AUDIENCE	CATEGORY
Treasury Staff	Policy

THE **TREASURY** — POLICIES AND PROCEDURES

Information Security Policy (ISP)

This document was endorsed by the Chief Information Security Officer (CISO)

It was last reviewed on 23 August 2012 and is scheduled for review on 23 August 2013

Endorsed

Date: 27/8/2012

For further information or questions, phone IT Security or email ITSA@treasury.gov.au

GUIDANCE ON TREASURY INFORMATION SECURITY POLICY

POLICIES AND GUIDELINES

This policy is based on the Australian Government security policies, principles, minimum standards and common procedures in the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

Staff should read this policy in conjunction with the *Treasury Information Security Staff Responsibilities* available on the Intranet.

REVIEW AND EVALUATION

This policy will be reviewed on an annual basis (12 monthly) and will be revised each time updates or revisions are made to the abovementioned Australian Government policies where appropriate. The policy will also be reviewed whenever there is a significant change to system functionality or architecture occurs.

COMPLIANCE

LEGISLATION/GUIDELINES/INSTRUCTIONS

The following legislation, guidelines and instructions apply to data processed, stored, printed, disseminated, or transmitted via Treasury IT resources. This also includes all forms of electronically stored information including floppy diskette, CDROM, tape and magnetic media including flash media, USB storage devices, handheld PDA devices, smart phones and tablets etc.:

- Crimes Act 1914;
- Privacy Act 1988;
- Financial Management and Accountability Act 1997 (the FMA Act)
- Telecommunications (Interception and Access) Act 1979;
- Freedom of Information Act 1982;
- Archive Act 1983;
- Copyright Act 1968;
- Electronic Transactions Act 1999;
- Commonwealth Anti-Discrimination Legislation;
- Public Service Act 1999 (APS Values and Code of Conduct);
- Protective Security Policy Framework (PSPF);
- Australian Government Information Security Manual (ISM);
- Standards Australia; and

- foreign governments whose information or systems may be affected by any areas of non-compliance.

The report contains a declaration of compliance by the agency head stating any areas of non-compliance, including details on mitigation measures taken to lessen security risks.

AUDITING OF COMPLIANCE BY THE AUSTRALIAN NATIONAL AUDIT OFFICE

All controls in the Australian Government security policies are regularly audited for compliance by the ANAO.

TECHNICAL COMPLIANCE CHECKING

Information systems shall be regularly checked to ensure compliance with security implementation standards.

VERSION CONTROL

Date Modified	Version	Section of document	Author of change	Summary of change
11 March 2009	0.1	Major Revision		Major Revision.
12 August 2009	0.2	Access Control/Inactive Accounts		Modify Section Page 20.
24 September 2009	0.3	Roles & Responsibilities		Responsibilities Move Accreditation & Certification Authority to Separate heading Page 9. Added no official info to be stored on I drive Page 13. Remove network drive from Non-Australian secondee para Page 18.
03 December 2009	0.4	Document Title ISM Sept 2009 edition Changes		Modify document title from ICTSP to ISP in line with changes in the ISM September 2009 edition. Incorporate changes from the ISM September 2009 edition.
18 February 2010	0.5	Minor additions		Minor additions as per I-RAP requested modifications (yearly review of ISP & include dispensation requirements).
30 March 2010	0.6	Patching & Vulnerability Assessments		Added Patching & Vulnerability Assessments – Annual I-RAP requirements.
15 April 2010	0.7	Physical Security		Added printer, MFD photocopy drum sanitisation requirements chapter.
30 November 2010	0.8	Information Technology Security Product Security		Added Product Selection & Acquisition requirements under new Heading Information Technology Security, Product Security. Added Hardware labelling requirements under new Heading Information Technology Security, Product Security, Product Classifying & Labelling.
15 December 2010	0.9	November 2010 ISM revision update		Minor revisions as per the November 2010

INFORMATION TECHNOLOGY SECURITY ADVISOR (ITSA)

The ITSA coordinates information technology security for the agency.

