KROLL Fraud Solutions

Social Media in the Workplace

Combat the Data Security Risks with Formal Guidelines for Your Employees

What is your company's stance on social media? This is a fundamentally tough question that most organizations are only beginning to tackle. But tackle it they must: According to the 2009 Deloitte Ethics & Workplace survey, some 55 percent of employee respondents said they visit social networking sites to varying degrees—both at work and home. Yet, only 22 percent of executive respondents stated that their company had a formal policy dictating how employees can use social networking tools.

When you consider the potential risks that social media use can pose to an organization—from reputational damage to outright breach of sensitive data—the picture becomes painfully clear: businesses must work harder to transform employees into data security ambassadors by giving them a clear set of guidelines on how to engage in social media safely and smartly.

Below, Kroll's Fraud Solutions practice outlines areas that organizations need to consider when developing a social media policy—defining not only what's acceptable, but giving your employees the tools and the know-how to keep sensitive information of all kinds safe.

Develop a social media policy that clearly identifies what is and is not acceptable communication and specifically states consequences. To begin, conduct a review of your organization's existing business conduct and ethics guidelines. Your social media policy should tie back to these guidelines and not contradict them. Possible policy elements could include:

- ***Clear guidelines on proper social media use:*** Avoid the inclusion of unrealistic mandates. The fact of the matter is employees will use social media whether you forbid it or not. It's far better to outline appropriate use of social media than outlaw it completely.
- ***Consequences of non-compliance:*** Clearly identify what can happen if an employee fails to follow the policy. Identify specific corrective actions, particularly if they could involve the potential for legal prosecution.
- ***Employee training:*** Couple best practices in social media use with your organization's ongoing privacy awareness training.
- ***Specifics on what employees can and cannot divulge:*** Set strict guidelines for disclosures—should individuals identify themselves as employees and/or reveal their position in the company? Must they include a disclaimer statement on comments? Other areas to cover: social engineering tactics, malware and suspicious downloads, and avoiding disclosure of capital intelligence.

KROLL Fraud Solutions

Update your social media policy regularly. Social networking technology evolves on a seemingly daily basis, so it's important for your organization to be prepared to evolve with it. Review the policy and make changes to it, as appropriate, on an annual basis to start. (Depending on your industry or market, more frequent review may be prudent). Make sure any changes are plainly communicated to employees with the understanding that the change is meant to accommodate any new social networking developments that directly affect the company.

Develop your "social media incident" response plan. Even with proper training and documentation, instances will occur where sensitive information is divulged. In these cases, it's important to also develop your reactionary plan. This will no doubt involve crisis communications to stem any negative effects of an information leak. If personal data was leaked that triggers a breach notification, a more traditional incident response will be required.

As a final reminder, and perhaps a rule of thumb for all employees: If you wouldn't divulge something in normal conversation with a stranger, don't share it online. In the world of social media, conversations live on forever, so it's especially important to practice prudent posting.

Kroll's Fraud Solutions
866 419 2052
www.krollfraudsolutions.com
www.kroll.com

This article was prepared for general information purposes only and does not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your own situation and any specific questions you may have.
© 2011 Kroll Inc. All rights reserved. Item #THT003-2011-03-29

Your Identity Is Your Business.
Protecting It Is Ours.