*Acceptable Use of Social Networking Policy*

Table of Contents

[Table of Contents 1](#_Toc525161222)

[Purpose 1](#_Toc525161223)

[Scope 1](#_Toc525161224)

[Policy 1](#_Toc525161225)

[Personal Use of Social Networking Sites 1](#_Toc525161226)

[Approval for Use of Social Networking Sites 2](#_Toc525161227)

[Secure Use of Social Networking Sites 2](#_Toc525161228)

[Violations 3](#_Toc525161229)

[Definitions 3](#_Toc525161230)

[References 4](#_Toc525161231)

[Related Documents 4](#_Toc525161232)

[Approval and Ownership 4](#_Toc525161233)

[Revision History 4](#_Toc525161234)

Purpose

This policy defines the requirements for properly and securely using social networking sites by employees who access the Internet via CompanyX (the “Company”) networks.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at CompanyX, including all personnel affiliated with Third-Parties. This policy also applies to personal use of the internet outside of CompanyX networks.

Policy

### 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** – CompanyX users are prohibited from accessing social networking sites via company computers and networks.

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

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

### Approval for Use of Social Networking Sites

**Training Required** - CompanyX 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 CompanyX 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 CompanyX computers or networks.

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

**Posting Information** – Unless explicitly approved by management, users are prohibited from posting any information indicating their employment with CompanyX. Examples include photos wearing CompanyX 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 CompanyX-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.

**Uses Of Instant Messaging Facilities (IM)** – Users must not use Instant Messaging (IM) or chat features of any social networking site while accessing these sites from CompanyX Information systems. If users wish to send personal instant messages, they must use a consumer IM client to keep personal information out of the business IM system archive of all messages.

Violations

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

Any employee or Third-Party 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.

Definitions

**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.

**Confidential Information (Sensitive Information)** – Any CompanyX information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by CompanyX from a Third-Party under a non-disclosure agreement.

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.

**Information Asset –** Any CompanyX data in any form, and the equipment used to manage, process, or store CompanyX data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and Third-Party data.

**Objectionable Information or Material** – Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by national or international, federal, regional, provincial, state, or local laws.

**Third-Party –** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

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: Facebook, LinkedIn, YouTube and Instagram.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002: 8.1.3 Acceptable Use of Assets

PCI-DSS: 12.3 Acceptable Usage

NIST: PL-4 Rules of Behavior

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 | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |