IT Checklist

for Small Business

INTRODUCTION

A small business is unlikely to have a dedicated IT Department or Help Desk. But all the tasks that a large organization requires of its IT Department and Help Desk are also needed by a small business. A small business needs to make sure that those tasks are allocated either to someone within the business, or to an outside provider. This is a checklist for small business owners and managers to help them make sure they don't forget the important items.

The items are arranged in order from tasks a small business is most likely to perform in-house to tasks for which a small business is more likely to engage an outside provider.

Every business is different and has its own needs. This document presents a list of common items that may be appropriate for some small businesses. It is not designed to cover everything required in running an IT system and it may not be appropriate in all circumstances. Take appropriate advice about the specific needs of your business before taking action.

CHECKLIST

Maintaining physical security over IT equipment, backup tapes or disks etc

If someone steals your computers or your backup tapes, you lose not only the equipment but all the data on it. Physical threat is as likely to come from careless or malicious staff as well as outsiders. Make sure you have your hardware and backup tapes or disks secured.

- You have a secure, locked, air conditioned or well ventilated space for servers and other equipment that does not have to be out in the open. As few people as possible have access to this space.
- Someone in the office has been allocated responsibility for locking up the area where servers and backup tapes are stored. A backup person is organized to cover times when the primary person is unavailable because of holidays, illness etc.
- Backup tapes and disks are routinely stored off-site in a secure location.
- Where equipment is out in the open, or is left unattended for periods of time, desktop machines are locked to the desk or to a portion of the building structure.
- The business has a policy on security of laptops and mobile devices when out of the office (for example: employees may not leave laptops in a car).

Creating and maintaining in-house rules about access, permissions, passwords and other safety, security and administrative rules

Intruders, old employees and kids hacking for fun can access your business's information unless you have rules for who can access what data.

- You have written rules (perhaps only one page) on who is allowed to access what data, how passwords or pass phrases, are to be formatted, how often they expire, at what intervals they can be recycled and other security issues.
- Your rules mean that no-one ever has to share their password with another user. If users share a computer, each person has an individual profile, user name and password. People in the office know that using someone else's password is like forging their signature.
- The rules in place identify what personal use of computers and internet access is reasonable in the circumstances for this business.
- The business's rules address safety issues such as ensuring that cables do not run across hallways or walkways, appropriate numbers of power outlets are available for IT equipment and that staff follow appropriate practices in using IT equipment to prevent accidents or injury.
- You have developed a communications strategy and have allocated responsibility to someone in the office for ensuring that new employees know about the rules.
- You have allocated responsibility to someone in the office to keep the rules up to date.

Downloading and deploying daily data files for anti-virus software

Viruses are invented daily, so you need to ensure that data files for your anti-virus software are downloaded and installed daily. Viruses in this context include all forms of malware, viruses, trojans, spyware etc.

- You have set up the anti-virus software to update hourly and to send an email alert to the responsible person or, if that person is away on leave or for illness, alerts go to someone else.
- If your business runs 7 days a week, then your have someone to receive and respond to alerts on all 7 days.

IT Checklist

for Small Business

Administration: Maintaining records of software licences, domain names, service contracts for peripherals like printers, liaising with vendors

Your software licences are valuable. It's easy to install software on a machine and "forget" that it is there. It is also easy to forget what service contracts you have in place for your equipment. Finally, it is easy to forget to renew a domain name. Domain names are cheap, but very valuable. If you don't renew your domain name, someone else can register it, and you will struggle to get it back.

- You have allocated responsibility to someone to keep a list of what software is installed on every machine, with what licence to ensure that the business is complying with the licence agreements and is protecting the business's assets.
- You have allocated responsibility to someone to keep a list of what domain names and web hosting arrangements you have, with expiry dates. You have a system in place to remind you of when to renew domain names (you should renew them about 3 months in advance of the deadline).
- You have allocated responsibility to someone for maintaining a list of all service contracts. Only one person is permitted to call a vendor for service.

