# 1 WHY EVERY ORGANIZATION NEEDS A SOCIAL MEDIA POLICY AND COMPLIANCE MANAGEMENT PROGRAM



From Twitter and Facebook to YouTube, blogs, smartphones, and tablet PCs, employees' access to the web—and employers' exposure to potentially costly and protracted risks—is greater today than ever before. Whether responding to customer inquiries via Twitter, posting coupons on Facebook, building brand awareness on blogs, or conducting product demonstrations on YouTube, the business community's

ever-growing social media use dramatically increases organizations' exposure to potential lawsuits, regulatory violations, security breaches, mismanaged business records, productivity drains, netiquette nightmares, public relations disasters, and other electronic risks.

When employed strategically, there's no denying that business blogs, corporate Facebook pages, instructional YouTube videos, private enterprise-grade social networking platforms, and other social media and web 2.0 tools can facilitate speedy and successful two-way communication with customers, as well as creative and constructive collaboration with colleagues.

Workplace use of social networking sites and web 2.0 technologies increased dramatically between 2007 and 2010, growing from just 11 percent to over 66 percent in a three-year span. Over 90 percent of organizations believe web 2.0 technologies are effective at increasing brand awareness, and another 89 percent consider these communication and collaboration tools essential when it comes to generating new business or supporting customer service. That's according to Clearswift's 2010 report, *Web 2.0 in the Workplace Today.*[1]



Similarly, when managed properly, employees' personal use of social media (via company accounts and systems as well as users' own personal sites and devices) can enhance workers' overall satisfaction with and commitment to their jobs. In fact, one-fifth of the group that the Clearswift report labels "Generation Standby" workers (younger employees who never fully switch off from the Internet at work or home) say that they would turn down employment if the boss did not allow them to access social networking sites or personal email during working hours.[2]

In the age of social media, employers must perform a balancing act. On the one hand, you want to provide enough social web access to keep your business thriving and maintain consideration for some level of personal usage. On the other hand, you are obligated to manage social media use effectively in order to protect your organization's assets, reputation, and future.

The most effective way to accomplish both goals is to implement social media policies, also known as acceptable use policies (AUPs), supported by comprehensive employee training, and enforced by best-in-class technology tools.

## TEST YOUR SOCIAL MEDIA COMPLIANCE MANAGEMENT KNOW-HOW

When it comes to communicating and collaborating with internal and external audiences, employees today enjoy a broad range of electronic options. From tweeting and blogging to surfing, Skyping, texting, and talking via mobile devices, twenty-first-century communication tools and technologies facilitate speedy interactions between organizations and their important audiences, including customers, prospects, investors, the media, decision makers, and the public.

Given the comprehensive mix of electronic business communication tools now available to companies and users, compliance management—more than ever—is a critical business skill. Take this brief quiz to determine your social media compliance management know-how.



1. As of 2011, social networking had surpassed email as the electronic communication tool of choice for most business users.
   ☐ True ☐ False
2. Because computers have been workplace staples for so long, most employers today are fully aware of—and adept at managing—electronic risks including potentially costly litigation, regulatory fines, security breaches, productivity drains, and public relations nightmares.
   ☐ True ☐ False
3. In the United States, federal and state laws governing the use, content, records, privacy, and security of electronic information have changed very little since the year 1995.
   ☐ True ☐ False
4. Government and industry regulations governing the use, content, records, privacy, and security of email and other forms of electronic business communication basically are the same today as they were in 2001.
   ☐ True ☐ False

5. The Federal Rules of Civil Procedure, which govern e-discovery, are mirrored by the rules of civil procedures in all 50 states.
   ☐ True ☐ False
6. Text messaging is completely different from email. Consequently, email risks and rules do not apply to text messaging.
   ☐ True ☐ False
7. In accordance with best practices, Acceptable Use Policies (AUPs) governing social media, blogs, email, mobile devices, and other electronic business communication tools and technologies should be reviewed and updated once every decade.
   ☐ True ☐ False



## THE NEED FOR STRATEGIC COMPLIANCE MANAGEMENT HAS NEVER BEEN GREATER

If you answered "true" to any of these seven statements, then it's time to brush up on your knowledge of social media compliance management—and electronic compliance management in general.

Effective compliance management is a priority for any organization—large or small, public or private, regulated or unregulated—that is eager to adhere to legal, regulatory, and organizational rules, while mitigating potentially costly risks. Effective compliance management, of course, begins with formal rules and written policies.

### *Social networking is risky business*

By now, most people are familiar with the type of high-profile, well-publicized email gaffes and Internet disasters that tarnish corporate reputations, savage stock valuations, launch million-dollar lawsuits, derail careers, and trigger media feeding frenzies. Thanks to social

media—and the widespread use of mobile devices to access social networking sites day and night—employers' exposure to electronic risks is greater than ever.

