Commonwealth OMBUDSMAN

Staff ICT Guidelines

Endorsed 25 August 2009

POLICY NO. **06|2009**

Introduction

Maintaining the confidentiality, integrity, and availability of the Ombudsman's office services and information is extremely important to office reputation and function. The Information and Communication Technology (ICT) systems are pivotal to this security and are susceptible to threats. These threats are constantly changing; therefore the office needs to be continually vigilant in defending itself against security issues.

Scope of this policy statement

This policy deals with the security of our technology resources and the associated responsibility of authorised users when accessing these ICT resources. These resources include, but are not limited to:

- the corporate network
- computer systems and software
- access to the internet
- electronic mail
- telephones and related services.

ICT security management framework

The Ombudsman's office is subject to the Australian Government – Protective Security Manual (PSM). Under the PSM it is a requirement that the office has a security management framework.

The office has established two specific roles an Agency Security Advisor (ASA) held by the Director – Finance, and an Information Technology Security Advisor (ITSA) held by the Director – Information Technology (IT)/Business Improvement Team (BIT).

The ASA and ITSA ensure that security measures taken to protect the office environment and IT systems are appropriate and effective. They are responsible for the preparation and updating of this policy.

The ITSA is responsible for undertaking frequent audits to ensure that staff are complying with published agency security policy and procedures.

Using Desktops and Office Provided Systems

Access to our ICT systems

All users (staff and contractors) of the office ICT services commence with the office by signing a number of documents including Use and disclosure of personal information indicating that they have read and understand their responsibilities outlined in this policy.

Access to ICT services is initiated by Human Resources and is authorised by the relevant office manager/officer/supervisor. All changes are approved in writing by the Director of IT/BIT and actioned by the ICT support team.

ICT access will cease upon termination of employment/contract or from the date the staff member is listed as inactive (in the case of temporary transfers). At the request of Senior

Management, access may also be restricted on the grounds that the user may have breached this policy.

Passwords

- A unique computer account will be issued to authorised users for the user's benefit.
- It is important to select and keep a secure password for your account. Do not share your password with anyone. Refer to managing your passwords in Appendix B.

Proper Care and Physical security

- The physical protection of IT property is important. Protect your equipment from improper use, food and drink spillage, electrical power management, anti-static measures, and protection from theft.

Access to Information and records management

Access to information and ICT services is limited to a need to know basis. Users are expressly forbidden unauthorised access to accounts, data or files on office systems or any other ICT resource. This includes:

- using another parties password to get access to ICT systems and information
- access to electronic documents and information which the individual would be otherwise restricted from accessing, or has no need-to-know.

All users of the ICT services have a duty to keep confidential:

- all office data unless the information has been approved for external publication
- information provided in confidence to the office by other entities or agencies
- all personal information about an individual without their prior approval (refer to Government Legislation below).
- Staff should take reasonable steps to ensure that important corporate data is stored appropriately in the office ICT environment in accordance with the Records Management Policy.

The office periodically audits staff access to data, to ensure that information is only reviewed on a need to know basis. Our Electronic Records Management system Objective, also allows you to monitor the audit trails of your own files. Should you become aware of suspected unauthorised access to your files please refer to the Breaches of Security Section below.

Infringement of copyright

Authorised users are expressly forbidden to engage in wilful or negligent infringement of copyright. An example is illegal copying or use of software or media that is in breach of the statutory licence (see Government Policy and Legislation in Appendix A).

Use of software licenses

All applications used by the office computer environment are licensed via an agreement between the office and owner/suppliers. Use of proprietary software (additional to the standard operating environment) is subject to approval from SAO Corporate and reviewed according to compliance, costs, terms of licence agreements, whole of Government purchasing arrangements and business needs.

Software, documentation and all other types of information licensed to the Ombudsman's office must not be sold or otherwise transferred without senior management approval.

The office applies strict adherence to software vendors' license agreements. When office computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Backup your work

To avoid losing data, always backup important work, save your files to the office network at least every 15 minutes. By consistently saving your 'work in progress', you reduce the amount of lost information you would have to redo, if you experienced an unexpected power loss. You should **not** store data on the desktop's hard drive.

