



Australian Government

Department of Education, Employment and Workplace Relations

Technology Solutions Group

Technology Branch

Information Security Operations & Forensics

DEEWR EXTERNAL SECURITY POLICY – FOR CONTRACTED SERVICE PROVIDERS AND USERS

November 2011



DOCUMENT PARTICULARS

Document name	DEEWR external security policy for Contracted Service Providers and users		
Classification	UNCLASSIFIED		
Document ID		TRIM File #	AD11/009490
Last updated	10 November 2011	Document status	Final
Due for review	9 October 2012		
Point of contact	GB2541		
Approval authority	Director IT Security Operations & Forensics	Date of approval	10 November 2011
	Group Manager, Finance and Business Services / Chief Information Security Officer (CISO)		10 November 2011

NOTE: This is a controlled document in its electronic form only. Paper copies of this document are not controlled and should be checked against the electronic version prior to use.

© 2011 Commonwealth of Australia.

This work is copyright. Apart from any use permitted under the Australian Copyright Act, 1968, no part may be reproduced by any process without the permission of the Department of Education, Employment and Workplace Relations.

Document History

VERSION	DATE	AUTHOR	SUMMARY OF CHANGES	STATUS	AUTHORISED BY
1.0	29/08/2011	GB2541	Initial Draft.	Draft	GB2541
1.1	29/08/2011	MS0451	Minor editorial changes	Draft	GB2541
1.2	21/10/2011	MS0451	Minor editorial changes	Draft	GB2541
1.3	3/11/2011	GB2541	Stakeholder feedback	Draft	GB2541
1.4	10/11/2011	GB2541	Stakeholder feedback	Final	GB2541
1.4	10/11/2011	CS0052	Approval	Final	CS0052

CONTENTS

PART 1	Introduction	4
1.1	Applicability	4
1.2	Structure and Design of this Policy	4
1.3	Policy Aims	5
1.4	Terms used within this policy	5
1.5	Hyperlinks	5
PART 2	Background Information	6
2.1	Background	6
2.2	Relevant Commonwealth legislation	6
2.3	Compliance with Commonwealth government policies	7
2.4	Classification of data	7
2.5	Reputational risk	8
PART 3	All Users	9
3.1	Authorisation	9
3.2	User responsibilities	9
3.3	Self-registration	9
3.4	Data protection and privacy of personal information	10
3.5	Unauthorised communication and use of information	10
3.6	Prevention of misuse of information processing facilities	10
3.7	Breaches	11
3.8	Investigations	12
PART 4	Contracted Service Providers accessing DEEWR ICT systems	13
4.1	Physical access	13
4.2	Cyber Security Incidents	14
4.3	Malicious code	14
4.4	Roles and Responsibilities	15
4.5	DEEWR System roles	16
4.6	Security Contacts	16
4.7	User self-management	17
4.8	DEEWR override	17
4.9	Authentication	18
4.10	Suspension and deactivation of absent or exiting Users	19
4.11	Termination of a Contracted Service Provider's access	19
PART 5	Contracted Service Providers storing, retaining or presenting DEEWR data	20
5.1	Protective Security Policy Framework (PSPF) mandatory requirement – GOV 12	20
5.2	ISM requirements	20
5.3	IT Security governance framework	21
5.4	IT Security Documentation	21
5.5	System security	23
5.6	System accreditation	23
5.7	Minimum security standards	23
5.8	Data segregation	23
5.9	Data destruction and media sanitisation	24
APPENDIX 1	Glossary	25

PART 1 Introduction

This document forms the Department of Education, Employment and Workplace Relations (DEEWR) IT security policy for Contracted Service Providers and external users of DEEWR Systems.

This policy applies to all users and applies to all Principal Agreements.

All Contracted Service Providers are governed by this policy to the extent that there is no inconsistency with the terms of a Principal Agreement.

1.1 Applicability

This policy provides instruction and treatment of DEEWR assets¹ that have no national *security classification*.

This policy applies to all:

- » Contracted Service Providers providing services to the department
- » Contracted Service Providers storing DEEWR data² within their Information and Communications Technology (ICT) systems and premises (System Owners)
- » Contracted Service Providers accessing DEEWR systems
- » Users including staff and employees of Contracted Service Providers.

This policy does not apply to:

- » Australian Government agencies that are subject to the Financial Management and Accountability Act 1997 (the FMA Act)
- » Systems storing or accessing classified data.

