

# School of Computer Science and Engineering policy with regard to self-administered computers

CSE Computer Security Committee

October, 2002

## Abstract

The School's Computing Support Group (CSG) provides a range of services to the computers located within the School or connected to the School's own networks.

As well as directly administering the majority of the school's servers, desktops and lab computers, the CSG allows for and provides facilities for those who choose to administer their own computers.

It is necessary though, that these 'self-administrators' ensure that their computers do not behave in ways that interfere with the operation of other computers, either within the School or external.

This document describes the resources provided by the CSG to those who self-administer their computers and sets out the requirements that these self-administrators must satisfy in order to be connected to CSE infrastructure.

## 1 Concepts and Definitions

The School of Computer Science and Engineering (the School) provides computing facilities (network infrastructure, servers, workstations and peripheral devices) for the use of staff and students of the School. The School's Computing Support Group (CSG) provides support for these facilities. The School recognises the following classes of computer:

**School computers:** computers (and associated hardware such as printers, monitors and keyboards) which are purchased using the School's Operating Funds.

**Non-school computers:** computers (and associated hardware) purchased using research grants or work/study-related funds other than the School's Operating Funds. These computers still remain a 'school asset'.

**Private computers:** purchased from other funds, often paid for by individuals.

**Virtual computers:** created by such tools as VMware. They have no physical existence but otherwise behave in the same way as real computer hardware. It is possible for a self-administered computer to run a CSG-administered Virtual computer.

The CSG also recognises ‘owners’ and ‘users’ of a computer. The owner is responsible for the presence and operation of that computer on the School’s network. The CSG owns all School computers and CSG-administered Virtual computers. All other computers (Non-school and Private computers and non-CSG-administered Virtual computers) must be owned by a person who is accountable for the computer and who the CSG and others can contact regarding that computer. Non-school and Private computers are owned by the person who provided or authorised funds for their purchase. Virtual computers are owned by the owner of the computer running the tool that created them. A person may own more than one computer.

The ‘primary user’ of a computer will either be the owner, or a person nominated by the owner to whom the computer has been allocated for use on a day-to-day basis. The CSG will ordinarily deal with the primary user (henceforth referred to as ‘the user’), however the owner is finally responsible for all issues pertaining to the computer.

Any computer on the School’s network is either CSG-administered or is self-administered. That is, either the CSG or the user has ‘administrative access’ to the computer. Administrative access confers the ability to perform actions such as: reconfiguring the operating system; installing software or modify files not owned by the user (unless specifically granted access by the owner or by an administrator); affecting the operating environment of users other than themselves; and changing or installing device drivers and modifying the hardware configuration (except for optional or removable components such as external USB or serial devices).

‘Software support’ consists of:

1. the installation of one or more separately bootable operating systems on the one computer.
2. the configuration of the operating systems to allow (at a minimum): connection to the School’s Ethernet or wireless networks; use of the School’s WWW and FTP proxies; use of the School’s printers; sending and receiving email through the School’s email system; and the access of the user’s home directories on a CSG-administered computer.
3. the maintenance of a standard single-boot CSG-installed operating system.<sup>1</sup>

Software support includes installation and configuration of application software where this requires administrative access.

‘Hardware support’ consists of repair or maintenance of a computer or its component parts (including keyboard, video display and mouse), as covered under the warranty agreement, when these break or fail to perform their expected function.

---

<sup>1</sup>The CSG may assist in the installation of multi-boot systems but will not subsequently support them.

## 2 CSG administration of computers

A computer is deemed to be CSG-administered when its operating system has been installed and configured by a member of the CSG and administrative access to the computer is restricted to the CSG (only CSG staff have legitimate root or administrator access to the computer). CSG-administered computers have locking or sealing mechanisms to prevent them from being opened and their BIOS and hardware removed or tampered with. The CSG very strongly recommends users of other computers similarly lock down their computers.

When the CSG administers a computer they ensure that the computer is operational and usable. This means that one of the School's standard operating systems is available on the computer and that standard applications are also available. The operating system and the applications will run and operate correctly; a user on the computer will have reliable access to School network resources such as printers and their home directory; and they will be able to access the Internet.