Answering basic questions from users about how to use the software and hardware and troubleshooting minor problems

Your investment in desktops, laptops and software licences is significant. It is no use investing in these unless your people can make use of the hardware and the software. And, while support and advice from colleagues is a good way to learn, you don't want the entire office to stop work while everyone crowds round one person's desk as they try to create a table of contents in Word.

- You have allocated responsibility to one person (with a backup if necessary) to replenish stocks of paper, toner etc for printers and fax machines.
- You have devised a process for users to get help in using software and hardware and troubleshooting minor problems (such as a printer not working). For example, the process might be that an employee first asks your in-house "power user" for advice and, if that person can't help, the employee seeks free help (eg from on-line newsgroups) or paid help (eg from an external adviser or trainer).
- Everyone in the business knows the process and you encourage them to use that process by following it yourself.
- New employees are told about the system and encouraged to use it.

Creating, maintaining and deleting users from the network

New employees need to be added as new users to the network, and just as importantly, old employees need to be removed as soon as they leave the business.

- You have allocated responsibility to one or two people to add new users to the network (this will be the 'network administrator').
- You have a system in place where a new user can be added to the network so they can be productive from the day they start work (without having to use someone else's password to access the network).
- You have a process in place to maintain a central registry of passwords to business-critical files or applications, or to retrieve passwords from departing employees. For example, an accounts clerk may have passwords to the on-line banking, or employees may have password-protected individual documents that the business will need.
- The person who calculates the final pay for an employee leaving the business is responsible for informing the network administrator that the employee is leaving. The network administrator is responsible for disabling that user from the network as soon as they receive notice.

Creating and re-setting network passwords

All new users on the network will need a password that they can change for their own needs. And whether we like it or not, users forget passwords and can be locked out of the network.

- The network has a "three strikes and you're out" policy: if a user gets the password wrong three times in a row, the user is locked out of the network.
- The network administrator can re-set the password of someone who is locked out within a very short time (say, 10 minutes). Someone is allocated as backup for this task to cover meal breaks, leave and other absences.
- The network operating system is set up so as to require users to change their network password regularly (say, every month or every 3 months).
- Password rules (eg how long a password must be, and how frequently it must be changed) are appropriate to the circumstances but are not so difficult that users are tempted to write them down.

IT Checklist

for Small Business

Installing new equipment (servers, PCs, laptops, printers, scanners etc, along with their related drivers)

In a small business, it is tempting to buy new equipment without having thought about how it will be installed. You don't want the entire business to come to a stop as 5 people try to install a new scanner "just like the one we have at home"!

- Make sure that the equipment you buy is suitable for a business network environment. Not all equipment suitable for home use will run on a business network.
- If you don't have an on-site IT pro, when you buy new equipment, consider arranging for the vendor to install it. While it will cost a little, it may be cheaper than having your staff fumbling at a task that is not their area of expertise.
- To reduce complexity, consider limiting your purchases to a few brands and types of equipment that you trust and are familiar with.
- Make sure that new drivers (eg printer drivers) are installed when you buy new equipment. Even if the new printer "seems to work" with the old drivers, make sure that everyone is using the same drivers for the same printer.

Setting up shared folders, granting / reducing permissions and managing disk quotas

Shared folders allow groups of employees to access the same files. Disk quotas restrict the amount of data that one employee can store on a server. There are security and performance implications for both.

- The business has appropriate rules in place so that people can see the data they need for their job, but data is generally secured.
- Someone (the 'network administrator') has been allocated the job of managing shared folders and granting permission to individuals or groups to see the files in those shared folders.
- Permissions to access shared folders are reviewed regularly (quarterly?) and permissions are deleted when they are no longer needed (perhaps because someone changed roles within the business).
- If appropriate, disk quotas are in place that limit the space that employees' files can take up on servers. The business server is not the place for employees to store large files they have downloaded from the web!
- All business data should be stored on the server where it can be secured, and backed up.

