

IT DISASTER PREVENTION

Action List

1. Consider how serious the **consequences** of system failure, misuse or data loss could be; use this to decide how much to invest in disaster prevention.
2. **Purchase proven** equipment and software; try to avoid bespoke systems.
3. Arrange any external **support** you may need: for example, installation, maintenance, training, troubleshooting and disaster recovery.
4. **Physically protect** your equipment; use surge protectors or uninterruptible power supplies and ensure that your premises are secure.
5. Establish **security** procedures (eg password control) and use anti-virus software and an Internet firewall.
6. Assign **responsibility** for the system to one individual; provide appropriate training and clear guidance on when to call on external experts.
7. Train **employees** how to use your IT system and specify what tasks must be referred to others; establish a procedure for reporting faults or problems.
8. Establish and implement an email and **Internet policy** to regulate employees' use of the Internet and to minimise the risks of a virus entering your system.
9. Restrict **software installation** and configuration to authorised, trained personnel; ban employees from installing unnecessary software.
10. Establish a safe installation and **upgrade procedure**, including backing up data, updating your anti-virus protection and running parallel systems while testing if necessary.
11. Carry out regular **routine maintenance**: for example, cleaning equipment, running system utilities, archiving old files and testing system performance.
12. Establish an effective daily **back-up** procedure, and store back-ups securely off-site; regularly test to ensure that you can restore data.
13. Keep clear **records** of system configuration, software versions and upgrades or patches; securely store copies of software and updates.

14. Prepare **contingency plans** in case of disaster, including manual systems for maintaining key operations; consider insuring your system and data.

Cardinal Rules

Do:

- **protect** your system physically and with appropriate software and procedures
- **train employees**
- identify and arrange any **external support** you need
- **back-up** your data
- make **contingency plans**

Don't:

- allow untrained employees to **install** unnecessary software
- ignore the need for **routine maintenance**
- assume that **procedures** will always be followed

Copyright © Business Hotline Publications Ltd, 2003. All rights reserved