1.2 Structure and Design of this Policy

This policy is made up of five parts.

Part 1 This part. (Introduction)

Part 2 provides background information providing the regulatory requirements and information that form the basis of this policy.

Part 3 applies to all users of DEEWR external facing ICT systems including user self registration systems. Examples include PRISMS, GEERS, ICS, TRA, and similar systems.

Part 4 applies to all Contracted Service Providers accessing DEEWR ICT systems. Examples include Jobs Services Australia providers (JSAs).

¹ Assets include data in any format including archived information, personal data, financial and accounting information. Data storage devices including removable media, tapes and disks

² Data refers to both logical (electronic) and physical (paper / documents) elements.

Part 5 applies to all Contracted Service Providers representing or acting on the behalf of DEEWR, storing, retaining or presenting DEEWR data. Examples include Job Service Australia providers (JSAs), “cloud” providers, web hosting vendors, and similar.

1.3 Policy Aims

It is a requirement that all Users who make use of DEEWR Systems and assets³:

- » Comply with all applicable Australian laws and legislation;
- » Do so only for the purpose of complying with the requirements of DEEWR programmes;
- » Ensure their actions do not result in falsification, inappropriate modification, disclosure or destruction of information;
- » Notify DEEWR if they become aware of any inappropriate access or use of DEEWR systems or data;
- » Are identified, authorised individuals who leave an auditable record of their activities;
- » Protect the confidentiality of information and DEEWR Systems; and
- » Ensure that DEEWR Systems remain operational.

DEEWR aims to ensure that DEEWR Systems remain operational and available to all authorised external Users.

1.4 Terms used within this policy

MUST / MUST NOT indicates a mandatory requirement. Compliance that is, in some cases, beyond the control of DEEWR. Non-compliance with **MUST** controls **MUST** be reported to DEEWR via the DEEWR contract manager.

SHOULD / SHOULD NOT indicates a requirement. Approval for non-compliance **MUST** be explicitly granted by DEEWR.

ARE REQUIRED represents industry best practice. DEEWR encourages all Contracted Service Providers to comply.

Systems are ICT infrastructure storing DEEWR data.

The terms “Contracted Service Providers”, “Service Provider” and “External User Organisations” are used interchangeably throughout this document.

1.5 Hyperlinks

This policy uses hyperlinks extensively throughout the policy to provide access to other supporting or reference documentation. The hyperlinks were current November 2011.

³ Assets include data in any format including archived information, personal data, financial and accounting information. Data storage devices including removable media, tapes and disks

PART 2 Background Information

2.1 Background

Whilst from a Commonwealth policy perspective DEEWR is responsible for the management of security risks, Contracted Service Providers may be held responsible criminally or civilly for the mismanagement of security risks. Contracted Service Providers are required to make themselves aware of the Commonwealth legislation and policies listed below.

From the *Australian Government Protective security governance guidelines - Security of outsourced services and function*:

When an agency adopts an outsourcing approach to service provision, accountability for the performance of the service or function and responsibility for outcomes remains with the agency. This agency responsibility includes the management of security risks where external service providers are being used.

2.2 Relevant Commonwealth legislation

Australian Legislation relevant to the use of DEEWR Systems or DEEWR provided data include and is not limited to:

- » *Financial Management and Accountability Act 1997*
- » *Evidence Act 1995*
- » *Crimes Act 1914* (particularly sections 70 and 76)
- » *Criminal Code Act 1995*
- » *Cybercrime Act 2001*
- » *Public Service Regulations 1999*
- » *Student Assistance Act 1973*
- » *Freedom of Information Act 1982*
- » *Archives Act 1983*
- » *Privacy Act 1988*
- » *Data-matching Program (Assistance and Tax) Act 1990*
- » *The Education Services for Overseas Students (ESOS) Act 2000*

2.3 Compliance with Commonwealth government policies

Contracted Service Providers **must** ensure their IT systems comply, where applicable, with relevant Australian Government instructions.