Downloading, assessing and deploying security patches for operating system and applications

As long as malicious users try to breach systems through security holes in software, software vendors will be issuing security patches. In 2003, hundreds of thousands of machines were infected by the Slammer virus, even though Microsoft had issued a security patch that prevented infection over 6 months earlier.

- You have considered and decided on a policy for installing security patches. For example, you may decide to install all security patches as soon as they are made available. Or, if your line-of-business or back-office systems are old, uncommon or heavily customized, you may have a policy of testing each security patch against your software to ensure that it will still work properly.
- You have allocated responsibility to one person for downloading, assessing (if necessary), and deploying security patches for the operating system and applications (line-of-business applications, back-office systems and desktop applications).
- You have a process in place (perhaps a routine security audit by an external person) to check that security patches are being deployed appropriately.

Setting up and maintaining the connection to the internet and liaising with the ISP when there are connection problems

For most businesses, the connection to the internet is vital. The market remains volatile and ISPs are routinely dropping prices, increasing service speeds and broadening service offerings. You may not want to change ISP every 6 months, but you should stay aware of changes in this market.

- In choosing an ISP, you explore a wide range of possible vendors to get the services you need and the best value for money.
- Someone has been allocated responsibility of managing the technical aspects of connecting to the internet. This might be the 'network administrator'. This person deals with the ISP about problems with the connection.
- Someone has been allocated responsibility for regularly checking competitive pricing and service offerings from ISPs.

IT Checklist

for Small Business

Making, testing, and restoring backups (from whole servers to single files)

What is your data worth? If you lost everything, how long would it take the business to be up and running again? What would it cost, in time or money, if your business lost the last month's data? A backup is only as good as what you can restore!

- You have a documented backup process and you have allocated responsibility to someone for backing up data from servers every day. This includes reviewing the backup log for any issues relating to the success or failure of the backup, and responding to those issues. Someone is available, and is trained, to cover for your main person if they are away for a day.
- You have a documented restore process and you regularly (monthly? quarterly?) test that you can restore data from your backups.
- At least some backup media are stored off-site. For example, if you back up every day, you might store every second day's data off-site. It may be appropriate to keep regular permanent backups offsite, such as a backup of financial data after each end-of-month procedure is completed.
- You have a policy that requires users to store data that is crucial to the business on the server. If a user stores a file on a desktop computer, that file will not be backed up during the normal backup process.

Disaster recovery (eg after prolonged power failure, fire, flood, theft)

Your business may depend on your IT system, and so you need to know that the business will survive even if the IT system is destroyed or damaged.

- You have acted to prevent disasters by installing surge protectors, power conditioning and uninterruptible power supplies. You have software in place to enable a controlled shutdown of servers and you have tested these systems.
- You have a plan in place for how to get your business up and running again. For example, some businesses make an arrangement with a similar business to act as a "warm site" so that there is at least one computer in their office that you could use to load your backup and get your business running again.
- You have written out the steps to be followed after a disaster. Remember that as owner or manager, you may not be available after a disaster to perform work like this, or even direct it.
- You have ensured that the relevant employees in the business know where to find the disaster recovery instructions and how to follow them. That probably means that the procedures are printed out, and are preferably far away from the disaster area.
- You have practised your disaster recovery steps at least once with the current team of people.

Troubleshooting network problems involving the WAN or LAN (including routers, firewalls, bridges, switches, cabling, wireless access points and devices etc) and setting up and maintaining systems for remote users to log in to the network from home or while travelling

Perhaps the most frustrating IT problem is when "the network goes down". It can be difficult to pin point the source of the problem and unless you have a networking expert in-house, you may need external help.

- You have consulted with an expert in security related to your operating system and are confident that your network is secure. This is especially important if you have a wireless network.
- The network administrator has written down the all the user names, passwords and settings for all network-related equipment. That information is kept securely, but is available to those who may need it to repair network problems.
- You have arranged that at least one person is available at all times with basic knowledge of how the network operates. You have arranged for a network expert to write down basic trouble-shooting steps for your in-house person to follow in the case of problems.
- You have established a working relationship with an external specialist who is familiar with your business and your network set up and can be available at short notice to fix urgent network problems.