Any problem or failures during the expected life of the computer will be resolved or repaired by the CSG.

For School computers the CSG will undertake any repairs or upgrades to ensure the computer will operate satisfactorily. For Non-school or Private computers the owner is responsible for any repairs and upgrades.

While being administered by the CSG all aspects and configuration of the computer, the operating system and any installed applications which can affect the usability of the computer are under the sole control of the CSG. This includes hardware configuration (excepting removable devices such as USB devices), network configuration, installed application software (where such software requires administrative privileges to install).

Users of CSG-administered computers can request configuration changes to those computers. Where practical, such requests will normally be honoured.

## 3 Self-administration of a computer

Administrative access includes 'root' (Unix/Linux) and 'administrator' (Windows) privileges. Since access to the inside of a computer can allow administrative access to be achieved, this also is considered to be a form of administrative access.

A computer is considered to be self-administered (that is, not CSG-administered) when any user other than CSG staff has available, gains or uses administrative access to that computer.

By self-administering a computer, the user takes responsibility for ensuring that the computer is usable for its intended purpose. This includes providing support, updating configurations, upgrading software, ensuring the computer is as secure as possible from internal and external threats, installing the latest security patches and anti-virus updates, and diagnosing problems. The user also takes responsibility for a number of services that the CSG normally provides, such as backups. See Section 7 for more detail.

Before being initially connected to the School's network, or after any Operating System installation, a member of the CSG may conduct a security audit on any self-administered computer.

## 4 Gaining and relinquishing self-administration

A user must have the consent of the owner to gain administrative access to a computer. If the user is a student then they must also have the consent of their supervisor. An email from the owner—and supervisor, if applicable, affirming their consent—must be copied to the CSG (System Support). The CSG must also be informed of any proposed changes to the computer that affect its connection to the School's network, for instance the installation of a new interface or operating system.

An owner may relinquish the administrative access of a user at any time and request the computer become CSG-administered. The CSG will then reformat the hard disk (obliterating *all* data), reinstall a standard operating system and applications onto the computer, and seal the computer. It is up to the user to retrieve any data they require off the hard disk before the computer is turned over to the CSG.

## 5 Operating systems and software available for self-administered computers

The CSG can make available a standard operating system and standard applications for any self-administered computer. The standard operating systems include the Debian and Redhat distributions of Linux, Windows NT 4.0 and Windows 2000, and Mac OS-9 and OS-X. Standard applications typically include compilers, editors, database systems, office products (spreadsheets, word-processors, etc.), WWW browsers, email clients and virus checkers. This list of applications varies with different operating systems.

Some of this software is also available for other computers (such as Personal computers), depending on licensing restrictions. Otherwise, procuring, licensing, installing and configuring software on self-administered computers is the responsibility of the owner.

## 6 Support of self-administered computers

Installation, configuration, problems and difficulties of self-administered Non-school, Private and Virtual computers are the responsibility of the owner. The CSG will generally help where and when it can with problems on self-administered computers, but this will depend on the nature of the problem and other issues at hand. The CSG has many responsibilities, few resources and other priorities. It may be that the only support that the CSG can reasonably offer is to reformat the hard disk and reinstall the operating system.

The CSG will ensure that access to CSE infrastructure is available for correctly configured self-administered computers. This includes access to the network, to printers and to home directories on CSG-administered servers.

For School computers the CSG will ensure that the computer hardware is operational and will repair or replace such computers which fail or break as a result of ordinary usage during the expected lifetime of the computers.

Hardware problems for other computers are the responsibility of the owner. The CSG will rarely be able to assist.