Instructions as at November 2011 include:

2.3.1 Attorney General's Department

- » Protective Security Policy Framework (PSPF)
- » PSPF - Australian Government information security management protocol
- » PSPF - Protective security governance guidelines Business impact levels
- » PSPF - Information security management guidelines - Agency cyber security responsibilities when transacting online with the public
- » Commonwealth Fraud Control Guidelines

2.3.2 Defence Signals Directorate (DSD)

- » Information Security Manual (ISM)

2.3.3 Australian Government Information Management Office (AGIMO)

- » AGIMO Web Accessibility Guidelines
- » National e-Authentication Framework (NeAF)

2.3.4 Office of the Australian Information Commissioner (OAIC)

- » National Privacy Principles (NPPs)

2.4 Classification of data

In September 2011 DSD reclassified electronic data in accordance with Information security management guidelines - Australian Government security classification system

DEEWR systems contain data rated at:

- » **FOU (For Official Use Only):** Unclassified information whose compromise may cause limited damage to national security, Australian Government Agencies, commercial entities or members of the public.
- » **G:** Government information not intended for public release, including dissemination limiting marker (DLM) information and systems.
- » **P:** PROTECTED information and systems.

2.5 Reputational risk

Contracted Service Providers **must** take all reasonable steps to protect the reputation of the Department.

Contracted Service Providers are responsible for maintaining the *confidentiality, availability* and *integrity* of websites and other data sources under their control that are directly or indirectly attributable to DEEWR. This includes a requirement to protect the brand name and reputation of the department.

Reasonable steps include ensuring:

- » The secure physical and logical storage of data to prevent the loss, destruction, modification and authorised disclosure.
- » Websites that directly or indirectly represent the department have been successfully tested in accordance with the documentation provided in the Open Web Application Security Project (OWASP) guide to building secure web applications and web services. See: http://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents

PART 3 All Users

3.1 Authorisation

Contracted Service Providers **must** ensure that their use of DEEWR systems is exclusively to support the operation of the Government programmes covered by their contracts with the Department.

3.2 User responsibilities

Each User of DEEWR Systems will be authorised to perform specific tasks on DEEWR Systems.

Users of DEEWR systems **must**:

- » **not** enter any information into DEEWR Systems which they know to be false
- » **not** falsify DEEWR data or information
- » **not** modify, disclose or destroy DEEWR data or information without permission
- » be accountable for all actions performed using their User ID
- » protect passwords from disclosure or compromise at all times
- » **not** share or distribute their unique identification or password
- » change their password at least every ninety days (a history of passwords will be maintained to prevent the re-use of the previous twenty passwords)
- » **not** attempt to bypass the procedures or access controls to perform unauthorised tasks
- » notify their Security Contact to temporarily disable their User ID if they are:
 - › planning to take leave for thirty days or more, or
 - › expecting to cease using DEEWR systems for a period of thirty days or more

Any person who identifies unauthorised activity **must** report this to the IT contact so that the matter may be referred for investigation or for consideration of appropriate disciplinary and/or legal action.

3.3 Self-registration

DEEWR provides the ability for users to self-register and create a user identity (user ID) and authentication.

Each user ID is specific to one person and cannot be changed, reassigned or modified. Any user who applies by the DEEWR self registration processes is responsible for the security and maintenance of their authentication credentials. This includes, but is not limited to: username; user ID; email address; and secret questions and answers. If a user forgets or loses their authentication credentials, a new user account **must** be created. Passwords, user IDs and e-mail addresses cannot be changed or modified by DEEWR.

See user *self management* below.

3.4 Data protection and privacy of personal information

Contracted Service Providers **must** comply with the provisions of their contracts with regard to:

- » the privacy and integrity of information, and
- » the prevention of fraud.

Users **must not** enter any information into DEEWR Systems which they know to be false. Users **must** exercise care to ensure that information is true and correct.

Contracted Service Providers **must** use information only for the purposes of meeting their obligations under their contracts. No information in DEEWR systems may be provided to third parties outside the terms of the contract.

3.5 Unauthorised communication and use of information

The unauthorised communication, use and/or modification of DEEWR information may be a criminal offence under the *Crimes Act 1914* and/or the *Criminal Code Act 1995*.

3.6 Prevention of misuse of information processing facilities

3.6.1 Use for unauthorised purposes is improper use

All use of the Department's IT assets **must** be for authorised purposes. Use of facilities for any unauthorised purpose or with unauthorised tools or processes is improper use of the facilities and a breach of this Policy.

Employees, contractors, and third party users should be advised that no access will be permitted except that which is authorised.