The ITSA is the Information Technology Security Manager (ITSM) that ensures that information security measures are coordinated across the entire agency and is designated as the agency's Information Technology Security Advisor (ITSA). The ITSA reports directly to the CISO on matters of information security within the agency and is the first point of contact for external agencies on any information technology security management issues.

The ITSA coordinates the IT Security Managers (ITSMs) and IT Security Officers (ITSOs) and is responsible for the development of strategic policy and daily administration of Information Technology Security within the Treasury.

The ITSA shall be responsible for:

- identifying and recommending IT security improvements to systems
- the implementation of approved IT Security policies and the management of associated technical arrangements for all systems containing Treasury information;
- the development of IT security procedures and guidelines and Departmental Security Instructions;
- maintaining a close working relationship and liaison with the Agency Security Adviser;
- ensuring the investigation and reporting IT security incidents with the ASA;
- the oversight of privileged user access;
- monitoring information security systems and responding to cyber security incidents;
- the operation of and reporting on departmental IT auditing capabilities;
- participating in the Treasury's IT change control process;
- the provision of advice and reports to the Manager, IT Architecture & IT Security Unit and the Executive Board on IT security related issues; and
- the provision of ongoing IT security awareness training for authorised users.

INFORMATION TECHNOLOGY SECURITY MANAGERS (ITSM)

The Information Technology Security Manager (ITSM) is a role within Treasury's IT Security Team to provide a conduit between the strategic directions provided by the CISO and the technical efforts of ITSOs.

The main area of responsibility of an ITSM is that of the administrative controls relating to information security within the agency.

INFORMATION TECHNOLOGY SECURITY OFFICERS (ITSO)

Information Technology Security Officers (ITSO) ensures that technical information security measures are appropriately considered and addressed within the agency.

All system users must comply with the relevant policies, plans and procedures for the systems they are using.

Any use of a resource may be logged on an audit file together with the specific user identification (user ID) assigned to the user. Such use (actions) are considered to have been undertaken by the user assigned that identification.

All access attempts (successful or unsuccessful) to the Department's network will be logged on an audit file. Authorised Users shall comply with all security policies, rules and procedures as required by the information system owner.

All authorised users have the following responsibilities:

- use systems in accordance with the *Treasury's Personal Responsibilities for Information Security Policy*;
- maintaining the confidentiality and integrity of information;
- ensuring that user identifiers and passwords are treated as private and protected accordingly. Users must ensure that the user ID and password issued to them is not shared with or divulged to any other person;
- being aware of their access privileges and not attempting to defeat security controls to obtain access to data or privileges assigned to other staff;
- ensuring that the information they acquire while using Treasury IT systems is not divulged to any person who does not need to know or is not authorised to know that information;
- are accountable for the data they import or export;
- performing protective marking checks and visual inspection of all data imported and exported;
- maintaining the confidentiality and integrity of software, whether developed or purchased by the Treasury;
- protecting IT equipment from theft, damage, loss and unauthorised access;
- comply with any data security policies, rules and procedures as required by the information owner(s);
- not to misuse IT resources provided; and
- report any misuse, suspected misuse or security breaches to the IT Security Adviser.

Prior to being given access to any Treasury information holding, an authorised user shall be advised of their responsibilities as outlined above and agree to abide by any additional usage provisions as documented in this Information Security Policy.

SYSTEM ADMINISTRATORS

System Administrators are regarded as privileged users and their access privileges usually comprise high levels of access to systems under their control. As such they receive additional training and will be held accountable for all their actions, as per conditions of access form they sign.

SYSTEM ACCREDITATION

ACCREDITATION AND CERTIFICATION AUTHORITIES

The Accreditation and Certification processes are formal procedures for ensuring that IT Networks, classified systems, gateways etc, meet the necessary security guidelines as set down in the *Policies and Guidelines* section. Approval authorities for these processes are:

Position	Roles and Responsibilities
Accreditation Authority	The Secretary has delegated the responsible for Accreditation of IT systems to the Chief Information Security Officer (CISO).
System Owner/ Information Owner	Senior agency manager (Senior Executive Service level) with formal responsibility for the information resource. Responsible for obtaining and maintaining accreditation of IT systems. Ensuring that associated information security documentation is developed and maintained including the System Security Plan. Developing and implementing the Security Risk Management Plan and determining the Risk Treatment Priority.
System Managers/Administrators	Responsible for maintaining the technical and operational effectiveness of the system on behalf of the System Owner.
Certification Authority	IT Security Advisor - Responsible for the Certification of IT systems.

