Appendix A: Government policy and legislation

A number of overarching legislative and policy documents govern the management of information and ICT security which has a significant bearing on the way staff can use electronic and ICT resources. Of importance to the office are:

Copyright Act 1968

Copyright protects intellectual property rights in literary (including computer programs), dramatic, musical and artistic works (includes photographs/charts/maps) and in films/videos, recordings/tapes and TV and radio broadcasts. Use of any part of a copyright work without permission of the copyright owner will infringe copyright unless proved otherwise.

Infringement of copyright will expose a user to personal liability for damages.

Examples of infringement of copyright (if undertaken without the permission of the copyright owner), includes:

1. converting a CD to another audio format, such as MP3, and using it on a PC
2. downloading a film, MP3 recordings, or software from the internet using office IT infrastructure, internet access or computers
3. uploading audio files, video files, software or commercial photographs, to the office websites and making these available to the public
4. advertising links to websites that directly offer copyright infringing material or direct users to copyright infringing material, including audio files such as MP3 recordings, video files, software or commercial photographs
5. sending copyright material, including audio files, such as MP3 recordings, video files, commercial photographs or software, to another person using the office infrastructure such as email
6. storing copyright material, including audio files, such as MP3 recordings, video files, commercial photographs or software, on office computers or servers.

Copyright infringement could apply to any file format.

Trade Marks Act 1995

A user must not copy a trademark or logo belonging to another party. Trademark infringement may expose the user to liability for damages.

Trade Practices Act 1974

The *Trade Practices Act* contains provisions which prohibit passing off and misleading and deceptive conduct. For example, if a user were to copy material from an external site onto the office website (including features such as logos and trademarks) so that persons accessing the website would believe that office had been authorised to carry the material, this would constitute passing off or deceptive or misleading conduct.

Spam Act 2003

This legislation sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages. Under the Act, users must not send unsolicited commercial electronic messages, i.e. messages that are sent without the recipient's consent. Any commercial messages that are sent electronically (including email, instant

messaging or telephone accounts) must include information about the individual or organisation which authorised the sending of the message and provide for a functional unsubscribe facility.

Anti-discrimination legislation

State and Commonwealth legislation prohibits discrimination on the basis of age, impairment/imputed impairment, industrial activity, lawful sexual activity, marital status, physical features, political belief or activity, pregnancy, race, religious belief or activity, sex, parental status or status as a carer. It is also prohibited to victimise a person who has made a complaint of discrimination under these Acts.

Defamation

A user must not publish a statement about another person (or entity) which could harm that other person's (or entity's) reputation. There is no need for the person to have been named specifically if he/she can reasonably be identified. Photographs and cartoons can also be defamatory if they hold someone up to ridicule or contempt. In a defamation case, truth is not always a defence.

Illegal material

Commonwealth and State laws prohibit publication of hard core pornography (in particular where it involves children, bestiality, violence, cruelty and/or exploitation). A breach of these laws would constitute a criminal offence and will also result in disciplinary action under the office's disciplinary procedures. Office rules prohibit any use of office equipment for viewing, storing or distributing sexually explicit, discriminatory, political or potentially offensive material.

Incitement to commit a crime

Users must not publish material which is an incitement to commit or instruction in crime eg, material on how to prepare explosive devices, or how to steal.

The protective security manual

The Protective Security Manual and DSD - ACSI 33 identify that agencies should maintain security and access controls to classified information they hold. These include: encryption of electronic data; identification and authentication for all software; restrictions on personal computer connections to local area networks (LANS), wireless local area networks (WLANS), wireless wide area networks (WWANS) and public networks such as the internet; use of firewalls to control and audit access between networks; measures to detect and eradicate computer viruses; and other intrusion detection mechanisms. Based upon these Government guidelines, these systems are installed as recommended to maintain compliance and are regularly reviewed for compliance purposes.

Appendix B: Management of passwords

Passwords

All hardware, including desktops, laptops and mobile phone are secured by passwords. Passwords are the 'keys' that unlock computers and other equipment. Your login details (**username** and **password**) should be treated like your bank PIN and protected at all costs. You are responsible for this information and should never share your password with anyone.

If someone has your password and logs into your account you will be held responsible for their actions. A third party can cause havoc to the office by deleting files, reading confidential emails, sending offensive or abusive emails, sending spam emails or entering into financial transactions on your behalf and running up large bills.

Change your password often

As passwords can be captured and cracked over time, ICT encourages you to change your Ombudsman password **monthly.** Please note ICT has built a password change prompt into Windows that will prompt you if you have not changed your password in the last three months (90 days). This must be completed to re-establish your logon capability.

ICT recommends that you do not use your Ombudsman password on any other network or internet site.

Please click here more information of password management.

Forgotten your password?