3.6.2 Advice to users on monitoring of system use

All users of DEEWR systems **must** be advised of the Department's policy on monitoring system use:

- » Any data or material created, captured, transmitted or stored using DEEWR IT resources may be viewed by authorised personnel as part of normal monitoring processes.
- » Users will not necessarily be notified that an item has been inspected.
- » Where inappropriate use is detected it is followed up and reported to the appropriate authorities including the Australian Federal Police.
- » The Department may disclose the contents of log files or data stored on IT facilities to appropriate third parties.
- » The Department may use any material gathered as evidence when misconduct or criminal action is being considered or undertaken.

3.7 Breaches

A breach of this Policy occurs when any person performs an act prohibited by the Policy. Examples include:

- » the sharing of user IDs and passwords
- » failure to notify the department of an inappropriate access or use of the system or data;
- » users using the system for a purpose not authorised by the Department;
- » failure to notify DEEWR when a User should be suspended
- » users attempting to inappropriately obtain increased access
- » users making any false or fraudulent declaration
- » users disclosing information obtained from DEEWR Systems to someone not authorised to receive it
- » Security Contacts failing to store User Security Declarations so they can be made available to DEEWR on request
- » the breach of DEEWR-provided 3rd party EULAs⁴ (examples include using DEEWR provided software, SSL certificates, or the like beyond the permissions set within the EULA).

3.7.1 Detection and reporting of breaches

DEEWR monitors all use of DEEWR Systems and through this or other means may detect a breach, potential breach or planned breach of security.

Contracted Service Providers, Security Contacts and individual Users **must** report all breaches they become aware of to DEEWR IT Security.

If a person suspects that a breach may have occurred, they **must** report this to DEEWR IT Security.

If a person believes that another person may be planning to breach security, they **must** report this to DEEWR IT Security.

DEEWR may impose immediate security restrictions on individuals or Contracted Service Providers to minimise its perceived security risk.

DEEWR may impose sanctions or restrictions on individuals or Contracted Service Providers who fail to report breaches to DEEWR

DEEWR may revoke a User's authorisation to use DEEWR Systems without notice upon receiving a report of a breach of security, or pending investigation of a matter, or for any other reasonable cause.

When reporting a breach or suspected breach to DEEWR IT Security, a Security Contact may propose a course of action aimed at ensuring that the breach is terminated quickly and does not occur again. The proposed action might include temporary suspension of a User's access, counselling or

⁴ End User Licence Agreement

disciplining a User. At its discretion, DEEWR IT Security may agree to this proposal and not impose any additional restrictions. In these circumstances, DEEWR IT Security may require the Security Contact to report the resolution of the breach.

3.8 Investigations

DEEWR may investigate any activity on receiving a report, or on reasonable suspicion that a breach has occurred or may occur.

Contracted Service Providers **must** co-operate fully with any such investigation, supply and provide records, access to employees and premises as required by their contracts.

DEEWR may have an obligation to report certain breaches to the Australian Federal Police, the Defence Signals Directorate or other authority.

PART 4 Contracted Service Providers accessing DEEWR ICT systems

4.1 Physical access

4.1.1 Protective Security Policy Framework (PSPF) mandatory requirement – PHYSEC 6

***PHYSEC 6:** Agencies must implement a level of physical security measures that minimises or removes the risk of ICT equipment and information being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.*

Contracted Service Providers are to ensure that they:

- » put in place appropriate building and entry control measures for areas used in the processing and storage of information
- » put in place physical security protection (which matches the assessed security risk of the aggregated information holdings) for all agency premises, storage facilities and cabling infrastructure
- » locate ICT equipment, where practical, in areas with access control measures in place to restrict use to authorised personnel only, and put in place other control methods where physical control measures are not possible
- » implement policies and processes to monitor and protect the use and/or maintenance of information, equipment, storage devices and media away from agency premises, and in situations where a risk assessment determines, put in place additional control measures
- » implement policies and processes for the secure disposal and/or reuse of ICT equipment, storage devices and media (including delegation, approval, supervision, removal methods and training of employees) which match the assessed security risk of the information holdings stored on the asset.

Service providers **must** operate a clear screen and clear desk policy.

Users **must** logoff from DEEWR Systems when they leave their workstation. Users **must** ensure that others are not able to view the data on their screen.