## 7 Responsibilities of the User

When gaining administrative access to a computer the user takes on responsibility for tasks normally performed by the CSG. This includes but is not limited to:

1. Complying with School and University rules and policies regarding use of computers.
2. Installing and configuring the operating system and application software. This covers all aspects of the system: for instance, creating printer configuration files and ensuring root mail is sent to the user rather than to root@cse.unsw.edu.au.
3. Maintaining and upgrading software. The CSG strongly recommends users join the appropriate mailing lists so they will be apprised of news and alerts concerning their software. Many software distributions have (semi-)automated update mechanisms; these are particularly useful for getting security updates for software.
4. Ensuring data and work stored on the self-administered computer is backed up. The CSG will continue to back up the user's home directories on CSG-administered servers.
5. Securing the computer and monitoring and maintaining the security of the computer. Section 8, *Securing CSE* covers this in more detail.

## 8 Securing CSE

### 8.1 Why Bother with Security

Security of CSE computers is required for a number of reasons:

**Shared resources:** The School's computing infrastructure, the campus-wide network and the Internet beyond is a collection of shared resources. The effective use of those resources depends on a high degree of co-operative responsibility by all users of them. Anything that impinges upon the fair use of those resources by others is a *bad thing*; and much of the security infrastructure is about preventing any (intentional or accidental) misuse of or denial of access to those resources.

**Criminal activity:** Computers and computer networks can be used for a number of criminal purposes. These might relate directly to crimes; or to gaining or sending information that breaches various laws.

**The good name of the School and the University:** The School of Computer Science and Engineering and the University of New South Wales are held in high regard nationally and internationally. Our continued success as a leading educational and research institute depends on, inter alia, maintaining that high regard. Any activity that reflects poorly on our good name is of itself a *bad thing*.

The purpose of security is to prevent, detect, monitor and remedy any of this *antisocial behaviour*. Typical examples of unsocial behaviour include Denial of Service attacks; transmitting viruses, etc; port scanning; and packet sniffing.

## 8.2 Breaches of Security

Any computer engaged in such antisocial behaviour will normally be isolated immediately and will not be reconnected until it has passed a security audit by CSG. It may be necessary to reformat the hard disk and reinstall the operating system.

When a member of the School is responsible for this antisocial behaviour they will be subject to the University's disciplinary proceedings as well as any criminal codes that might apply.

Such activity is often instigated by an unauthorised user: anybody not authorised by the owner or user of the computer who gains access by any means. Such access is commonly gained by using worms, viruses, trojans and other bad stuff that exploit various vulnerabilities in the setup of the computer. A computer thus compromised is often a platform for attacking other computers. These vulnerabilities are often the result of:

- poorly chosen or well-known passwords;
- poorly written software (whether buggy or poorly designed);
- poor configuration of software and systems ; or
- poorly secured hardware (such as allowing access to a computer where someone is already logged on or allowing booting from a floppy).

Hence, effectively securing a computer consists, first and foremost of eliminating these vulnerabilities.

## 8.3 Achieving Security

The basic aspects of securing a computer are:

**Physical security:** preventing them being stolen or being opened; having their BIOS or hardware tampered with or removed; or allowing the computer to be booted from a floppy or other removeable device.

**Configuring with security in mind:** selecting software and configuration options with security of the system being a primary concern. This includes choosing secure passwords.

**Essential services only:** reducing the number of things that can be attacked. Most computers only need to accept SSH connections for satisfactory use. Listening for other connections (NFS, ftp, WWW, etc) increases the number of vulnerabilities that might be exposed and exploited. As a general principle, turn off **all** services; then only turn on that services that are found to be essential.

**Current software:** staying up to date with virus signatures and security updates. New viruses often reach CSE within a day of being reported overseas. Vulnerabilities in other system and services are similarly exploited within days of discovery. It is essential to regularly to check for and to install software updates from a reliable source. This should be done at least weekly.

**Ongoing watchfulness:** monitoring system security is essential. This will vary from system to system, but will include making sure that monitoring tools are running and checking reports and logs from those tools and from other system services.

More details on securing a computer system are available at ...

As part of its charter to maintain security of the CSE network, the CSG regularly security scans of computers on the network and sends warnings to the users and/or owners of any computers which have been compromised or which appear to be vulnerable. If the issue is critical then the computer will be isolated and will not be reconnected until it passes a security audit. Similarly, if the owner or user is not able to satisfactorily secure the computer, then it may be isolated for the protection of the rest of the network.