Deploying existing software to new users, setting up new software and deploying new software to existing users

This task needs to be undertaken with some care. First, to ensure that the software is installed and set up appropriately and second, to ensure that licensing arrangements are followed.

- If you have an IT Pro in-house, then you have discussed how software is to be deployed and set up. You are confident that software.
- If you do not have an IT Pro in-house, then you have established a working relationship with a professional who can guide you in deploying and setting up software. You have a firm understanding within the business of when tasks will be done in-house and when you will call in outside help.

IT Checklist

for Small Business

Training users in how to use new software and hardware

The more your users know about the software they use every day, the more productive they can be. You don't want office staff wasting time on page numbers every time they have to produce a Word document when a few hours of training would teach them how to do it once and for all. Few users manage to teach themselves anything beyond the basics, but sending people to generalist "Introduction to X" or "Intermediate Y" courses often doesn't help. To be effective, you have to be specific.

- You have talked with the staff of the business and written down what tasks they need to perform using their software.
- You have made plans to get appropriate information or training for them to perform those tasks effectively and efficiently.
- You have a way of checking back with employees soon after training about whether they can now perform the relevant tasks. If skills learned in training are not used on the job immediately, they may be lost and the training will have been wasted.

Cleaning up machines that have been infected with viruses, trojans, worms or other malware

In spite of your best efforts, some machines will get infected with viruses or other malware. (Laptops are more vulnerable than desktop machines.) You need them cleaned up properly, and in the case of severe infection this is a job for an expert.

- You have decided how you will isolate infected machines from the network, and employees know when to tackle the clean-up job themselves and when to call in an expert.
- If you don't have an IT Pro on staff, you have established a working relationship with an IT Pro who can be available to clean machines at relatively short notice.

Customizing software to suit the needs of the business

"Customizing" can mean lots of things: writing a quick macro in PowerPoint, creating a stand-alone application based on Excel, or writing customisations that live within your line-of-business application or accounting system. Sooner or later, most small businesses will do one of these. Some can be done in-house by "power users", but if it's something that is important to the business (and not just important to the user), you need a professional.

- You have decided what customisations are appropriate for your business and decided, in general terms, how they will be created. When is it appropriate to let the in-house "power user" have a week or two to work on some Word macros, and when will you call in an expert?

Server management (eg mail server, web server)

Even micro businesses may run a server to manage mail, but many small businesses will run print servers, mail servers, and maybe web servers for intranet or internet sites. Server administration is a specialist skill and few small businesses would have an in-house expert.

- You have consulted with an expert administrator of your servers to write out the routine steps to follow for good administration of the database.
- You have appointed someone as responsible for undertaking those routine steps.
- You know what you can do in-house and when to call in an expert and have communicated this to staff.
- You have established a working relationship with an external specialist who is familiar with your business and your server set up and can be available at short notice to fix urgent server problems.

Database administration (eg SQL server)

Very small, or micro, businesses may not run a significant database. But most line-of-business applications and medium-to-large accounting systems rely on an underlying database. Database administration is a specialist skill and few small businesses would have an in-house expert.

- You have consulted with an expert administrator of your database (Microsoft SQL Server, MySQL etc) to write out the routine steps to follow for good administration of the database including securing the database and backing it up.
- You have appointed someone as responsible for undertaking those routine steps.
- You know what you can do in-house and when to call in an expert and have communicated this to staff.
- You have established a working relationship with an external specialist who is familiar with your business and your database set up. You have arranged for that specialist to run brief regular (quarterly? six-monthly?) checkups and be available to fix urgent database problems.

This checklist has been prepared in consultation with CPA's Information Technology & Management Centre of Excellence.

CREATIS 7814 04/05