Users **must** ensure that printouts of DEEWR Systems information are accessible only to those authorised to access that information. Paper and electronic media records **must** be disposed of securely.

Contracted Service Providers **must** ensure that DEEWR Systems information cannot be accessed by facility maintenance workers, cleaners or other people not authorised to access the information.

4.2 Cyber Security Incidents

Cyber security incidents include and are not limited to:

- » unwanted disruption or denial of service (e.g. DDoS attack)
- » website defacement
- » malicious code outbreak (e.g. virus or malware)
- » data spillage, data loss
- » loss or compromise of cryptographic keying material (i.e. SSL certificate)
- » attempts to gain unauthorised access to a computer system or its data
- » unauthorised use of a system for processing or storing data
- » changes to system hardware, firmware or software without the knowledge or consent of the System Owner.

4.2.1 Cyber Security Incident reporting

It is highly recommended that all cyber security incidents not involving DEEWR data be reported to CERT Australia. CERT Australia can help mitigate ICT threats.

Contracted Service Providers **must** report any breaches or cyber security incidents involving DEEWR provided data or assets containing DEEWR data to DEEWR IT Security as soon as possible by contacting: itsa@deewr.gov.au

The report must provide:

- » the date the cyber security incident was discovered
- » the date the cyber security incident occurred
- » a description of the cyber security incident, including the personnel and locations involved
- » the action taken
- » to whom the cyber security incident was reported
- » the file reference (if any).

4.3 Malicious code

It is recommended that, when malicious code is detected, Contracted Service Providers:

- » isolate the infected system
- » scan all previously connected systems, and any media used in a set period leading up to the cyber security incident, for malicious code
- » isolate all infected systems and media to prevent reinfecting the system
- » change all passwords and key material stored or potentially accessed from compromised systems

- » advise system users of any relevant aspects of the compromise, including changing all passphrases/passwords on the compromised systems and any other system that uses the same passphrase or password
- » use current antivirus software to remove the infection from the systems or media
- » report the cyber security incident and perform any other activities specified in the Incident Response Plan (IRP).

4.4 Roles and Responsibilities

4.4.1 Identity Management

4.4.1.1 Contracted Service Providers are responsible for their Identity Management.

Identity Management includes but is not limited to:

- » the creation of new user IDs
- » the management of User roles
- » the management of User details
- » the deactivation of user IDs which are no longer required
- » making this Policy available to all Users and promoting compliance with it.

DEEWR will provide an Online Identity Management System for specific Contracted Service Providers. Those Contracted Service Providers, commonly known as the External User Organisation, **must** use the Online Identity Management System to complete the requirements stated in this Policy.

In circumstances where the Security Contact cannot perform his or her role or has left the External User Organisation, DEEWR may contact the Contracted Service Provider or External User Organisation and agree to appoint another person.

4.4.2 User IDs

Each user ID is specific to one person and cannot be changed, reassigned or modified. Any user who applies by the DEEWR Self registration processes is responsible for the security and maintenance of their authentication credentials. This includes and is not limited to username, user ID, e-mail address, secret questions. See user *self management* below

External User Organisations **must** issue a user ID only to people who have signed an undertaking to comply with this security Policy on a User Security Declaration form supplied by DEEWR or through an online system provided by DEEWR to obtain this undertaking.

Contracted Service Providers and External User Organisations **must**:

- » Assign a DEEWR-generated user ID to all Users in accordance with the requirements of this Policy

- » Ensure that for each instance that a User accesses DEEWR Systems that the User uses their assigned user ID.
- » Ensure that Users do not use another user's user ID.

4.5 DEEWR System roles

DEEWR will define a number of roles to which Users may be allocated within DEEWR Systems. These roles will determine the actions a User may undertake and the applications a User may access.

Security Contacts may assign any of their Users to any of the available roles.

Contracted Service Providers **must** apply the “need to know” and “least possible privilege” principles in assigning Users to roles. For example, External User Organisations should authorise the smallest possible number of people to make claims and appoint the smallest possible number of Security Contacts.

4.6 Security Contacts

Organisation Security Contacts (OSCs) and Site Security Contacts (SSCs) are both forms of Security Contacts.

The External User Organisation is to appoint and maintain at least two individuals to be OSCs.

If the person appointing individuals to be the OSC does not have a DEEWR Systems user ID, then they **must** use the Initial Access Request Form to appoint the initial OSCs.