### *Inappropriate tweets and posts trigger lawsuits and regulatory audits*

Anyone with Internet access can establish a Twitter presence, Facebook page, or LinkedIn account and start sharing negative, critical, defamatory, or otherwise harmful comments about your organization's people, products, financials, and future. Given the potentially costly and protracted risks inherent in social networking, it's essential for organizations to establish social media rules and written policies governing the type of content that employees may—and may not—post on business—and personal—social networking sites.



### *Unauthorized photos and videos cause humiliation and crush credibility*

Armed with nothing more than a smartphone, your employees, disgruntled ex-employees, and office visitors can capture, upload, and post embarrassing or otherwise damaging photos and videos of executives, staff, clients, company secrets, facilities, and operations, or even themselves. With more than 350 million active users accessing Facebook through mobile devices,[3] it's essential for organizations to establish formal rules and policies governing the use of BlackBerries, smartphones, cell phones, tablet PCs, and other mobile devices.

### *Leaked secrets sink companies and sabotage careers*

Should dissatisfied workers or angry ex-employees post confidential company information or disclose customers' personal financial data on social networking sites or blogs, the devastating results can range from negative publicity and public scrutiny to regulatory investigations, litigation, and declining stock valuations.

A quarter of employees surveyed in 2010 said they had sent regrettable content via social networks and email, according to Clearswift's *Web 2.0 in the Workplace Today report*.[4] One year earlier, 14 percent of employees admitted to emailing confidential company information to third parties; 6 percent emailed customers' credit card data and Social Security numbers to outsiders; and another 6 percent emailed patients' protected health information to third parties, reveals the *2009 Electronic Business Communication Policies and Procedures Survey* from American Management Association and The ePolicy Institute.[5]

Social media use increases the likelihood that employees will expose confidential internal data and customers' private (and legally protected) information to outside parties, triggering regulatory audits and lawsuits in the process. Concern about confidentiality breaches has prompted professional football teams to ban Twitter. Hollywood studios now insert legal clauses in actors' contracts forbidding them to write about films in mid-production on any social networking site or blog. Most of the household-name companies on Germany's DAX 30 stock market index have outlawed the use of Facebook and Twitter over concerns about industrial espionage and lost productivity.



## Courts and regulators view tweets and posts as electronic business records

Just like email, social media can create business records, or electronically stored information (ESI). If employees use the company system to tweet on Twitter, network on Facebook, post on business blogs, or upload videos to YouTube, that content may be subpoenaed, must be produced, and could be used as evidence in lawsuits and regulatory investigations. Employers are responsible for the legally compliant preservation, protection, and production of social media content, as well as email and other ESI.

## Social media create productivity drains

Although 87 percent of employees lack a clear business reason to use Facebook, some use it as much as two hours a day while at work, according to Nucleus Research.[6] Add to that the fact that 52 percent

of employees spend up to two hours a day on email, and another 20 percent devote four or more hours to email, according to American Management Association/ePolicy Institute research,[7] and that equals a lot of wasted time and money. Best practices call for the implementation of personal use rules to help manage employees' social media use—and misuse.

### *Social networking puts employees at risk*

Social networking can lead to not working. In 2009, 2 percent of bosses fired workers for content posted on personal social networking sites; 1 percent dismissed employees for posts on their personal blogs; 1 percent terminated workers for misuse of the corporate blog; and another 1 percent fired employees for videos posted on YouTube, according to American Management/ePolicy Institute research.[8] We can expect those numbers to rise as employees' use of social media grows.



### *Social media can be a barrier to employment*

Forty-five percent of organizations review job applicants' personal Facebook profiles as part of the interview process. Another 35 percent of employers have rejected job applicants on the basis of the content posted on Facebook, according to a CareerBuilder survey.[9] Unfortunately, as detailed in Chapter Five, social media background checks can backfire for employers, putting companies at risk of discrimination claims by rejected job candidates.

### *Compliance management begins with social media policy*

In the twenty-first century, it is essential for all companies to develop and enforce written policies governing social media use, content, and business records. Even if your organization does not currently have a social media presence, you cannot afford to turn a blind eye to the communications phenomenon that is social networking. Don't wait for a social media disaster to strike. Put a strategic social media policy and

compliance management program to work immediately to help reduce (and in some cases prevent) disasters triggered by employees' business and personal use of online communication and collaboration tools.

## SOCIAL MEDIA BEST PRACTICES: POLICY IS ESSENTIAL TO COMPLIANCE MANAGEMENT

1. Social media and web 2.0 content, use, and records create increased exposures to legal, regulatory, security, productivity, records management, public relations, and other potentially costly risks.
2. When managed strategically, social networking and web 2.0 tools can facilitate speedy and successful two-way communication with customers, as well as creative and constructive collaboration with coworkers.
3. When managed effectively, employees' personal use of social media can enhance workers' overall satisfaction with and commitment to their jobs.
4. The most effective way to manage social media risks is to implement social media rules and policies, supported by comprehensive employee training, and enforced by best-in-class technology tools.