Desktop Computers Standards and Guidelines

Section 1 - Scope

(1) These standards and guidelines cover the use of desktop computers or laptops, which are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units. Desktop computers or laptops include IBM-compatible personal computers (PCs), Macintoshes, and Unix Workstations.

Section 2 - General Obligations

(2) Users and custodians of Desktop computers are subject to the "Conditions of Use" and "Code of Practice" specified in the University's IT Security Policy.

Hardware Security

Generally, staff must:

a. Lock offices when not present. Office keys should be registered and monitored to ensure they are returned when the owner leaves the University.
b. Secure desktops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.
c. Secure hard disks. External hard disks should be secured against access, tampering, or removal.
d. Mark personal computers clearly with the name of the owner.
e. Locate computers away from environmental hazards.
f. Store critical data backup media in fireproof vaults or in another building.
g. Register all University computers with the IT Service Desk.

Access Security

(3) Utilize provided password facilities to ensure that only authorized users can access the system. Please refer to the "General Password Policy" for more information.

(4) Generally:

a. Where the Desktop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures.
b. If staff need to leave their desks during the day (e.g. morning tea, lunch), the console should be locked to prevent casual access to their files.

Data and Software Availability

(5) Users should back up and store important records and programs on a regular schedule.

(6) Departmental data must be stored on central data servers i.e. departmental network shared drives.

(7) Users should:

a. Check data and software integrity.
b. Fix software problems immediately.

Confidential Information

(8) Users should:

a. Encrypt sensitive and confidential information where appropriate.
b. Monitor printers/Facsimile machines used to produce sensitive and confidential information.
c. Overwrite sensitive files on electronic media (CDs, floppy disks, fixed disks, data tapes, or cartridges) and destroy/shred before being disposed of in the rubbish.
d. Ensure that paper documents or fax film rolls with private information that is no longer required are cross-shredded to discourage "Dumpster Diving" (where an intruder could retrieve confidential information from the trash bins) or use a document shredding service.

Software

(9) Software is protected by the Copyright Act. Unauthorized copying is a violation of University Copyright policies. Anyone who uses software should understand and comply with the license requirements of the software. The University is subject to random license audits by software vendors. If in doubt, please check with the IT Service Desk on software licensing.

(10) Auditing of Staff Desktop PCs will be conducted by IT from time to time to ensure that the University is in compliance with copyright laws and acts.

Viruses/Worms

(11) Computer Viruses/Worms are self-propagating programs that infect other programs and systems. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

(12) To decrease the risk of viruses and limit their spread, users should:

a. Check all software before installing it. Generally, staff should NOT install share/freeware downloaded from the internet.
b. Use software tools supplied by IT to detect and remove viruses.
c. Use firewall software (supplied with some OS's).
d. Isolate immediately any contaminated system (i.e. physically remove the network connection).
e. Report any infections or strange activity (such as constant hard drive activity) to the IT Service Desk.

Computer Networks

(13) Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

(14) While IT has responsibility for setting up and maintaining appropriate security procedures on the network, each

individual is responsible for operating their own computer with ethical regard for others in the shared environment.

(15) The following considerations and procedures must be emphasized in a network environment:

a. Check all files downloaded from the Internet. Avoid downloading share/freeware files.
b. Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on University networks.
c. Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers.
d. Always backup your important files.
e. Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over a University network.
f. Never store University passwords or any other confidential data or information on your laptop or home PC or associated floppy disks or CD's. All such information should be secured after any dialup connection to the University network.
g. The use of Modems attached to University networked workstations is prohibited.

Status and Details

Status	Historic
Effective Date	27th July 2015
Review Date	14th January 2015
Approval Authority	Chief Information Officer
Approval Date	14th November 2011
Expiry Date	6th June 2017
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Robert Irving Chief Information Officer
Enquiries Contact	Technology and Digital Services +61 2 6773 5000