You will need to contact IT support (Help desk) – [redacted] or phone [redacted]

Choose good passwords

Choosing a good password is a very important part of network security. Modern cracking software applications, contain extensive lists of commonly used passwords, including entire dictionaries, lists of names, lists of movie names lists of common pet names etc.

A good password is all of the following:

- compliant to DSD requirements for password complexity
- easy to remember
- hard to guess

A good password does/should NOT:

- contain words that are in ANY dictionary
- contain names of any kind
- contain your user name
- contain dates (in any format)
- be written down, emailed or given to anyone (an administrator should never need your password)
- be the same as any password you have used online

Choosing a password that is all of these things can be difficult. Here are some tricks that may help you.

1. Misspell words in unusual ways
2. Replace names with private nicknames
3. Use a phrase. Obscure song lyrics are a good example
4. Use an acronym of a long phrase
5. Use second, third or last letter acronyms
6. Capitalise and punctuate incorrectly
7. Insert unusual characters in the middle of words (eg ~`|_^)
8. Replace letters with other characters/symbols
9. Make letters out of symbols (eg |-| |_| |V| l3 |_)

You should use several of these tricks together to make a good password. Using these tricks, you should be able to generate 15 to 20 good passwords that are relatively easy for you to remember.

The easiest way to choose a good password is to think of a sentence (perhaps a line from a song or poem). Then, use the first letter of every word in that sentence to make up your password. An example being 'I like working at the Ombudsman's office because it's secure' would be: ilwatoobis. Throw in a random piece of punctuation in your passwords to make them even less likely to be guessed such as '!ilwatoobis' Then throw in a random capitalisation and you have a secure password, eg '!ilwatoobiS'.

Appendix C: Management of emails

Classification of Emails and Documents

Our office system is secure for 'In-Confidence' material. Classification of the office environment has been determined following independent assessment against government policy and guidelines (PSM and ACSI 33) and the office's internal security controls. The policy and procedures are subject to periodic review against the recommended procedures.

Staff should note that:

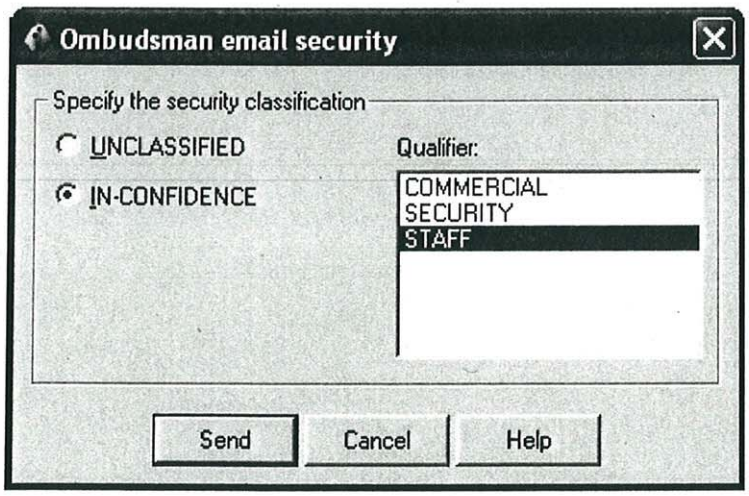
- information above the level of 'IN-CONFIDENCE' should **not be** stored on the office network infrastructure or applications.
- 'IN-CONFIDENCE' classifications can be used when sending secure email to other Australian Government agencies using FedLink (see below).
- connectivity outside the local office environment such as to the Internet is inherently insecure. You should exercise caution when you send personal or confidential information externally.

Connection to FEDLINK

FedLink is a network connection that enables secure communications between Australian Government agencies. It is an encryption mechanism that provides secure and trusted communications across the internet. This allows Commonwealth departments and agencies to transmit and receive information securely up to and including the classification of their own network (on our case 'In-Confidence').

Our ICT team have established network connectivity to the Fedlink network via a Secure Internet Gateway. The environment has been configured in Microsoft Exchange/Outlook to enable sending and receiving of classified emails to the level of 'In-Confidence'. This means that we can only send or receive material classified at the X-IN-CONFIDENCE level or below.

To securely send email to another Australian Government agency at the 'In-Confidence' level you **must select** the 'IN_CONFIDENCE' classification and one Qualifier on your email prior to sending.



Outlook will send anything with this classification to another Australian Government agency by the secure FedLink connection.

Therefore, we are not able to electronically send or receive any material that carries a National Security Classification of:

- Restricted
- Confidential
- Secret
- Top Secret

Or Non National Security Classification

- Protected
- Cabinet-in-Confidence
- Highly Protected

Please refer to the intranet for guidelines for classification of emails.

Staff needing to work with documents or communications at levels above 'In-Confidence' should discuss the security requirements with their supervisor or refer to the Agency Security Advisor.

Note: when staff need to access security classified information, they must have the level of security clearance equivalent to the highest level of classification to which they have access.

It is particularly important to consider these aspects of security when engaging external contractors.