DEEWR may require the person appointing the OSC to provide information sufficient to satisfy DEEWR's that they have the authority to make this appointment.

After an OSC has been issued with a User ID the OSC should then proceed to create one or more SSCs to perform the External User Organisation's Identity Management responsibilities.

4.6.1 Security Contact tasks

All Security Contacts may perform Identity Management tasks including:

- » creating user IDs for individuals
- » allocating DEEWR System Roles to Users
- » changing a User's home site
- » enabling or disabling a User's DEEWR systems access
- » terminating a User's right to access DEEWR Systems on behalf of the External User Organisation (Deactivate User transaction)
- » changing the account details of a User
- » resetting passwords.

Site Security Contacts:

- » are restricted in the scope of their operations to specified sites
- » cannot assign and revoke Security Contact rights.

Organisation Security Contacts:

- » are not restricted in the scope of their operations to specified sites
- » can appoint and revoke the appointment of all Security Contacts.

Security Contacts will be required to:

- » certify that any new User has signed an undertaking to comply with this Policy on a “User Security Declaration” form supplied by DEEWR
- » store the “User Security Declaration” form securely on the External User Organisation’s premises and produce the completed forms to DEEWR on demand.

At its discretion, DEEWR may provide an alternate, online mechanism to obtain the User Security Declaration and this mechanism would replace the earlier method.

Security Contacts **must** ensure that every User has a valid e-mail address recorded in DEEWR’s Online Identity Management System.

DEEWR may communicate with DEEWR Systems Users for day to day functions by email including incident management and other functions.

4.7 User self-management

External User Organisations **must** ensure that all details supplied to DEEWR through the Online Identity Management System are accurate. The External User Organisation may require Users to update their own information directly, or the Organisation’s Security Contacts may perform this task.

User password self-service provided in the DEEWR Identity Management system will require that all Users:

- » have a valid, current e-mail address
- » record one or more questions and answers including information known only to the User.

4.8 DEEWR override

DEEWR reserves the right to manage all aspects of External User Organisations DEEWR Systems user IDs, including DEEWR Systems Roles, Security Contact authorisation and all system access rights and will make reasonable efforts to notify External User Organisations when this occurs.

4.9 Authentication

Each User **must** only use the user ID assigned to them to access DEEWR Systems.

Each time DEEWR Systems are accessed, the User **must** be authenticated.

The authentication methods which may be used are:

- » user ID/password
- » one-time password generator “Smart Token” issued by DEEWR
- » Federated Identity Management (FIM).

4.9.1 user ID/password authentication

For tasks other than those used in Smart Token authentication, authentication of Users will be by means of a user ID and password.

Only a Security Contact can assign initial passwords and perform password resets. Users **must** immediately change a reset password or initial password during the first successful logon.

A password **must** be at least nine characters long and contain characters from three of the following four categories:

- » lower case characters (a-z)
- » upper case characters (A-Z)
- » digits (0-9)
- » punctuation and special characters (e.g. !, \$, #, or %).

The password **must not** contain the User’s user ID, first name or last name.

Users can directly change their passwords at any time except for the forty-eight hours immediately following their last change of password.

Access rights will be suspended automatically after five failed attempts (account lockout following attempt to logon with bad password) and may only be reinstated by a Security Contact.

4.9.2 One-time password generator (Smart Token) authentication

Smart Token authentication **must** be used to perform the following tasks:

- » assign a DEEWR-generated DEEWR System user ID to an individual (Create User transaction)
- » terminate a User’s relationship with the External User Organisation by deactivating the User’s user ID.

DEEWR will issue a Smart Token to each Security Contact and will manage the Smart Tokens.

4.9.3 Federated identity management (FIM)

Federated identity management (FIM) is an authentication process that lets users use the same identification credentials to logon to multiple systems. DEEWR is investing in and developing FIM for specific systems.

4.10 Suspension and deactivation of absent or exiting Users

A Security Contact **must** disable a User's user ID when that User is taking leave or is, for any other reason, expected to cease using DEEWR Systems for a period of thirty days or more.

Users planning to take leave for thirty days or more or are, for any other reason, expecting to cease using DEEWR Systems for a period of thirty days or more **must** notify their Security Contact, so that their user IDs can be temporarily disabled.

DEEWR systems will disable user accounts automatically after forty days of inactivity. A Security Contact may re-enable accounts disabled in this manner if they are still required.

External User Organisations **must** deactivate a User's user ID through the Online Identity Management system upon the termination of the User's employment or association with the External User Organisation.

DEEWR Systems will decommission Users' user IDs automatically ninety days after a user ID has been disabled. These user IDs will no longer be available for reactivation in the DEEWR identity management tool (e.g. i:am) by a Security Contact. However, these user IDs will be available for investigation if required by DEEWR.

4.11 Termination of a Contracted Service Provider's access

DEEWR may immediately terminate a Contracted Service Provider's access in whole or in part when DEEWR considers that this Policy:

- » has been breached, or
- » is being consistently breached.

DEEWR may also terminate a Contracted Service Provider's access in whole or in part when DEEWR considers that doing so would protect the security, integrity or availability of DEEWR Systems.

When DEEWR partially terminates a Contracted Service Provider's or External User Organisation's access, it may:

- » terminate the Contracted Service Provider's or External User Organisation's access to parts of DEEWR systems, and/or
- » terminate some or all of the Contracted Service Provider's or External Users Organisation's employees' access to DEEWR systems.

Access will only be re-established when the Contracted Service Provider satisfies DEEWR that:

- » the Policy has not been breached, or
- » actions have been taken to ensure that no further breaches will occur.

PART 5 Contracted Service Providers storing, retaining or presenting DEEWR data

Note: Sections 4.1: Physical Access and 4.2: Cyber security incidents equally apply to Contracted Service Providers storing or retaining DEEWR data.

5.1 Protective Security Policy Framework (PSPF) mandatory requirement – GOV 12

GOV 12: Agencies must ensure the Contracted Service Provider complies with the requirements of this policy and any protective security policies

Agencies are to:

- » apply necessary personnel security procedures to private sector organisations and individuals who have ongoing access to Australian Government assets, as specified in the Australian Government Personnel Security Protocol, and
- » ensure the safeguarding of government assets, including ICT systems by:
 - › specifying the necessary protective security requirements in the terms and conditions of any contractual documentation, and
 - › undertaking assessments visits to verify that the Contracted Service Provider complies with the terms and conditions of any contractual documentation.

5.2 ISM requirements

All ISM requirements listed below must be met, though Contracted Service Providers (system owner) may choose to be non-compliant. If choosing to be non-compliant, the Systems Owners will need to make a case to the DEEWR Chief Information Security Officer (CISO) or the Agency Head outlining the reason for non-compliance.

As a general rule, the ISM requires “*industry partners handle information appropriately and implement the same security measures as their sponsoring agency*”.

The following mandatory control requirements are drawn from the ISM:

Service providers’ systems storing DEEWR data

*Control: 0873; Service providers’ systems **should** be located in Australia.*

*Control: 1073; Service providers **should** not allow information to leave Australian borders unless approved by the sponsoring agency.*

The location of the Service providers’ systems (servers and data storage) is to be documented within the Security Risk Management Plan (SRMP).

Service providers' ITSM

*Control: 0744; Service providers **should** provide a single point of contact who will act as an equivalent to an ITSM.*

The name and contact details of the person designated as the IT Security Manager is to be documented within the SRMP.

5.3 IT Security governance framework

5.3.1 Protective Security Policy Framework (PSPF) mandatory requirement – INFOSEC 4

INFOSEC 4: *Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security.*

5.3.2 Information Security Policy

Contracted Service Providers are required upon request to make available their Information Security Policy. It is highly recommended that the policy addresses the following topics:

- » personnel responsibilities
- » configuration control
- » access control
- » networking and connections with other systems
- » physical security and media control
- » emergency procedures and cyber security incident management
- » change management
- » information security awareness and training.

5.4 IT Security Documentation

So that DEEWR is able to understand and assess the risk of externally hosted data and systems, contracted service providers are required to provide the following IT security documentation:

- » System Security Plan (SSP)
- » System Risk Management Plan (SRMP)
- » Incident Response Plan (IRP)

DEEWR will provide templates to assist in the production of these documents.

IT security documentation is used to clearly define:

- » security vulnerabilities the department may be exposed to as a result of implementation of a system
- » the consequences of the exploit of said vulnerabilities
- » the controls put in place to mitigate either the likelihood of the exploit of a vulnerability or the consequences thereof
- » processes and responsibilities that may be required in the case of a cyber security incident.