INFORMATION SECURITY MONITORING

VULNERABILITY ANALYSIS

Emerging security vulnerabilities are to be addressed by conducting vulnerability analysis activities and addressing security risks identified as a result of the analysis process.

All new IT systems should undergo a vulnerability assessment before going into production, if a significant change to a system has occurred, or as specified by the IT Security Team or System Owner.

The IT Security team will monitor Government and public domain information for new vulnerabilities in operating systems and application software.

The IT Security team will determine the methodology, process, tool sets and security checklists that will used during vulnerability assessments.

CHANGE CONTROL

The Treasury operates a controlled production environment, supported by a change control processes and procedures.

Any system change must be processed through the change control process. Key steps will include:

REPORTING MISUSE OF IT RESOURCES

It is incumbent upon all staff to report any misuse or suspected misuse of IT resources or information holdings to the IT Security Adviser.

Policy Breaches

All suspected breaches of this policy will be investigated by the Treasury IT Security Adviser and followed up with management as necessary.

If staff are found to have misused the IT resources to which they were granted access, and/or have performed activities prejudicial to the security of those IT resources, their actions will be documented and passed to senior management. Senior management may then take disciplinary action under appropriate legislation.

MALICIOUS SOFTWARE (MALWARE)

Malware (malicious code) is a generic term referring to:

- computer viruses;
- worms;
- Trojan horses; and
- Bots (Robots).

The intent of authors of such software is usually to cause damage to computing systems through various means. Consequently such software represents a significant risk to the safe operation of Treasury's IT systems.

Staff are directed to exercise caution when opening email attachments or downloading files from the Internet especially from an untrustworthy source.

The risks of malicious code infections can be significantly reduced if the following precautions are taken:

- log off and shutdown your PC before leaving the office for the day;
- empty your deleted items folder when exiting Outlook email;
- do not open any suspect files or messages; and
- report any suspect messages to the IT Help Desk.

Malicious Code Control

Anti-virus software must be installed on all Departmental work stations, laptops and servers.

System administrators must ensure that all newly acquired software is subjected to virus detection checks using an approved antivirus product before use. All magnetic media used for data exchange between the Department and other agencies must be scanned for malicious code before use.

Reporting Virus and Malicious Code Incidents

All virus incidents must be reported immediately to the ITSA and the IT Help Desk. In the event of the detection of a virus or other malicious code:

- sending fraudulent email, breaking into another user's mailbox or reading their email without permission;
- sending any fraudulent electronic transmission;
- violating any software license agreement or copyright;
- harassing or threatening other users or interfering with their access to Treasury IT resources;
- taking advantage of another user's naiveté or negligence to gain access to IT resources for which they have not been authorised;
- encroaching on others' use of IT resources through such activities as excessive game playing, sending excessive or frivolous messages or printing excessive copies; and
- disclosing or removing third-party proprietary information.

PHYSICAL SECURITY

PHYSICAL SECURITY OF COMPUTER HARDWARE

All Departmental IT resources and assets must be protected at all times from unauthorised access, theft, illicit use, illegal modification and intentional damage.

All LAN servers, modems and LAN diagnostic equipment must be located in secure, locked areas and access is to be restricted to authorised Departmental IT staff, or maintenance technicians escorted by Departmental IT staff.

These requirements extend to all locations where the Department's IT resources are in use.

DEPARTMENTAL SECURITY INSTRUCTIONS

Additional physical security policy is contained in the Departmental Security Instructions which is located on the Intranet.

SECURE DISPOSAL OR RE-USE OF STORAGE MEDIA AND IT EQUIPMENT

IT Security will dispose of, or declassify IT storage media and IT equipment consistent with the highest classification of data resident on the media. This will be in accordance with the ISM and PSPF.

