



Business Communication Specialists

Privacy Protected: 4 Proven Tips to Keep your Employees' Information Secure in the Workplace

Your employees put their trust in your management, and it's important to return the favor by keeping their personal information secure at all times. For both professional and legal reasons, having a secure network and protocols protects confidential data that limits your company liability, ensures you're compliant with a broad set of privacy regulations and give your employees full confidence in your operations. Following network security best practices can help improve the reputation of your firm, while preventing any negative events or publicity. There are 4 simple principles which can help keep your employees' information secure in the workplace:

Protect Daily Employee Computer Use

In the course of everyday business, your employees will communicate with countless clients, prospects and co-workers. Take steps to secure their privacy by investing in quality anti-virus and malware tools to prevent unauthorized downloads which can compromise their privacy and yours.

Setup a Secure Firewall

The first, and most important, step to take to secure confidential data is to prevent unauthorized external access. With a secure firewall and a dedicated security server, you can ensure the files cannot be taken from an external source. With data encryption you can further protect the integrity of the data at all times to ensure protected of corporate information.

Create tiered internal access

By placing your employee information on a secure server you can limit access to further ensure that information is only available to those who need it. Creating tiered security levels for each employee, protects information internally by only allowing access to those who meet the criteria specified at that level. You should audit the logs on the server regularly to ensure only authorized users are accessing these files.

Develop a Loss Protection Policy

By monitoring your servers from both internal and external access, you remain alert to any unauthorized access to the files. With a contingency response plan you can ensure any breach is mitigated and immediately addressed to limit data loss, abuse, corporate espionage or identity theft.