Disclosing/publishing Information

Information that can be publicly disclosed on the internet

A major risk for the office is the inappropriate release of, or use of confidential information to the media or other parties, which can seriously damage the reputation of the Ombudsman. In line with this, staff must not publicly disclose internal office information via the internet that may adversely affect the Ombudsman's office relations or public image. All external internet postings (*being posted on behalf of the office*) must be cleared with Public Affairs or Senior Management prior to being placed in a public spot on the internet.

Refer to Guideline 1.11 Use and Disclosure of Personal Information

The office's domain and name management requirements

The office network names and domain are coordinated through the IT team and Senior Assistant Ombudsman (SAO) Corporate. The current domain names approved for office network use are:

- comb.gov.au
- ombudsman.act.gov.au
- ombudsman.gov.au
- pio.gov.au
- postalombudsman.gov.au

These names are the property of the office and used for the business of the Commonwealth Ombudsman. Staff need to be aware whenever using these domain names, they must also clearly indicate that, unless properly authorised, the content expressed is their own, and not necessarily that of the office. All external representations on behalf of the office must first be cleared with appropriate supervisors or senior management. Staff must not use office ICT services for personal postings or messages that are political, inflammatory, hostile or provocative.

Hypertext links

It is preferable to hypertext link material from webpages rather than copy it. The links make the document size more manageable and also ensures that the information being

referred is the most current and the correct version. Refer to our Records Management Policy.

Personal Use of ICT Resources

Use of ICT services for personal use

Personal use of the ICT resources, such as the internet, is permitted provided such use is not excessive, is lawful, does not negatively impact upon the user's work performance, hinder the work of other users, or damage the reputation, image or operations of the Ombudsman's office. Such use must not cause noticeable additional cost to the operations of the office. Staff should not download music or large files unless there is a business need as such downloads may cause additional costs to be incurred by the office. In a situation where personal use is being questioned, whether or not use was reasonable in the particular circumstances will be a matter to be determined by the user's supervisor or Senior Assistant Ombudsman.

ICT resources **must not** be used for private commercial purposes. Users must not publish their Ombudsman's office e-mail address on a private business card.
The office will not be responsible for the loss or damage or consequential loss or damage, arising from personal use of the office ICT resources.

Use of the internet or other office resources in accessing pornography or gambling

The use of the Ombudsman's ICT resources to access pornographic material or to create, store or distribute pornographic or other potentially offensive material of any type or use for gambling will not be tolerated under any circumstances.

Staff found to have breached this policy will be subject to disciplinary action in accordance with the disciplinary procedures contained in Workplace Policies and Procedures. Criminal offences will be reported to the police.

Use of the office 'name and logo'

The Commonwealth Ombudsman's name, crest or logo may only be used with prior approval from the Director of Public Affairs, or Senior Management.

Employees day to day responsibilities

Computer viruses and management of emails

A computer virus is a program that replicates itself. It does this by copying itself onto another program, computer or document. Viruses can be sent in attachments to an email file, be present on a disk or CD or be hidden in websites, such as advertisements or pop-ups.

The office operates virus control/scanning software as part of the external connectivity for the office network. However staff need to be virus aware and take some precautions in normal work practice such as:

- Do NOT open email attachments that you were not expecting – even if you know the sender. The sender's details can be faked.

- Do NOT click on a website address in an email. Copy and paste the URL into your browser. An email can show one address but take you to another.
- If you think you have been infected with a virus inform the Help Desk.
- Do not run, download or forward any unsolicited documents. Anything that runs on your PC should be virus checked and approved first.
- Treat any email with attachments as suspicious, particularly if it has not been received via a secure gateway.
- NEVER open any files with a double file extension, (e.g. iamavirus.txt.vbs). Under normal circumstances you should never need to receive or use these.
- Avoid downloading executables (eg files ending in '.exe, .vbs, .bat, .js, .cmd etc) or documents from the internet. These are often used to spread computer viruses. **DO NOT** open or download unsolicited executables or documents from the internet.
- Although JPG, GIF and MP3 files are not normally infected with viruses, some viruses can be disguised as these file types, also some recent software problems with image viewers and/or MP3 players have allowed them to contain viruses. Some caution is recommended when opening these file types. Jokes, pictures, graphics, screensavers and movie files should be treated with the same amount of suspicion as other file types.
- Any virus warnings or hoaxes should be sent to the Help Desk who can help confirm whether or not they are genuine. Do not forward these warnings to anyone else.
- Ensure that you follow the same procedures at home and elsewhere. Viruses can easily be spread from one location to another.
- It is worth noting that the office has network connectivity to the Fedlink network via a secure internet gateway. If you want to know more then see Appendix C below

Good practice in using the internet — website security

Use external websites with caution, read all privacy policies before giving your email address or other details. Websites requiring you to enter personal information details should have a closed padlock icon showing on your browser window indicating data will be encrypted.

