

# White Paper

(Summary)

## Employers Guide:

*The widespread personal use of “Social Networking” by employees on company time and company networks.*

*(My space, Twitter, Face book etc.)*

- According to recent survey, 50% of employers completely prohibit social media use by workers.
- HR director says, “If you’re using social networking at work such as instant messaging, personal email, Facebook, Myspace, etc. you should be fired.
- ...”This generation does not know its wrong to do personal communications at work and can’t leave it at home including their cell phone.”...”There is no standard from company to company or department to department regarding policy.”
- I.T. Director- “All I know is my I.T. costs are going through the roof due to malware and corruption on the PC’s due to misuse. We must do something....”

### Problem:

**Employee productivity is off 25% due to distraction by personal cell phone use (voice, email, text messaging etc.), use of company pc to do personal email, instant messaging, and social networking in general, surfing non business websites and tying up available bandwidth and corruption of pc Windows operating system.**

**Old Solution: (did not work)**

**Post company policy on Internet and personal technology use.**

## White Paper – social networking “continued”

### **New Solution:**

**Take a proactive approach to I.T. security:**

**Install Netgear Unified Threat Management solution to manage security:**

- **Prevent employees from visiting non business website**
- **Block social networking and instant messaging**
- **Block web surfing by category (guns, adult etc.)**
- **Protect network with malware protection, email protection**
- **Log Internet usage by user and category.**

**Implement “good practices” with overall network security including:**

- **Anti-virus, anti-spyware on PC Workstations and Servers**
- **Automatic update of anti-virus definitions**
- **Manage correct operation of anti-virus software on each device**
- **Use measures to prevent unauthorized users to load programs on pc workstations.**
- **Secure wireless access to prevent unauthorized use.**
- **Verify Internet and Workstation firewalls.**
- **Verify security of shared resources**
- **Other site specific procedures suggested by your I.T. consultant**

Tulsa Oklahoma based Anchor Technology, Inc. has been installing security appliances since 2003 that do content filtering, block websites by category, email anti-virus and logging of visited websites per user. Beginning in 2009, Anchor Technology, Inc. selected the new Netgear ProSecure line of security appliances to take network security to a different level, and is now a ProSecure Platinum partner. Netgear had been in the network computer products for years but by acquisition invested millions in proven technology to deliver the best solutions to small and medium businesses that they can afford.

[www.anchorhk.com](http://www.anchorhk.com)

[www.netgear-prosecure.com](http://www.netgear-prosecure.com)