010 | IS Template |
| | | | | |