Some internet sites use a secure browser – look for an 's' after the 'http' in the web page address or URL.

Do not trust sites (especially pop-up windows) that suggest you install any type of software – even if they claim the software will improve the security of your computer. The owners of malicious websites often use this as an opportunity to install software on your computer so they can track your personal details.

Breaches of security

Information about security incidents and investigations are invaluable to help us manage security risk. All security incidents should be reported to the ASA and recorded. Examples of security incidents are:

- criminal actions such as theft, break and enter, vandalism or assault

- natural occurrences such as fire or flood, which could compromise agency security
- incorrect handling of classified information
- incorrect storing of information
- accessing official information without authorisation
- sharing official information with a person who is not authorised to access it
- sharing computer passwords
- any unauthorised use of official resources.

The office must report security incidents involving Communications Security (Comsec) and ICT systems to DSD in accordance with the Australian Government Information and Communications Technology Security Manual (ACSI 33).

Senior management must be notified immediately when:

- Sensitive office information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorised parties.
- Unauthorised use of office information systems has taken place, or is suspected of taking place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- There is any unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages.
- Security problems should not be discussed widely but should instead be shared on a need-to-know basis.
- Please also refer to the Fraud Guidelines.

Additional ICT Services

Portable Storage Devices (PSD's)

What is a portable storage device?

A portable storage device ('PSD') is defined as a small, lightweight, portable, easy to use device, which is capable of storing and transferring data. Common PSDs include portable external hard drives, CDs/DVDs, USB keys, laptops/notebooks, personal digital assistants (such as Pocket PC, Palm, BlackBerry), and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones). PSD's have considerable risks for personal and office information security

Such risks arise from the technical capabilities of PSDs (high storage, fast speed of transfer and 'plug and play' functionality) along with their physical characteristics (small size, light weight, low cost, high portability). The office has put in place procedures to enhance security procedures around these devices; these are done under *Privacy Act 1988* obligations.

The following rules should be followed when using PSD's:

- When transporting corporate information all staff must use identified devices supplied by the office and maintain associated security procedures.

- When using PSD devices on home computers virus protection must be maintained to protect unwanted data being transported to the Ombudsman network.
- PSD devices should only be used as a means of transporting data from point to point, not as a permanent storage facility. As such, they should be backed up at every opportunity.
- PSD devices are not transferable to other staff by individuals; these must firstly be returned to the IT team for clearing/re-allocation.
- PSD's not being used must be returned to IT as soon as possible, for clearing and safe storage.
- The IT Section will maintain records of PSD possession.
- All PSD's remain the property of the Commonwealth Ombudsman's office.
- Physical security is to be maintained over these devices at all times.
- Once issued the security of the devices and content is the responsibility of the user.
- Personal PSD's **MUST NOT** to be used for storage of corporate data and **MUST NOT BE** connected to the office workstations or network.
- All issues such as loss or theft must be reported to the IT Help Desk.

Access and ICT security at home

You can request access to the office email system at home by contacting the Help Desk via *Resolve*. Please note that *Resolve* access is not available remotely. Access should not be assumed and each request for home access will be assessed according to need and circumstances of the individual applying for the service.

Broadband internet access can increase computer security risks. If you have broadband or are thinking of installing it, install a personal firewall; operate virus controls and maintain currency of patches to the application. If using wireless connectivity operate secure wireless functionality to ensure other systems are not using your environment. Always use non-administrator accounts for normal use.

Make sure that your desk top is protected from attack or unauthorised use. Do not allow other people in your household access to office services or information.