Hardware that contains Departmental data or software must not be removed from the Department's premises for repair unless the data has been sanitised and declassified, or removed in accordance with guidelines published in the ISM and PSPF.

Items that cannot be sanitised are to be destroyed in accordance with guidelines published in the ISM and PSPF.

SANITISING PRINTER CARTRIDGES MULTI-FUNCTION AND PHOTOCOPY DRUMS

Laser printer cartridges, MFD and photocopy drums must be sanitised prior to being destroyed or recycled.

  - a Common Criteria evaluation against a DSD approved protection profile;
  - a Common Criteria evaluation through the AISEP or a Common Criteria scheme recognised under the Common Criteria Recognition Arrangement;

- second preference - products that are currently in evaluation in the AISEP or DSD;
- third preference - products in evaluation in a scheme where the outcome will be recognised by DSD when the evaluation is completed and published on the EPL or Common Criteria portal; and
- fourth preference - products that are neither in evaluation or have not completed any evaluation.

When choosing a product, the justification for any decision to choose a product that has not completed an evaluation must be documented. This must include a risk assessment identifying the mitigation strategies and the residual risk. The CISO must sign off and accept the residual risk before the product is purchased.

Product Specific Requirements

A Consumer Guide is provided on the EPL which gives specific guidance on the evaluated products use. Where product specific requirements exist in a consumer guide for a product, the agency must comply with the requirements outlined in the consumer guide.

When selecting high assurance products and HGCE the agency must contact DSD and comply with any product specific requirements.

Leasing Arrangements

The agency should consider security and policy requirements when entering into a leasing agreement for products in order to avoid potential cyber security incidents during maintenance, repairs or disposal processes.

MEDIA SECURITY

Classification of Treasury Network

Treasury's electronically stored data covers the full spectrum of classifications from UNCLASSIFIED to TOP SECRET and consists of:

- electronic publications, corporate and administrative documents;
- financial data relating the operations of the Treasury;
- confidential data used as a basis for econometric modelling, forecasting and policy formulation; and
- national budget documents.

The Treasury's primary network is currently certified and accredited to PROTECTED level. Documents which are classified above this level MUST NOT be stored or created on this network or the local drive of PCs connected to this network.

AUSTEO and AGAO material MUST NOT be produced or stored electronically on Treasury information systems.

Removable Media

Removable storage media is not secure and as such CD-ROM, DVD, floppy disks, or portable USB storage devices (USB memory sticks) or music players (iPods) are NOT to be used for storing classified information.

Treasury approved removable media such as CD-ROM, DVD, Floppy Disk or portable encrypted USB storage devices (USB memory sticks) must be stored and transported in accordance with their security classification. Advice on these requirements can be obtained from Treasury's Facilities and Security Unit.

Privately Owned Removable Media

Privately owned removable media including USB devices, I-Pods, PDA devices, mobile phones, smart phones, tablets etc. must not to be used to store or transport Treasury information.

Labelling Removable Media

All removable storage media that contains classified material must be conspicuously marked to indicate the classification of the data stored on them. Covers and storage cases etc. must also clearly show the appropriate classification level on the outside. Removable media includes:

- removable hard disk drives;
- floppy disks;
- tapes;
- jazz/zip drive media; and
- CD-ROM media (CDR, CDR-W, CDR-DVD etc.).

Security classified removable media must be recorded in a Classified Documents Register, in accordance with procedures outlined in Australian Government security policies.

Disposal of Media

Staff members must contact the Treasury Security or IT Security sections before disposing of electronic storage media such as CD-ROM, DVD, floppy disks or portable USB storage devices.

If information on the IT storage media or removable storage device is classified as an official record, it is not to be destroyed. The Records Services Team must be contacted for further advice.

Media is defined as any hardware that contains data. This includes:

- floppy disks;
- hard disks;
- USB memory devices;
- USB devices;
- optical (zip) cartridges; and
- data backup tapes.

Should a staff member receive SPAM email or material that is of an inappropriate nature, they should:

- delete it immediately;
- forward the message to Unsolicited Email; and
- if the sender persists, contact the IT Help Desk.

Treasury staff must not forward chain letters by email as they are regarded as SPAM.

Secure Email Facilities
The Treasury provides a software product to allow Treasury staff to classify their emails. The classification of all emails and associated attachments leaving Treasury is mandatory.

Treasury officers are expected to classify emails correctly and ensure that their recipients can receive appropriately classified emails. Sending classified emails to unsecured recipients can result in a Security Breach being issued. Repeated offences may result in disciplinary action.

Secure Internet email facilities via the FEDLINK network exist between Treasury and various other government agencies. A complete list of participating FEDLINK agencies is published on the Department's Intranet.

The following information must not be sent to agencies not connected to the FEDLINK network, or to public/private email addresses:

- Official Unclassified information including the following Dissemination Limiting Markers:
  - FOR-OFFICIAL-USE-ONLY (FOUO)
  - Sensitive
  - Sensitive: Legal
  - Sensitive: Personal

Employee Representatives
Employee representatives (for example the Social Club Committee) may email staff they represent about representative duties. They must not use Treasury's IT system to transmit material related to elections that are external to the department, to promote or advance participation in industrial action or to promote political purposes.

Email Restrictions
To sustain the email system's performance and protect it from malware infection, Treasury restricts large external email messages. Details are available on the Intranet. In addition work emails which may be inadvertently blocked may be released by contacting the IT Help Desk.

Accessing WEB Based Email Accounts
Staff must not use Treasury facilities to access private Web based email accounts such as Hotmail, Gmail etc. either using POP3 or Internet based email accounts.

Copyright
Staff researching and using information in electronic and printed publications, must be aware of obligations under the Copyright Act 1968. Breaches of copyright laws may attract severe penalties. If in doubt, contact the Manager of Information Services before copying any material from the Internet.

- Federal & State Police;
- Defence Signals Directorate (DSD);
- ASIO; and
- relevant intelligence agencies.

Inappropriate Use of ICT Resources Including the Internet Email and Computing Resources
Instances of apparent inappropriate use will be investigated in accordance with the Treasury Incident Detection and Response Procedures by IT security. If inappropriate use is established, staff may be subject to disciplinary action.

The Treasury IT Security team undertakes continuous monitoring of all Internet and email facilities. The IT Security Adviser, in conjunction with IT System Administrators, investigates increases in Internet activity, as well as all instances of inappropriate activity.

In addition to the regular monitoring, a staff member's Manager may request an Internet usage report if they suspect that a staff member has not complied with this policy. The relevant General Manager and/or Executive Director will be notified of any situation where a breach of the acceptable use policy of any IT resource has occurred.

If a staff member is found to have misused the resources to which they have been granted access, and/or have performed activities prejudicial to the security of those resources, their actions will be documented and passed to senior management.

Sanctions against contract employees will accord with the terms and conditions of their contract, while sanctions against other external users will accord with the relevant legislation.

If that investigation concludes there has been a breach of the Public Service Code of Conduct a sanction may be imposed under section 15 of the Public Service Act 1999.

Sanctions may include:

- a reprimand;
- deduction from a staff member's salary;
- reduction in staff member's salary;
- re-assignment of duties;
- reduction in a staff member's classification; or
- termination of a staff member's employment.

Alleged criminal offences (for example, under the Criminal Code Act 1995, Crimes Act 1914, Archives Act 1983, Financial Management and Accountability Act 1997 and any relevant State or Territory legislation) will be referred to the Australian Federal Police or the relevant State or Territory policy for investigation.

Offensive Information
Staff must not use Treasury's IT facilities to:

- access, view, store, publish, or distribute material that may be considered offensive, indecent, objectionable or pornographic; and

Publishing Procedures

Publishing procedures that apply to paper publications also apply to electronic publications.

Do not use the Internet connection to transmit or publish any material on Treasury's home page or elsewhere, except in accordance with departmental directives or authorised by the Information Owner.

