Social Networking Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Social network services are used by individuals and organizations to meet, establish, and maintain relationships with others. In business, ABC Company’s sales department uses social network services to convey information about new products and services and to solicit customer feedback. This policy recognizes that social network services are integral to ABC Company operations.

# II. Purpose

Social network services can create risks to the individual and ABC Company. The purpose of this policy is to address the responsible and effective use of social network and social media services.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company Information Resources.

# IV. Policy

Publically accessible information systems are not owned, operated, or controlled by ABC Company. This Policy applies to collaborative tools such as social network services, social media, user generated content, and social software including, but not limited to, Facebook, Twitter, Myspace, YouTube, MetaCafe, Google Apps, Wikis, blogs, and similar collaborative and information sharing Social network services where users can add or generate content.

The appropriate department head must give consent on the planned use of social networking services. Where appropriate, a risk assessment should be performed to determine the Internet based service assets, threats, vulnerabilities, and impact on ABC Company. The department head will:

* Approve the establishment of official external presences on Social network services.
* Ensure the role and scope of the Internet based service is clearly documented.
* Ensure the Internet based service is monitored and periodically evaluated for compliance with security requirements, fraud, and/or objectionable material.
* Ensure that the information posted is relevant and accurate and only provides information approved for public release.
* Ensure the Internet based service includes a disclaimer when personal opinions are expressed.
* Ensure users of Social network services are aware of the potential value of the content.

As a general rule, department heads will not approve the following types of information to be posted on social network services:

* Conversations between Staff members.
* Announcements, documents, discussions, or other information shared in internal meetings.
* The names of clients, partners, suppliers, or other Staff.
* Internal e-mails, notes, memos, and other interpersonal communications.
* Internal documents not specifically marked for external distribution.
* Pre-publication drafts of documents ultimately intended for public distribution.
* Planning documents or production documents.
* Software code.
* Organizational charts (org charts)
* Organizational contracts, policies, and other legal documents.

In general, department heads may allow the following types of information to be freely disclosed:

* Information published on unprotected sections of ABC Company’s web site.
* Information published by ABC Company’s Public Relations department.
* Publicly available business information.
* Advice and general professional insight that does not expose internal operational procedures or imply or disclose any proprietary or otherwise protected information.

The IT Department is responsible for providing and managing Internet connectivity. IT shall be responsible for protecting ABC Company Staff, equipment, and data from malicious software and activity. IT will take immediate actions are required to preserve information confidentiality, availability, and integrity. IT will deny access to sites with prohibited content and prohibit users from engaging in unapproved activity via social networking sites. Prohibited activity includes pornography, gambling, hate crimes, and related activity.

When accessing Social network services, in an authorized personal or unofficial capacity, ABC Company Staff shall employ sound operations security measures as indicated below:

* Settings: to protect privacy, apply the appropriate restrictions and settings provided by the social network sites. Monitor social network privacy changes and features. Change privacy settings to “friends only” so that hackers cannot see profile information.
* Security awareness: educate ABC Company Staff on the dangers of clicking on links in text messages and e-mail. Know how to detect false profiles and fake e-mail messages.
* Friends: take care when accepting friend requests in case the profiles in question are fakes. Most hackers don't have time to create long and interesting profiles. Also, it is probably a fake if they have lots of friends and have only had a profile a short amount of time.
* Disclosure: revealing too much information about yourself or your organization creates risks. Remove any sensitive information you do not want disclosed to others. Organizations should implement social networking policies dictating who in your organization is permitted to post information, the type of information that can be posted, how it is to be managed, and how the organization’s on-line social identity and intellectual property will be protected.
* Smartphones and Wearable Computing Devices: in some cases the device has been programmed with the password to social networking sites. This makes it easy for the user but also makes it easy for a hacker. Ensure your device has a password lock or other security mechanism.
* Protection software: ensure all devices used to access social networking sites have malware protection. This includes anti-virus and anti-spyware protection. Some protection software includes the ability to remotely wipe a Smartphone or Wearable Computing Device if it is lost or stolen.
* Patch management: ensure your application, operating system, third party software (pdf readers, flash, etc.), and web browsers are patched and updated on a regular basis.
* Incident response: notify social network security teams if you detect suspicious activity. The security teams can remove infected pages and apply filters to restrict future activity.
* Privacy policy: read and understand the privacy policy posted on the social network. If you don’t agree to their terms, don’t use their service.

Official uses of social network services are permitted, however, because these interactions take place in a public venue, ABC Company Staff shall maintain a liaison with the Legal Department and IT security to ensure organizational awareness and controls. IT Security shall:

* Maintain a registry of official external presences on Social network services.
* Develop and maintain threat estimates on current and emerging Social network services.
* Integrate guidance regarding the proper use of social network services into Staff training and awareness activities.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all Staff members with access to ABC Company’s Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.04, APO07.01, APO11.07, APO12.02, DSS01.04, DSS06.04, MEA03.04

GDPR Article 25, 32

HIPAA 164.308(a)(1)(i), 164.308(a)(2)

ISO 27001:2013 6.1.3, 8.3, 9.1, A.5.1.1, A.6.1.2, A.7.2.1, A.8.1.3

NIST SP 800-37 3.2, 3.4, 3.7

NIST SP 800-53 AC-5, PL-4, PS-6, PS-7, SA-9

NIST Cybersecurity Framework ID.AM-6, ID.GV-3, ID.RA-6, PR.AC-4, DE.CM-3, DE.DP-2

PCI 3.7, 6.1, 7.1, 8.1, 8.4