

Countering and reducing ICT security risks

1. Physical and environmental risks

1. Physical and environmental risks	Reducing the Risk
Theft of equipment from staff areas and Theft of equipment from public areas	Insurance (applies to all topics) Physically locking down with cables etc Record serial numbers Burglar alarm/bars, window locks General office security, know who's on site etc Marking equipment (Selectamark) Policy and rota for locking up Lockable cabinets Monitoring Cameras
Theft of equipment off the premises (e.g. laptops)	Check insurance coverage for offsite Staff awareness Usage policy Password protection Lock in secure cabinet when in office Do you really need to use the laptop or can you just take data with you on memory pen, CDR? Sign in and out procedure
Fire!	Good backup policy Policy for equipment use Fire alarms/extinguishers (ensure staff know which type of extinguishers to use on electrical equipment) Sprinklers (ensure critical equipment cannot be affected by water damage) Portable appliance testing (reduce risk of electrical fires) Don't leave equipment on standby Fireproof safe important documentation
Flood	Keep equipment away from water sources (pipes etc) Raise equipment off ground "Flood rescue policy" – or disaster policy
Power Surge / Outage	UPS (Uninterruptible Power Supply) on important equipment (servers, router, switches etc) Surge protection/circuit breakers on other equipment Don't plug high powered equipment into extension leads with computing equipment on them e.g. heaters etc
Loss of back up media	Fireproof safe Copies offsite Multiple back ups (don't rely on one tape/CDR/DVD) Check back up is working and that can restore Backup policy and routine to be adhered to

2. Data Risks

2. Data risks	Reducing the risk...
Files being deleted accidentally	Regular backup and restoration check (applies to most topics) Backup policy (ditto) Staff training and awareness (ditto) Passwords/restrictions Read only folders Training and induction for staff
Files being deleted maliciously [e.g. by discontented staff (or ex-staff)]	Folder permissions Account management (change passwords) Contracts and policy
Files being corrupted or infected by viruses	Anti virus (install, run, update automatically & check) Firewall updates Disk maintenance Staff awareness of virus activity and suspicious emails
Files being viewed by unauthorised staff	Permissions Log on screen savers, lock workstation when away from desk
Users installing unlicensed (or unapproved) software	Acceptable use policy Group policies Block download access through firewall Management of licences/software media resources etc Operating system tweaks
Database alterations by unauthorised staff	Passwords on database access Access restrictions Configurable permissions for users e.g. read only etc. Policy and training
Data being viewed by contractors	Confidentiality policy/agreements Contract
Loss of data on mobile devices e.g. memory keys, CDRs, Portable Hard drives, floppy disks	Don't put anything important or irreplaceable on mobile devices Security programs Thumb print recognition Don't use as whole-system back up devices
Technical support staff having full remote access rights to systems	Confidentiality policy/agreement Use of web based support tools which request rather than permanently open access Change password if changing company
Unauthorised use of server administrator password	Only key users to know this Confidentiality policy/agreement

3. Breakdowns and Maintenance Risks

3. Breakdowns and maintenance (PCs and Servers combined)	Reducing the risk...
Hard drive crashing or dying – risk of data loss	PC and server warranties (applies to all topics) Plan ahead financially and strategically (ditto) Tech support and Service Level Agreement (SLA) (ditto) Regular maintenance (policy issue) Spare disc/redundancy/RAID (Redundant Array of Independent Disks) on server Back up Don't keep important stuff on PC drives if have server
Power supply dying	Surge protectors on PCs UPS (Uninterruptible Power Supply) on server and critical PCs Redundant power supply on server
Memory failing	Check event logs for errors Replace hardware as policy
Other failures- motherboards, drives, graphics cards etc.	As above Data recovery costs (high!)
Operating system (OS) unsupported (e.g. Windows 95, 98, NT Workstation, NT Server)	Upgrade to supported OS If can't then ensure firewall etc. is secure
Potential security risks through operating system not being updated	Download and install automatic updates Service packs Check updates are being applied

4. Network Security Risks

4. Network security Risks	Reducing the risk...
No log on passwords	Policy issue Set up and change regularly! Use unusual/varied passwords not names, postcodes etc Complex server password Set up on server for agreed period (e.g. 3 months)
Server being used for spam relaying	Firewall Maintain firewall
Unsecured wireless network	Set WEP (Wireless Encryption Protocol) security (as minimum) Consider cabling? Secure SSID (Service Set Identifier) broadcasts (change name of SSID from default)
Staff able to plug in unsecured USB (Universal Serial Bus) devices	Policy Block USB ports/CDROM/Floppy Scan any media plugged in using security monitoring program (large orgs only)
No passwords (or defaults being used) on routers and firewalls	Password protect / change password from default

5. Internet Use Risks

5. Internet Use Risks	Reducing the risk...
Email used for sending confidential information	Email/Internet Policy (applies to many topics below) Encryption/digital signature/ certification Use alternatives such as fax or post Password-protect documents
"Pop-ups" and browser hijacks (malicious software installs and takes over your web browser)	Use alternative browser such as Firefox Pop up blocker Anti-spyware programs – install, run regularly and update
Spam	Anti-spam software Don't publish easily harvestable addresses on website Don't send mail to multiple
Phishing attacks (directing you to fake websites that try to steal information such as credit card numbers)	Policy/awareness by staff Anti-spam software
Online purchasing of personal items	Blocking of secure sites (firewall) Blocking through use of software or online service Request invoices for good rather than using credit cards
Visiting unsecured or offensive sites	Policy Blocking through use of software or online service
MSN Messenger for personal or unauthorised use	Can be blocked on firewall but can also be got around due to behaviour of MSN
Downloading and installing programs/toolbars from unknown sources	General awareness
Downloading of copyrighted music and video files through files sharing sites ("torrent", Peer to Peer)	Policy
Website hosting is insecure	Check hosts Service Level Agreement etc.

For an explanation of any unfamiliar terms try the [ICT Hub Knowledgebase Glossary](#)

Copyright © 2006 Superhighways Partnership and Lasa Information Systems Team



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 2.0 UK: England & Wales License](#).