The DSD *Information Security Manual (ISM)* provides extensive guidance to the content and production of the Security documentation.

The ISM and the ISO standard 27005 *Information technology - Security techniques – Information security risk management* are recommended as best practice for developing and in implementing risk management plans.

5.4.1 Security Risk Management Plans (SRMPs)

The Security Risk Management Plan is the instrument used to describe system risk, and to facilitate the acceptance of that risk. The SRMP is also used to describe the rationale for non-compliance against ISM controls, if applicable.

5.4.2 System Security Plans (SSPs)

Where the SRMP describes a system's risk for the consumption of System Owners, the SSP is designed to give more detailed descriptions of system security controls for System Managers and technical staff. SSPs will detail the implementation of all security controls identified in a system's SRMP. These controls may be technical, procedural, policy or otherwise.

5.4.3 Standard Operation Procedures (SOPs)

Where a system's security controls are procedural, these procedures should be described in one or more SOPs. SOPs should be referenced and linked from within a system's SSP.

5.4.4 Incident Response Plans (IRPs)

Contracted Service Providers are required to make available an Incident Response Plan.

The Incident Response Plan details processes and responsibilities that may be required in the case of a *cyber security incident*. The IRP should be the first point of reference for serious system breaches or failures, and so should adequately detail things like recovery processes and investigation requirements.

5.5 System security

The Contracted Service Provider is responsible for the physical and logical access controls to their systems.

5.6 System accreditation

It is highly recommended that contracted service providers build and assess their systems to meet the requirements of:

- » Australian Government Defence Signals Directorate (DSD) Information Security Manual (ISM)
- » ISO Standards
 - › 27005 Information technology – Security techniques – Information security risk management
 - › 27002:2006 Information technology – Security techniques – Code of practice for information security management

5.7 Minimum security standards

Contracted Service Providers **must** ensure that all ICT systems containing DEEWR data:

- » have installed and maintained antivirus software
- » are kept current with all critical operating system and application security patches and updates
- » ensure all users have individual logon accounts with complex passwords
- » ensure adequate system logging is in place to support cyber incident response or other enquires
- » ensure that logging of privileged user (e.g. administrator , root, etc) actions is enabled and logs are stored to support cyber incident response or other enquiries
- » rename default Administrator accounts and disable Guest accounts
- » if using wireless networking:
 - › use robust encryption (WPA or higher is recommended)
 - › change the default administration name and password to the router or similar device.

5.8 Data segregation

In shared environments involving virtualisation and “multi-tenancy” mechanisms, the Contracted Service Provider is required to ensure logical and network segregation between systems containing DEEWR data and other tenants.

5.9 Data destruction and media sanitisation

All ICT systems including backup and redundancy systems containing DEEWR data **must** be sanitised and overwritten to prevent forensic recovery of any DEEWR data:

- » prior to the disposal, trade in or sale of any equipment
- » at the termination of the contract, or
- » as instructed by DEEWR.

APPENDIX 1 Glossary

Authentication	Presentation and validation of credentials such as user ID and a password or one-time password, linking a person to a specific user ID.
Authorisation	Establishing the right of a particular user ID to access an application, or facility within a system, or to the system as a whole.
Contract	A contract between DEEWR and a business for the supply of services to DEEWR.
Cyber Security Incident	<p>Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.</p> <p>A cyber or security incident can range from a simple virus to the disclosure of sensitive information.</p>
DEEWR systems	The DEEWR computer system, including the ECSN Portal and other secure pages and all other DEEWR online computer applications, information technology data, equipment and processes.
DEEWR systems role	A label for a defined set of applications and facilities which may be assigned to a User to authorise that User to perform specific functions.
External User Organisation	An entity supplying services to DEEWR, bound by a contract and required to use DEEWR Systems.
EULA	End User License Agreement
FOUO	For Official Use Only
Password/Passphrase	Passphrases equally applies to Passwords.
Password reset	If a User forgets their password, they may request a new password from a Security Contact. The Security Contact authenticates the User and issues the new password. The need for this service is greatly reduced by password self-service.
Policy	The “DEEWR External Security Policy – For Contracted Service Providers and Users”.
user ID	The name and details used to identify a specific User within DEEWR Systems, sometimes known as Account.
User	A person who accesses DEEWR Systems