Use of Internet Facilities Supplied by Other Departments

In the case of the Internet being accessed via a service supplied by another Department, for example the DFAT Satin Low system, Treasury staff must adhere to that Department's acceptable use policies. Treasury IT will endeavour to make these policies available to staff who use these facilities.

Systems Development and Maintenance

The development of new systems and the maintenance of existing systems are subject to the change control process.

Security Requirements of Systems

The control objective is to ensure that security is built into all Treasury information systems. Business requirements for new IT systems or enhancements to existing systems must specify the requirements for controls.

Security in Application Systems

The control objective is to prevent loss, modification or misuse of user data in application systems. Controls that must be initiated include:

Location	
Input data validation	Data input to application systems shall be validated to ensure it is correct and appropriate.
Control of internal processing	Validation checks shall be incorporated into systems to detect any corruption of data.
Message authentication	Message authentication shall be used for applications where there is a security requirements to protect the integrity of the message content.
Output data validation	Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Security of System Files

The control objective is to ensure that IT projects and support activities are conducted in a secure manner. Controls include:

Controls	
Control of operational software	Procedure shall be developed to control the implementation of software on operational systems.
Protection of system test data	Test data shall be protected and controlled.
Access control to program	Control shall be maintained over access to program source

The following controls should be put in place to detect attacks include:

- deploying an IDS;
- monitoring logging alerts; and
- using other mechanisms as appropriate for the detection of exploits using the known vulnerability.

ACCESS CONTROL

Access Control Responsibility

As part of the department's IT risk mitigation strategy, access to IT systems is controlled and is granted on the basis of a demonstrated business requirement and a defined "need to know" basis.

The department reserves the right to limit, restrict or extend access privileges to its information holdings and IT resources as required.

A mandatory minimum requirement of a baseline security clearance at base level is required to gain access to internal Treasury IT resources.

All requests for access to Treasury IT systems are submitted electronically to the IT Help Desk via the Staff Administration Management System (SAMS).

IT Help Desk

The IT Help Desk is responsible for the day-to-day administration of the Treasury IT system access control function. Services provided by the IT Help Desk includes, but is not limited to:

- administration of access control mechanisms including registration of new users, termination of old logon ids, password resetting;
- provisioning of privileged user access;
- modifying of system access rights; and
- maintaining the department's access control documentation.

System Owners/ Information Owners

Systems Owners/ Information Owners are responsible for maintaining the level of awareness of their staff relating to access control and ensuring that staff comply with promulgated Access Policy requirements.

Staff with direct line management responsibilities, are responsible for the timely processing of staff movements within their area to ensure that access rights and privileges are set or amended appropriately.

Systems Owners/ Information Owners are be responsible for:

- ensuring that the management of their information holdings are appropriately protected using security controls;
- determining the classification of their information holdings and determining the appropriate level of security controls required;

- all applications development and maintenance work is to be performed in the development and test environments;

- users must logoff or activate a password-protected screen saver when they leave a PC for any period of time;

- users must logoff the network at the close of business each day; and

- IT audits are periodically conducted to determine the level of user compliance.

IT Services Matrix

A table of IT services per group is at Annex A.

Privileged Users Matrix

The privileged user matrix is maintained by IT security in a Excel spread sheet, and via reports extracted from the SNARE security log audit system.

Passwords and User Identifiers

Each system user must be granted a unique user identifier and password. The initial password supplied to a user must be set to enforce the user to apply a personal password.

Passwords must not be disclosed or shared with another person as they protect the user identifier against misuse.

Unique user identifier and passwords ensure that the Treasury is:

- granting access to information only to people who have a work related need;

- informing users they are accountable for their access which is audited through the use of their assigned user identifier;

- ensuring logical password access controls and procedures are in place;

- ensuring information users observe all approved practices and procedures set down on password use; and

- minimising access to privileged functions.

Identification Principle

The naming convention to be used for Treasury network User IDs is:

- fms where 'f' is the user's first initial, 'm' is the user's middle initial and 's' is the last initial of the user's surname, giving a maximum of 3 characters. Variations of this can be used as needed, at the discretion of the System Administrator.

