

Corporate email policies lower unnecessary legal and security risks.

This Free E-Book is brought to you by [Natural-Aging.com](http://Natural-Aging.com).

**100% Effective Natural Hormone Treatment**  
**Menopause, Andropause And Other Hormone Imbalances**  
**Impair Healthy Healing In People Over The Age Of 30!**

Corporate email policies lower unnecessary legal and security risks.

By Anti Spam League

Corporate email policies lower unnecessary legal and security risks. by Anti Spam League

What comes to your mind when you think about your email? Email makes possible almost instant communication with your co-workers without leaving your desk, a quick note to a family member who lives far away, but also has a very annoying downside such as junk mail. Since the introduction of the Internet, email has been one of its primary uses. The fact that it is a fast, cheap and easy means of communication, makes email a great business tool. But there are also a series of threats for employers associated with email usage. Email threats such as confidentiality breaches, legal liability, lost productivity and damage to reputation cost organizations millions of dollars each year.

In the majority of cases, companies are held responsible for all the information transmitted on or from their systems. As a result, inappropriate emails can result in multi-million dollar penalties in addition to other costs. For example, a Federal Communications Commission (FCC) employee unintentionally sent a dirty joke entitled 'Nuns in Heaven' to 6,000 journalists and government officials on the agency's group email list. This employee's lapse in judgment and electronic mistake resulted in negative publicity and national embarrassment for the FCC. In the US, Chevron settled a case filed by four female employees for \$2.2 million. The employees alleged that sexually harassing emails sent through the company's email system caused a threatening work environment. One of the sexually offensive messages was a joke sheet titled '25 reasons why beer is better than women'. A company can also be liable if one of its employees sends an email containing a virus.

Confidentiality breaches can be accidental, for instance when an employee selects a wrong contact name in the 'To:' field, or intentional, such as the case where an employee uses his corporate email account to send confidential information to one of the company's competitors. In the latter case, both the employee and the recipient could be charged with trade secret theft. Nonetheless, whether it is by mistake or on purpose, the result of the loss of confidential data is the same.

Lost productivity due to inappropriate use of a firm's email system is becoming a growing area of concern. A recent survey revealed that 86 per cent of workers used their company email to send and receive personal emails. Given that it has become very hard in our modern world to segregate people's personal lives outside of the workday, companies struggle to find effective ways of balancing employee freedoms and corporate protection. In addition to personal emails, unwanted spam messages are a significant time waster. Spam and personal abuse of email can also cause a corporation's email system to waste valuable bandwidth resources. A Gartner Group study held under 13,000 email users

## Corporate email policies lower unnecessary legal and security risks.

found that 90 percent receive spam at least once a week, and almost 50 percent get spammed more than 6 times a week. Personal emails cause network congestion since they are not only unnecessary, but tend to be mailed to a large list of recipients and often include large attachments such as mp3, executable or video files that users do not zip. Adopting an anti-spam system alone has not proven effective to stop spam. The combination of spam-blockers with other methods of spam control technologies such as SIDF, SPF, Bayesian Filters, Blacklists, Whitelists, Anomaly Detection, and Spam Signatures has proven to be much more effective. There are also special organizations such as the Anti SPAM League.org that give Internet users the chance to report those individuals and companies that are responsible of spamming. You can become a member for free and learn how to control the spam problem by visiting their website at [www.antispamleague.org](http://www.antispamleague.org). For more details on how to deal with spam, read the article 'How Can I Stop It? – The Challenging Task of Controlling Spam'.

How can a company protect itself from these threats? The first step in securing your organization is to create an email usage policy. Every company needs to establish a policy regarding use of and access to company email systems, and then tell all employees what its policy is. After you have created your email policy you must make sure it is actually implemented. This can be done by providing regular trainings and by monitoring employees' email using some type of email security software. The email policy should be made available and easily accessible to all employees and should be included in employee handbooks and company intranets. It is best to include the email policy, or a short statement regarding the policy, in employment contracts. In this way the employee must acknowledge in writing that he/she is aware of the email policy and of the obligation to adhere to it.

What are some of the benefits of having a clear and effective email policy? First, it helps prevent email threats, since it makes your staff aware of the corporate rules and guidelines. Second, it can help stop any misconduct at an early stage by asking employees to come forward as soon as they receive an offensive email. Keeping the incidents to a minimum can help avoid legal liability. For example, in the case of Morgan Stanley, a US investment bank that faced an employee court case, the court ruled that a single email communication – a racist joke, in this case – cannot create a hostile work environment and dismissed the case against them. Third, if an incident does occur, an email policy can minimize the corporation's liability for the employee's actions. Previous cases have proven that the existence of an email policy can prove that the company has taken steps to prevent inappropriate use of the email system and therefore can be freed of liability. Fourth, if you are going to use email filtering software to check the contents of your employee's emails, you must have an email policy that states this clearly. Some employees may argue that by monitoring their emails, companies are violating their privacy rights. However, court cases have shown that if the employer has warned the employee beforehand that their email might be monitored, the employer has a right to do so. People usually respond better when they know where they stand and what is expected of them.

The recent spike in the volume of spam traveling across the Internet, combined with the dangers of phishing and virus attacks that frequently accompany these messages, has forced corporations to reconsider how they determine which messages will be allowed into their network. For years, companies have addressed their email security needs through a mixture of third party software solutions designed to address specific areas of vulnerability. Today, however, this approach appears to be ineffective. New threats adapt to even the latest security technology, helping hackers and

## Corporate email policies lower unnecessary legal and security risks.

spammers stay a step ahead of most stand-alone protective measures. System administrators remain in a reactionary mode, waiting for the next attack and hoping their mixed bag of security software is up to the test.

