

IT and Security Best Practices

Does your company have a computer usage policy in place, and if so, is it adequate to protect the company? As technology advances and business innovations are moving into a universal electronic age, business security policies and practices must evolve accordingly. With virtually every employee in a company maintaining a computer at their workstation, or at least having “access”, companies are operating more efficiently. Or at least that is the belief. It may startle you to learn that 70% of internet pornography traffic occurs during the 9-5 workday or that 64% of employees acknowledge that they use the internet for personal use during the workday. Moreover, 27% of companies have fired employees for misuse of company email or the internet, and 37% of employees say that they often surf the internet at work. The statistics are alarming and at the same time are indicative of the necessity for clear and enforceable workplace policies to protect your company.

Still thinking that this is not issue at your company or in your office? Consider this matter from an economic standpoint. A company with 1,000 internet users could potentially lose in excess of \$35 million in productivity annually just from an hour a day of internet usage and web surfing per freelancing employee. If you believe that your company is not that big and would not lose such amounts of money, think again. Failure to implement a company internet usage and conduct policy is essentially putting your company at further risk for litigation, security breaches, theft of proprietary information and other “computer crimes.” The real question is whether your company can afford not

to have such policies in place. Nothing is failsafe, but the absence of even a basic policy is an invitation to another form of workplace liability.

In 2003 Chevron USA paid \$2.2 million to settle a sexual harassment suit that stemmed from an inappropriate email. Remember that an email from a company email address is a direct reflection on that company. Actions of employees while at work are deemed actions of the company. The liability is too broad to not be addressed and covered.

The following are examples of purpose and scope security policies which address some of the topics. These should be integrated into company policy and should be included in appropriate employment agreements.

Email

- Purpose
 - The purpose of this policy is to prevent any negative impact to the namesake of said company and/or any detrimental or invidious affiliation stemming from misuse of company email or any other electronic communication.
- Scope
 - This policy applies to all email sent and forwarded from company email address and is applicable to all those employees, vendors, contractors, agents, and officers with access,

either express or implied,
permanent or temporary, to
company email and other
electronic communication.

○ Policy Itself

▪ **Prohibited Use**

- Company email shall not be used to forward, create, or distribute any offensive or disruptive messages, images or any other expressive form. Including but not limited to offensive or discriminatory messages regarding; race, gender, national origin, sex, disability, age, sexual orientation, political affiliation, and religious beliefs.

▪ **Personal use**

- While use of company email may be permitted, it is done so only in a very limited scope. Personal emailing should be kept to a minimum and should never contain any of the aforementioned prohibited materials. In

addition, chain letter emails as well as jokes should not be sent, forwarded or received to the company email address.

▪ **Monitoring**

- Emails sent, received, stored or forwarded from Company email are deemed company property and are permitted to be viewed and monitored by the company without prior notice to the employee.

Proprietary Information

○ **Purpose**

- The purpose of this clause is to outline the authorized and acceptable uses of company owned computer equipment. Misuse of company computer equipment exposes the company to viruses as well as possible compromise of the

network, system, security and services.

- **Scope**

- This policy applies to all employees, vendors, contractors, agents, and officers with access, either express or implied, permanent or temporary, to company computers and other electronic devices.

- **Proprietary Information**

- Any information or data that is created on the company computer system becomes and remains property of Company.
- Information received and stored during the normal course of employment becomes property of the company.
- Employees are bound to not disclose any confidential company information to anyone outside of the company absent explicit permission

from an officer of the company.

Internet Usage

- All internet usage on company owned, leased, or related equipment should be limited to job related websites and work related information seeking only
- The company reserves the right to monitor and document internet connections or communications without prior disclosure or permission

Enforcement

- Any employee who is found to have violated any policies set out in this document may be subject to disciplinary action including and up to termination or suspension.

David L. Ganje, Esq. is a member of Bioconnex, the Albany Chamber TechForce Council Committee Southern Saratoga Chamber, is counsel to the Upstate New York Laboratory Robotics Interest Group, and maintains a private commercial and business law practice at Ganje Law Offices in Albany with a web address of <http://www.ganjelaw.com/>.