- wes_fms where 'wes' stands for Work Experience Student. 'fms' is the initials of the student as described above. These userids won't be added to Central Database as it requires a 3 character userID format.

- nas_fms where 'nas' stands for Non-Australian Secondees. 'fms' is the initials of the person as described above. These userids won't be added to Central Database as it requires a 3 character userID format.

Password Controls

All IT systems must adhere to the following minimum password standards:

Access permissions set on generic or anonymous accounts is to be strictly limited to the information and systems required for the purpose for which the account was created.

All usage of anonymous or generic accounts is to be monitored.

Anonymous and Generic Accounts

The use of anonymous or generic IDs shall only be permitted as an exception and where they are suitable for the work to be performed.

Approval for the creation of anonymous or generic IDs may only be given by the Treasury ITSA.

Access permissions set on generic or anonymous accounts is to be strictly limited to the information and systems required for the purpose for which the account was created.

All usage of anonymous or generic accounts is to be monitored.

Non-Australian Secondee accounts

Non-Australian secondees are commonly people from Pacific Region countries who are here on behalf of their governments to learn more about economic policy. People from other countries also work in Treasury for short periods.

Non-Australian secondees will:

- be set up with userIDs in the format of nas_fms, where nas stands for Non-Australian Secondee and fms represents initials of the user;
- when given user accounts on Treasury's Protected network they will be given access to an I: drive, e-mail and Internet browsing only; and
- when given user accounts on Treasury's unclassified network they will be given access to Internet browsing and web based e-mail;

The Domain Users group will only be assigned to these userIDs. These users won't be added to Central Database and no access to Intranet applications are to be assigned.

Time restrictions on the account are set to 07:00 – 19:00.

External Presenters and Trainers Generic Accounts

External presenters and trainers engaged on an ad-hoc basis by Treasury will be given limited access to the Treasury network via a generic userID. These external people will be escorted while in the building by Treasury staff.

The use of the generic userID by these presenters / trainers will decrease the risk of these people accessing information they are not authorised to view.
The access on these accounts will be set up as follows:

- external presenters and trainers will be given the password for the generic userIDs Presenter1, Presenter2, Presenter3 etc;
- userIDs will be disabled by default;
- userIDs will not be given access to any network drives or Treasury Intranet Applications;
- userIDs will be given access to Office Applications and Internet Explorer; and

Staff going on extended leave, maternity leave, secondment etc. where the period will extend beyond 3 months will have their accounts locked until the return to the agency. The exceptions to this policy are:

- Staff going on maternity leave may via Human Resources (HR) request remote access to the Treasury Intranet to check on Staff Notices and employment opportunities;
- Seconded staff who are required to regularly return to the agency for briefings etc. can request limited user account access and remote access to the Treasury Intranet.

Screen and Session Locking
All IT systems are to be configured with a screen and/or session lock that activates:

- after a maximum of 15 minutes of system user inactivity; or
- if manually activated by the system user.

The locking mechanism is to be configured to:

- completely conceal all information on the screen;
- ensure the screen does not appear to be turned off while in the locked state;
- ensure the system user re-authenticates to unlock the system; and
- deny system users the ability to disable the locking mechanism.

Resetting of Locked or Forgotten Passwords
Passwords must only be reset or unlocked in accordance with the Department's Password Procedures.

Responsible Access to Treasury Information
Information owners will grant access to their information holdings as appropriate to their staff member's role. Consideration should be given to the need to know information principle, data sensitivity and possible risk of damage to or loss of the resource.

Treasury reserves the right to limit, restrict or extend access to information holdings.

Use of the Treasury Network
The Treasury IT resources may only be utilised for Treasury-related purposes.

System users may use Treasury IT resources (including email and Internet) for incidental personal use, provided such use does not:

- interfere with Treasury businesses activities;
- involve any form of solicitation or commercial activity outside of Treasury business;
- potentially embarrass The Treasury, Treasury Ministers or the Government.

An authorised user is NOT permitted to:

- transmit, store and/or distribute material that is libellous, defamatory, obscene, offensive, harassing, racist, obscene, or pornographic in nature;
- dispose of personal information without permission;

Non-repudiation	Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action.
Key Management	A key management system based on DSD standards, procedures and methods shall be used to support the use of cryptographic techniques.

