

TECH ADVISOR

FOR SCHOOLS, GOVERNMENT & BUSINESS

Notebook Theft and losing your confidential data

Visit **ACT4NETWORKS.COM** for more information on computer security and Internet Filtering

INSIDE OUR NEXT ISSUE:

REDUCING COMPUTER NETWORK MAINTENANCE.

ARE TAPE BACKUP SYSTEMS A WASTE OF MONEY ?

APPLIED COMPUTER TECHNOLOGIES
700 INDUSTRIAL DRIVE
CARY, IL 60013
(847) 639-7000

WWW.ACT4NETWORKS.COM

PROVIDING TECHNOLOGY SOLUTIONS FOR OVER 20 YEARS

More Information on our web site:

• Disk-2-Disk Backups

Never worry if your tape drive failed again.

Stop buying expensive tapes every year.

Free up your staff from baby-sitting your backup.

• E-mail Archiving

Are you asking for trouble by ignoring this federal mandate?

WWW.ACT4NETWORKS.COM

Did you know that 10% of all notebooks get stolen each year? What sensitive data could be lost on a school notebook? Financial records? personnel information? The school address book? Is your notebook configured to automatically connect to your network giving a thief access to even more? How much could you lose beyond the cost of the computer if someone stole a staff notebook?

To make sure that your data doesn't fall into the wrong hands, you should make sure that your notebook's data is secured. How? There are a couple of ways to make sure that no one but you can access the data on your computer.

First, consider a hardware encryption program like PointSec from Checkpoint Software. PointSec encrypts your hard drive and requires a password to complete the boot up process making your PC functionally useless to a thief.

Isn't Windows password security enough to keep people away from my data you might ask? In a word NO! All a thief has to do to bypass Windows security is remove the hard drive from your computer, attach it to another computer that he can boot

up and then read your hard drive like it's his own personal data drive. Encryption stops that cold. Unless a person has the security code, the hard drive is unreadable.

Let's talk about another data theft technique. Ever walk away from your PC and leave it running. Maybe you while you go to lunch? A data thief can plug a flash drive into your PC and copy all of your data and no one is the wiser. It gets even worse if you're connected to the network server and they steal all of that data too! Impossible? No, very easy.

How do you stop it? Encrypt any data that goes onto ANY portable device with Checkpoint Media Encryption. Anyone that needs access to data that goes out of your computer must have the proper access key to read it.

A couple of years ago, the Chicago Board of Education lost an entire data base full of employee personnel and payroll records when two contract employees went to lunch and left their computers running inside their offices. When they returned, their computers and all of the data were gone. Don't get caught unprepared like they did!

Securely Share Data with Off-Premises Workers

More and more organizations have employees that work outside of the traditional office or spend large amounts of time on the road. How do you get information to them? Do employees share documents collaboratively in your organization no matter where they are? Can they easily check their calendars? How about team-building and customized knowledge bases for everyone to reference?

Many administrators are justifiably cautious about opening up their networks to off-site workers fearing potential security risk exposure. Others rely on sending large document packets via e-mail and then become frustrated when they're stopped by aggressive SPAM filters or ISP usage rules.

Why don't you consider a secure collaboration system like SharePoint! SharePoint provides secure a document management system that allows protected access for off-premises staff as well as regular network users. Organized document management has never been so easy for small to mid-sized organizations. It doesn't require any high end technical help to maintain either. You can develop organizational calendars, and securely provide access to internal data

bases inside your network.

SharePoint can be a real boon to organizations like yours that need to manage documents and distribute information easily. You can control who reads, creates or modifies documents. You can even designate an approval process dictating who approves what documents before they are considered ready for distribution.

Not all employees need to access your entire network remotely if you've got a SharePoint collaboration system that gives them access to only what they need.

Is it expensive? Would you be surprised to know that you may already own it and it just needs to be configured for your use?

Call ACT for help in getting this valuable asset implemented on your network right away.

Can't afford to develop your own SharePoint solution? Ask about our ACT SharePoint services using our servers. It's surprisingly affordable!