



CLIENT ADVISORY

THE NEED FOR COMPANY EMAIL AND INTERNET POLICIES

Recent surveys reveal some startling statistics: upwards of 85% of employees use e-mail at work for personal purposes; 62% of organizations report employee sex site surfing; and 55% of employees have received inappropriate e-mails during work.

The informality and ease with which materials can be sent via e-mail messages or uploaded and downloaded from the web has significant potential for abuse. Clearly, the loss in employee productivity that results from these activities is damaging to any business. Increasingly, businesses must also consider the risk of claims for employee misconduct involving the internet including discrimination, harassment, copyright infringement, defamation and financial fraud.

In order to protect themselves and deter inappropriate use, employers should enact and enforce policies governing the use of internet and e-mail systems and clearly communicate these policies to their employees. The policies should spell out in detail which activities are permitted and which are prohibited and should make clear that employees do not have an expectation of privacy in their e-mail or internet use while at work.

Internet and email policies should be customized for the needs of the business and, therefore, a boilerplate approach is not effective. There are, however, common elements which should be included in any policy. First and foremost, the policy should address whether company equipment is strictly for business use or whether some personal use is permitted. The policy should also include the following:

- *Employees have no expectation of privacy in use of business internet and e-mail hardware and software.*
- *Internet and e-mail equipment is the property of the business along with access codes, passwords, messages attachments and downloaded files.*
- *Internet and e-mail files, messages and attachments are subject to being accessed and reviewed by management at the discretion of the company without notice.*
- *E-mail and internet use is to be consistent with all policies of the company, such as those prohibiting sexual harassment.*
- *Systems cannot be used to violate any law, regulation or company policy.*
- *E-mail and internet systems are not to be used to create or distribute offensive messages that are defamatory, obscene, derogatory or threatening.*
- *Systems cannot be used to send or receive copyright material, trade secrets or proprietary information without management approval.*

- *Employees cannot visit sexually explicit or other inappropriate web sites and cannot engage in online computer games or gambling.*
- *Statement concerning the importance of maintaining security against computer viruses and hackers and a reporting procedure in the event such threats are detected.*
- *Violations of the policy may result in discipline ranging from a verbal warning to discharge from employment.*

Depending on the nature of the business, the following provisions might also be included:

- *The policy may be broadened to include voice mail and fax communications.*
- *Confidential or privileged information may only be transmitted if safeguarded and/or encrypted.*
- *Employees are accountable for all activity in the company computer system conducted under their individual password.*
- *Employees may not engage in online chat, bulletin board or discussion forums.*
- *Executable files may not be downloaded without authorization.*
- *Email attachments should be opened only when the identity of the sender is known.*

Once the policy is drafted, communicated to employees and implemented, it should be enforced in a uniform matter.

In order to create an internet and email policy that is right for your company, consider the following questions:

- *Will the policy adversely affect the business culture by eroding trust?*
- *Should private use be allowed? If so, how much? Should private use be monitored?*
- *Does permission for private use create an expectation of privacy?*
- *Does the policy remain in effect for remote access work and after-hours work?*
- *What discipline measures will be used for violations of the policy?*

The policy should be tailored to the individual **culture** of the organization. In some businesses, some personal and remote use of company systems is commonplace. A strict policy prohibiting personal use with such a business may have the effect of dissuading new hires and creating unrest among existing employees. Conversely, some businesses such as brokerage houses and financial institutions, have far greater regulatory compliance requirements. In those instances, a more stringent policy would be required.

This area of law continues to develop almost on a daily basis. Do not let the absence of an internet and e-mail policy present a major unforeseen risk to your business.