16.3 Computer equipment and software

Policy summary

As the custodians of a large amount of electronic information that is either legally, personally, commercially or politically sensitive, all Corrective Services NSW (CSNSW) staff have a duty to ensure that the security of information is maintained.

CSNSW expects its employees to protect its information against accidental or unauthorised modification, disclosure or loss.

Management of Public Correctional Centres Service Specifications

Service specification	Safety and security

Scope

This section applies to all correctional centres and other facilities administered by or on behalf of CSNSW, and all CSNSW employees.

Table of contents

1 Computer equipment and software

1.1 Use of computer equipment in CSNSW locations

The following conditions apply in relation to the introduction of computer hardware, the use of CSNSW telephone lines and access to the internet at all CSNSW locations. This includes:

- correctional centres
- police/court cell complexes
- the Court Escort Security Unit (CESU)
- transitional centres.

The Officer in Charge (OIC) must ensure that their staff comply with these conditions:

- prior to taking into a correctional centre any computers, modems, storage device or other computer equipment, staff must obtain the approval to do so from the Governor or General Manager (GM), CESU
- staff are not permitted to connect any computer hardware to a CSNSW telephone line or network without the approval of the Governor or GM, CESU
- a general level of internet access granted to all CSNSW staff is accessible from any corporate computer that is connected to the network.

An officer entering a correctional centre to undertake specific tasks that relate directly to that officer's work role is not required to comply with the above conditions.

Certain external providers may, with the approval of the Commissioner, bring an internet-enabled laptop into a correctional centre when this is essential for the provision of the service they are contracted to supply. The Governor, in consultation with the service provider, must determine whether the equipment will be:

- stored in a secure location within the centre when not in use, or
- taken into and out of the centre by the service provider.

Any external provider approved by the commissioner to bring an internet-enabled laptop into a correctional centre will be added to the list *Authority to bring a mobile phone into a correctional centre* on the Custodial Corrections intranet page, as such equipment falls under the definition of a mobile phone **(refer to COPP section 16.16 *Mobile phones and other devices*)**.

Under no circumstances are non-Department of Justice issued computers, including laptops with connections to the internet, to be attached to the CSNSW network. Such connections can seriously compromise the security of CSNSW systems.

1.2 Unauthorised software

To protect CSNSW from virus outbreaks, copyright violations, and unauthorised software must not be installed on CSNSW computers. It is vital that this policy is enforced in all CSNSW facilities.

Unauthorised software is defined as software that does not have the approval of Digital & Technology Services (DTS). If particular software is required for work related purposes, DTS must be contacted so that a proper evaluation of the product can be conducted.

If already evaluated software provides the same functionality as the requested product, then to reduce complexity the already evaluated product should be used (refer to section 7.2.4 of the *Information security policy*, available on the DTS Intranet site).

All Governors, GMs and OICs must ensure that unauthorised software packages are not introduced into any of the computers at their correctional centres or other CSNSW facilities.

If there is any doubt concerning the status of a software package (i.e. whether it is authorised, unauthorised, or suitable for evaluation, Governors, GMs and OICs are to instruct their staff to contact the DTS Desk by telephone on (02) 8688 1111 (choose option 3) for advice.

1.3 Unauthorised use of computers

Governors, GMs and OICs of other CSNSW facilities are reminded that it is their responsibility to ensure that the integrity of the data contained within the CSNSW's corporate systems (e.g. Business Information Management System (BIMS), Offender Integrated Management System (OIMS) is not compromised by unauthorised use of the computers accessing the data. A review must be conducted on a regular basis to verify that the access staff have to computer systems is required for their work.

All CSNSW staff must be made aware that information available through CSNSW corporate systems is strictly confidential and must not be disclosed to unauthorised persons under any circumstances. All staff must be aware that deliberate misuse of CSNSW information may result in criminal prosecution.

Governors, GMs and OICs must ensure their staff are aware they:

- must never permit anyone to use their Access Account or Password to a corporate system
- must log off at the completion of any query or update of a corporate system
- must never leave their desk or work location with their computer or terminal still accessing a corporate system
- must regularly change personal passwords to all corporate systems to which they have access and
- must never use the same password to access different corporate systems.

1.4 Repair and servicing of computer hardware

Repair and servicing of computer hardware must always be in line with the conditions of the hardware's warranty. Governors, GMs and OICs must ensure that they have records of the warranty conditions for all the computer hardware used by their staff.

If there is any doubt as to the warranty conditions for a piece of hardware, Governors, GMs and OICS must instruct their staff to contact the designated System Support

Officer for their complex or region, or the DTS Desk by telephone on (02) 8688 1111 (choose option 3) for advice.

Under no circumstances are CSNSW staff to violate a current warranty by the unauthorised repair or servicing of computer hardware.

Governors, GMs and OICs must ensure that computer hardware (e.g. PCs, laptops, or servers) removed from their facilities for repair, servicing or transfer to another facility does not contain:

- data of a corporate nature
- data that may compromise security
- data that would breach CSNSW obligations to protect the information it possesses on staff and inmates.

Any queries with regard to the removal of such data from hardware should be directed to the designated Systems Support Officer for their complex or region, or the DTS Desk.

2 Quick links

- *Related COPP*
- *Forms and annexures*
- *Related documents*

3 Definitions

BIMS	Business Information Management System
CESU	Court Escort Security Unit
COPP	Custodial Operations Policy and Procedures
CSNSW	Corrective Services NSW
DTS	Digital & Technology Services
GM	General Manager
OIC	Officer in Charge

4 Document information

Business centre:	Custodial Operations
Approver:	Kevin Corcoran
Date of effect:	16 December 2017
EDRMS container:	18/7574

Version	Date	Reason for amendment
1.0		Initial publication
1.1	12/03/20	General formatting update and improvements
1.2	26/11/20	Amendment at [1.1] *Use of computer equipment at CSNSW locations* to prohibit connection of non-Department of Justice computers to the CSNSW network.