Using Cryptographic Products

Only DSD approved cryptographic algorithms and protocols are to be used. If a product is to be used for the protection of classified information then it must have completed a DSD crypto evaluation (DCE), or other cryptographic evaluation recognised by DSD.

NETWORK SECURITY

All changes to network configuration should be documented and approved through a formal change control process.

For each network the agency must have:

- a high-level diagram showing all connections into the network; and
- a logical network diagram showing all network devices.

Network diagrams should:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

GATEWAY SECURITY

All gateways connecting to Treasury ICT facilities must meet the following standards:

- are the only communications paths into and out of internal networks;
- by default, deny all connections into and out of the network;
- allow only explicitly authorised connections;
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network);
- provide sufficient logging and audit capabilities to detect cyber security incidents and attempted intrusions; and
- provide real-time alerts.

Configuration Control

Changes that could introduce vulnerabilities, new security risks or increase security risks in Treasury's gateways need to be documented and have IT Security approval before being implemented.

BlackBerry Devices

Staff using BlackBerry devices for Treasury business use are responsible for the protection of the BlackBerry device and the data contained on them at all times. It is the responsibility of the user to adhere to the guidelines of the BlackBerry Acceptable Use Policy which is signed by each staff member assigned a BlackBerry device.

Only the email and calendar facility on the Blackberry can handle classified information. The telephone facility on the Blackberry cannot be used to make sensitive or classified phone calls or SMS messages.

Loss or Theft of Laptops Portable Devices or Media

If a Treasury staff member:

- loses a Treasury owned laptop, Blackberry or other portable device;
- loses any removable media (CD/DVD, USB device etc) containing official information; or
- their Treasury laptop, Blackberry, portable device or media is stolen, then

they must contact the IT Help Desk immediately. The IT Help Desk will notify the ASA and ITSA immediately and also advise the staff member that they must also report the loss/theft to the nearest police station and obtain a report number.

The Help Desk will keep a record of the loss or theft and coordinate the replacement asset and reporting requirements.

Unauthorised Hardware and Software

Privately Owned IT Equipment and Software

Staff are not permitted to connect privately owned IT equipment to the Treasury network or IT systems. This includes:

- laptops;
- iPods;
- MP3 Players;
- PDA devices;
- portable tablet devices (iPads etc);
- smart phones;
- mobile phones; and
- portable USB storage devices (cameras, hard drives & USB memory sticks).

Staff are also NOT permitted to install privately owned software onto Treasury computers or IT systems.

All non-Treasury magnetic and optical media must be virus scanned using the approved Treasury virus scan product before being used in Treasury IT systems.

APPENDIX A - IT SERVICES MATRIX

The following table represents the services which are enabled for each specific group. All services which are not explicitly enabled for a group are disabled.

Group Name	Service	Location	Restrictions
Internal Staff	HTTP	Intranet web servers Internet web servers	Nil
	HTTPS	Intranet web servers Internet web servers	Nil
	SMTP	Internal Email servers External mail gateway Treasury DMZ	E-mail is restricted in accordance with the guidelines stated in the departments E-mail Gateway configuration document.
	MAPI	Internal E-mail servers	Used to send e-mail from desktops to server.
	Reuters	Accessible via AOFM connection to Reuters.	Reuters is connected to an AOFM firewall, which is used to separate 3rd party services. Proprietary software and username and password are required to access services.
	Microsoft File and Print sharing	Internal Treasury Network	Access is restricted by Active Directory group membership controls.
	Remote Access VPN	DMZ	Access is restricted by Active Directory group membership controls.
	SAP	Treasury DMZ	Access is restricted by Active Directory group membership controls.
	CBMS	DOFA	Access is given by DOFA and is restricted by role based assignment. Individual machines are given access via the firewall by Mac address or IP address to this application. Machines must be configured with the CBMS software to access the program.
AOFM	HTTP	Intranet web servers Internet web servers	Nil
	HTTPS	Intranet web servers Internet web servers	Nil