If you have a portable (PSD) item such as a laptop computer, PDA, USB Pen or mobile phone, it is extremely important to maintain security over the devices. Ensure access to the device is controlled. If devices are being used for VPN connectivity to the Ombudsman's network, ensure the configuration has been installed and tested via the Help Desk. Use secure PSD (supplied by ICT) devices for transport of data.

Ensure devices cannot be easily taken from your car, desk or home office. You may even want to lockdown equipment where necessary.

Management of telephone

Identify the need

Discuss your need for an office mobile phone with your Supervisor. Should your Supervisor agree lodge, a request for a mobile phone with the Help Desk using *Resolve*. The Help Desk will ensure that appropriate approvals for your request are obtained.

Mobile phone purchases

An office mobile phone is only issued where there is a genuine business need for the employee. Once issued the ongoing need for the mobile phone will be reviewed from time to time by Senior Management. Unless a continuing need is identified the phone may be recalled.

The mobile phone must not be used for unlawful activities, or for commercial purposes, or other unauthorised use.

Phone numbers on the office mobile telephones are the property of the Commonwealth Ombudsman's office. They may be transferred to the staff member where this is technically possible at the cost to the staff member. Should you wish this to occur lodge the request with the Help Desk using *Resolve*. Help desk will request approval from the SAO Corporate.

Stolen mobile phones

- Report any theft of a mobile phone directly to the carrier as soon as possible. This is Optus support: 1300 307 937 (Pin #[redacted])
- For Telstra devices please call 1800 032 072 (Account Number:[redacted], password for 3G mobiles = '[redacted] password for others = [redacted])

Advise the carrier:

- the phone number of the stolen phone
- the name of the custodian
- inform them that it's an Ombudsman's office mobile, and
- request must be made for a bar to be placed on the service.

Help desk should be notified as soon as practical.

Additional information on matters such as international roaming can be found by clicking here (when reading this on-line) or on the intranet.

Mobile phone costs (including blackberries)

Phone operational costs will be charged to the business unit for the full charges imposed by the carrier. The office will allow up to $20 worth of private calls (including text messaging) from official mobile phones per month. This is in recognition:

- that staff issued with mobile phones are often working away from their normal work environments and may not have access to a land line phone
- that staff in these circumstances have personal obligations which require them to keep in contact with family and friends
- the cost of recovering minor personal call usage costs exceeds the value of those calls.
- Where monthly calls exceed $20 staff will be asked to reconcile their phone bill identifying personal versus business calls and then to pay to the office for any personal use exceeding $20.
- When staff are travelling internationally telephone calls using a mobile phone are often more costly than a land line. Calls to home to check in is covered by your

travel allowance and using your mobile phone for such calls would be considered personal use.

- Staff using a blackberry should consider that using the internet does incur a cost. Therefore such usage should only be for office purposes.

New or upgrade of ICT services

When staff identify a need for new or updated ICT services a written change request should be submitted to the Help Desk using *Resolve.*

ICT responsibility and access rights

ICT access and monitoring

The office may access and monitor office equipment and services for a range of reasons. This includes hardware owned by the office and software including e-mail, websites, server logs and electronic files. Access may be required for audit purposes, or checking suspected unlawful activities or breaches of office policies. The office may keep a record of any monitoring or investigations.

Prior approval must be obtained from a Deputy Ombudsman, or Senior Assistant Ombudsman, before a user's e-mail, files or data may be accessed. Any information obtained under this approval will be treated as confidential, and will be treated on a need-to-know basis.

There are situations in which ICT staff may intervene in user accounts, temporarily suspend account access or disconnect computers from the network in the course of maintaining the office. Although ICT staff may from time to time become aware of the contents of user directories they are bound to keep this information confidential.

The Ombudsman's external network security processing

The office ICT team operates security between the office network and Internet, the principle components being, network firewall, email gateway hosting and scanning and content filtering.

Email gateway: The office operates a security program called 'Tumbleweed' for checking incoming emails for virus and spam filtering.

Content filtering: ContentKeeper allows the office to control category (e.g. adult content, gambling, malicious etc.), control file type (MP3, Jpeg, etc) and allows the office to monitor internet surfing with reports. Reports include real time, current day and historical reports.

Need help?

If you have any concerns or uncertainty about interpretation of this guide, contact the Help Desk using *Resolve* as indicated below, and they will assist.

CONTAINS DELETIONS UNDER FOI