



This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.
<https://e-janco.com>

Social Networking Policy

Managing and Controlling Employee Social Networks



2025



Table of Contents

Policy – Social Networking	3
Definitions	3
Overview.....	3
Rights to content	8
Rules for Social Network Engagement	11
Social Network Best Practices and Guidelines	13
Security Standards.....	16
BYOD Security.....	17
Protect Sensitive Data	17
Disaster Recovery and Business Continuity.....	18
Best Practices in Managing Social Networks and Social Relationships	19
Steps to Prevent Being Scammed by Social Media	20
Appendix.....	21
Job Descriptions	22
• Chief Experience Officer	
• Manager Social Networking	
• Social Media Specialist	
Electronic Forms.....	23
• Internet and Electronic Communication Agreement	
• Social Network Policy Compliance Agreement	
Protection from Ransomware, Phishing, and Whaling Attacks.....	24
Social Networking Best Practices	28
Twitter.....	28
Truth Social	30
LinkedIn.....	31
Blog	33
What's New	36



Policy – Social Networking

Definitions

Social Networking - Connecting with a community of people in your network through services like Facebook and Twitter with various methods of online interaction. A blog with a broad user base also is a social network

Social Media - Online media like blogs, podcasts, videos, and news with a strong participatory element through comments, ratings, or other mechanisms. Social media is generated by the people and for the people with content created by anyone with a voice.

Overview

So
co
ha

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

ed to connect and
most want to know what's
pate.

Assume your competitors are using social networking to communicate and monitor your enterprise's social networking status. Disaster Recovery and Business Continuity Plans need to be updated to:

- ✦ Enhance Communication Plans: Just as your enterprise has an existing communication plan (often a press statement from executive management to media) understand how to repurpose these messages and communication on social networks.
- ✦ Experiment and Build a Base: Enterprises should experiment with tools like those provided by the Department of Homeland Security and understand how to use these tools. Companies should also start to monitor, and then experiment.
- ✦ Educate, Train, and build Awareness Before an Event. Companies as they test their DRPs and BCP should incorporate these social networks into the planning and execution processes. Companies need to indicate to the world what is an official channel, where people should go for news, and how each function plans to respond using these tools. These tools can help educate citizens on how to prepare for disasters, where to go for help, how to develop a crisis plan, and even basic life-saving medical techniques.

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's weblog or blog, journal or



Social Network Policy

Managing and Controlling Employees' Social Network Access

Statement

This policy applies to all employees and contractors who identify themselves or represent themselves as being associated with ENTERPRISE in

- ✦ Multi-media and social networking websites such as Twitter, MySpace, Facebook, Yahoo! Groups, and YouTube
- ✦ Social networks (Both ENTERPRISE Social networks and Social networks external to ENTERPRISE)
- ✦ Wikis such as Wikipedia and any other site where text can be posted
- ✦ All of these activities are referred to as “postings” in this Policy

Please be aware that violation of this policy may result in disciplinary action up to and including

te
Th
of
W
th

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

g policy. The absence of or lack
the application of this policy.
professional judgment and take
supervisor if you are uncertain.

- ✦ Social network postings should have clear disclaimers that the views expressed by the author in the social network are the author's own and do not represent the views of the company. Be clear and write in the first person. Make your writing clear that you are speaking for yourself and not on behalf of the company.
- ✦ Be authentic, honest, and conversational in your posts. Leave the marketing to speak and press release format for other parts of the website.
- ✦ Use good judgment about content and be careful not to include confidential information about your company, customers, or vendors.
- ✦ Information published on social networks should comply with the company's confidentiality and disclosure of proprietary data policies. This also applies to comments posted on blogs, forums, and other social networking sites.
- ✦ Be respectful to the company, other employees, customers, partners, and competitors.
- ✦ Social media activities should not interfere with work commitments. Refer to IT resource usage policies.
- ✦ Online presence reflects on the company. Be aware that your actions captured via images, posts, or comments can reflect that of our company.
- ✦ Do not reference or site company clients, partners, or customers without their express consent. In all cases, do not publish any information regarding a client during the engagement.

Rules for Social Network Engagement

Social Networking is now the way of the world. Everything from personal communication, photo distribution, eCommerce, news dissemination, and political debates is now done on social networks. To that end, the IT Governance process needs to consider that. Rules need to be put in place on how an enterprise, its spokesmen, and employees interact and have social network engagement.

Understand the audience

Each social network has a different audience and disseminates information differently. Try out the of existing social networks.

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

- ✚ Twitter
- ✚ YouTube
- ✚ Wikipedia
- ✚ Buffer for distribution
- ✚ Others

If the technology group does not set rules and standards, the user community will take it upon themselves to integrate consumer apps into their work lives. This, in turn, can cause issues with the “social reputation” of the enterprise.

As a first step try out social networking with a low-cost pilot. Many open-source tools are widely available to experiment with. Another option is hosted applications which usually offer a small number of corporate licenses at a very low price.

Set Realistic Goal

Do not promise operational organizations and management that the enterprise's social network will do everything. Establish a pilot project with defined metrics. Be willing to walk away.

Set reasonable goals for user adoption and focus your initial deployment on a few groups that are eager for social networking tools. Establish pragmatic metrics and measure business value. This will be the basis for an ROI analysis for senior management's approval before rollout.



Social Network Policy

Managing and Controlling Employees' Social Network Access

Job Descriptions

Three (3) full job descriptions are included with this policy template. They are provided separately in a directory.

- Chief Experience Officer
- Manager Social Networking
- Social Media Specialist

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>



Social Network Policy

Managing and Controlling Employees' Social Network Access

Electronic Forms

Two (2) Electronic forms are included with this policy template. They are provided separately in a directory.

- Internet and Electronic Communication Agreement
- Social Network Policy Compliance Agreement

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>



Protection from Ransomware, Phishing, and Whaling Attacks

Ransomware attacks are aimed at enterprises that need to have systems operational to function. Executives are most likely to be targets of a whaling attack. Phishing attacks are aimed at anyone with an e-mail address, whaling attacks target senior management at companies where knowing a top executive's password opens a back door to sensitive insider information. With private information becoming public via social networks, senior executives are being targeted via "whaling" attacks.

These whaling attacks are a form of personalized phishing, or spear phishing, aimed at senior executives or others in an organization who have access to lots of valuable or competitive

inf
cre
ins
W
de
W



nk account data, passwords,
often target people who have
There's no obvious signature to
hing email enter your server.
en play on executives' feelings

and sense of self-importance.

Ransomware Attacks

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions on how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

There are several vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam - attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files. If you want the technical details, the Infosec Institute has a great in-depth look at how several flavors of ransomware encrypt files. But the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only by the attacker.



What's New

2025 Edition

- ✚ Updated all the included electronic forms
- ✚ Updated all the included job descriptions

2024 Edition

- ✚ Added Best Practices for Truth Social
- ✚ Updated all the included electronic forms
- ✚ Updated all the included job descriptions

2022 Edition

- ✚ Added job description for Chief Experience Officer
- ✚ Updated all the included electronic forms
- ✚ Updated all the included job descriptions

2021 Edition

- ✚ Added strategy on how to implement enterprise social networking
- ✚ Added materials on Ransomware attack protection
- ✚ Updated materials on phishing and whaling attack protection
- ✚ Updated all the included electronic forms
- ✚ Updated all the included job descriptions

2020 Edition

- ✚ Updated all the included electronic forms
- ✚ Updated all the included job descriptions
- ✚ Updated to meet the latest mandated requirements