The role of email in Sarbanes-Oxley compliance cannot be overstated. The Sarbanes-Oxley Act of 2002 and associated rules adopted by the Securities and Exchange Commission (SEC) require certain businesses to report on the effectiveness of their internal controls over financial reporting. Effective internal controls ensure information integrity by mandating the confidentiality, privacy, availability, controlled access, monitoring and reporting of corporate or customer financial information. Companies that must comply with Sarbanes-Oxley include U.S. public companies, foreign filers in U.S. markets and privately held companies with public debt. U.S. companies with market cap greater than \$75M and on an accelerated (2004) filing deadline are required to comply for fiscal years ending on or after Nov. 15, 2004. All others are required to comply for fiscal years ending on or after April 15, 2005.

Because the bulk of information in most corporations is created, stored, transmitted and maintained electronically, IT departments are responsible for ensuring that sound practices, including corporate wide information security policies and enforced implementation of those policies, are in place for

employees at all levels. Information security policies should govern the following items:

- Network security
- Access controls
- Authentication
- Encryption
- Logging
- Monitoring and alerting
- Pre-planning coordinated incident response
- Forensics

Most of us would agree that today email is the primary internal and external communication tool for corporations. Unfortunately, it is also one of the most exposed areas of a technology infrastructure. Email systems are critical to ensuring effective internal control over financial reporting, encryption of external messages and active policy enforcement, all essential elements of compliance. Companies must install a solution that actively enforces policy, stops offending mail both inbound and outbound and halts threats before internal controls are compromised, as opposed to passively noting violations as they occur. An effective email security solution must address all aspects of controlling access to electronically stored company financial information. Given the wide functionality of email, ensuring appropriate information access control for all of these points requires:

- A capable policy enforcement mechanism to set rules in accordance with each company's systems of internal controls;
- Encryption capabilities to ensure privacy and confidentiality through secure and authenticated transport and delivery of email messages;
- Secure remote access to enable remote access for authorized users while preventing access from unauthorized users;
- Anti-spam and anti-phishing technology to prevent malicious code from entering a machine and to prevent private information from being provided to unauthorized parties.

On a final note, some clear guidelines for a good and effective email policy include the following points:

Corporate email policies lower unnecessary legal and security risks.

a) Emails should comply with the proper RFC protocols for email, 2) Employees should not attempt to obscure content or messages in emails, 3) Companies should post privacy policies where they can be read and understood, prior to submission of a request, 4) Employees should not send email to unverified or nonexistent email addresses, 5) Companies should offer users opportunities to opt-out of programs.

Given that developments in email and the Internet are changing so rapidly, it is essential to review the email policy at least once every quarter. Keep an eye on new developments in email and Internet law so that you are aware of any new regulations and opportunities. When you release new updates, it is preferable to have each user sign as acknowledgment of their receipt of the policy.

With all of this said, if you want to reduce electronic risks in the workplace you must take the initiative. Electronic disasters can ruin businesses, sink careers, send stock prices plummeting, and generate public relations nightmares. Do not wait for a disaster to strike; prevention is always your best defense. Visit [www.AntiSpamLeague.org](http://www.AntiSpamLeague.org) and they will help you develop and implement written email usage and privacy policies that clearly reflect your organization's expected standards of electronic behavior, along with privacy and monitoring policies.

The purpose of the Anti SPAM League is to help consumers and business owners reduce the amount of SPAM they receive. In addition, our Anti SPAM organization believes that educating site owners in the area of SPAM prevention and ways to successfully and responsibly market their sites, is key in making a difference.

## **Tips For Insuring Your Property Abroad**

### **By HolidayHomeNow**

Once you've bought your new property abroad, you'll need to insure the building and its contents.

Getting insurance for your property abroad is just as easy as getting it for your home in the UK. Insurance policies can be quoted for online and even purchased online, but before you rush into an insurance contract, take the time to compare not only the prices but also the level of cover you're getting; more often than not, cheap prices mean lower quality cover.

You can't afford your insurance policy to let you down when it comes to your property abroad. You're at a distance from the property, so you may not be able to see the damage first hand, but have to rely on whoever is maintaining or managing the property for you. Alternatively, if you're living in the property, you want to know that you can call the insurance company, regardless of the time difference and begin to sort out the problem immediately.

What to look for:

- Check exclusions - like all insurance policies, you should make sure that you know exactly what's covered and what isn't. This is particularly important if you're renting out the property, or using it as a holiday home. Insurers often place additional restrictions during periods when the property is unoccupied, and it is worth comparing these restrictions across several policies before you commit to one.

Corporate email policies lower unnecessary legal and security risks.

- Security requirements - insurers often place harsher security requirements on your property abroad than they would at home. Check what security requirements the insurer requests, and decide whether you are happy to abide with them.
- For rental properties - rental properties need to have accidental damage and public liability insurance included on their policies. If you are using a rental agency, they may help you to arrange this; but if you're managing the rentals on your property abroad by yourself, then you must make sure that you have the appropriate cover.
- Excess - the excess amount can be greater on your property abroad than you would find in the UK. If you feel the excess is too high, ask the insurer why it is set at that level, and see if you negotiate a lower excess. Alternatively, look at another policy.

HolidayHomeNow has been set up to provide useful, practical information for those people researching and looking into buying a second property or holiday home abroad. For more information have a look at their website



**This Free E-Book has been brought to you by [Natural-Aging.com](http://Natural-Aging.com).**

**[100% Effective Natural Hormone Treatment](#)**

Corporate email policies lower unnecessary legal and security risks.

**Menopause, Andropause And Other Hormone Imbalances  
Impair Healthy Healing In People Over The Age Of 30!**

