Australian Government
Department of Employment and Workplace Relations

Third Party IT Vendor Deed Guidelines

RFFR accreditation must be achieved before a Third Party IT Vendor can enter into a deed with the Department to provide Software-as-a-Service to Applicable Entities.

V1.0

May 2023

Version Control

Version	Change summary	Date
1.0	First release	May 2023

Table of Contents

Contents

Version Control **2**

First release **2**

May 2023 ..... **2**

Guideline Management **5**

Disclaimer 5

Purpose of Guideline 5

Reading Notes 5

Audience 6

Review Date 6

Advice on these Guidelines 6

Glossary 6

Definitions 6

1. ESAF and RFFR Accreditation **7**

1.1 Vendor requirements 7

1.2 RFFR Accreditation process 7

1.3 Access and information security assurance requirements for TPES Systems 8

2. Privacy, FOI and Protected Information **10**

2.1 Overview 10

2.2 The Australian Privacy Principles 10

2.3 Privacy Incidents and the Notifiable Data Breach Scheme 11

2.4 Privacy complaints 12

2.5 Awareness and Training Expectations 12

2.6 Personnel Compliance 13

2.7 Freedom of Information requests 13

2.8 Protected Information 13

2.9 Offences related to Protected Information 13

2.10 Consent 15

2.11 Subpoenas or notices to produce 15

3. Records Management **16**

Supporting Documents for this Chapter 16
3.1 Overview 16
3.2 Records Framework 16
3.3 Management of Records 17
3.4 Movement of Records 19
3.5 Transfer of Records between Vendors 20
3.6 Data Migration 20
3.7 Data Security Considerations 21
3.8 Decommissioning of Systems 21
3.9 Breaches and Inappropriate Handling of Records 21
3.10 Retention of Records 22
3.11 Disposal of Records 23

Guideline Management

Disclaimer

These Guidelines are not a stand-alone document and do not contain the entirety of Third Party IT Vendor (**Vendor**) obligations. These Guidelines form part of the Third Party IT Vendor Deed (**the Deed**) (refer to clause 1.3 of the Deed) and must be read in conjunction with:

- the Deed executed by your organisation, including any other reference material issued by the Department of Employment and Workplace Relations under or in connection with the Deed; and
- Right Fit For Risk Cyber Security Accreditation - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au).

These Guidelines may be varied by the Department at any time at the Department's absolute discretion and Vendors must perform all obligations in their Deed in accordance with these Guidelines.

These Guidelines are not legal advice and the Commonwealth accepts no liability for any action purportedly taken in reliance upon these Guidelines and assumes no responsibility for the delivery of services by Third Party IT Vendors to entities providing services to the Commonwealth (Applicable Entities). These Guidelines do not reduce the obligation of Vendors to comply with their relevant legal obligations and, to the extent that these Guidelines are inconsistent with obligations under the Privacy Act, social security law[1], the WHS Laws or any other legislation or laws relevant to the respective jurisdiction in which Vendors operate, the relevant legislation or laws will prevail.

Purpose of Guideline

These Guidelines form part of the Deed and provides information for Vendors on their continuing obligations.

Reading Notes

These Guidelines adopt the following conventions:

- **MUST** indicates a mandatory requirement that a Vendor is required to satisfy to obtain or maintain Accreditation of the TPES System.
- **MUST NOT** indicates something that if practiced, exercised, or implemented will breach a TPES System Accreditation requirement.
- **SHOULD** indicates something that is not mandatory but is recommended which either supports a mandatory obligation or is considered best practice.

[1] social security law means "(a) the Social Security Act 1991; and (b) the Social Security (Administration) Act 1999; and (c) any other Act or provision of an Act that is expressed to form part of the social security law, and (d) a legislative instrument made under an Act or provision in paragraphs a, b or c above."

Audience

Vendors who have accredited TPES Systems[2] under the Deed with the Department.

Review Date

This document will be reviewed annually. However, if there are security, or other material or operational reasons, these Guidelines may be updated on an as needed basis. This may mean that reasonable additional actions may be required by Vendors to maintain Accreditation of their Accredited TPES System (*Deed reference clause 5.1(f)*).

It is the responsibility of Vendors to ensure that they meet the requirements of the latest version of these Guidelines when published. The current version of these Guidelines and a version history is available at www.dewr.gov.au.

Advice on these Guidelines

Feedback on these Guidelines or suggestions are welcome at SecurityComplianceSupport@dewr.gov.au.

Glossary

All capitalised terms in these Guidelines have the same meaning as in the Deed unless otherwise indicated or defined below.

Definitions

'ACSC' means the Australian Cyber Security Centre.

Digital Transformation Agency's Hosting Certification Framework means the Whole of Government Hosting Strategy Hosting Certification Framework guidance for Australian government customers available at https://www.hostingcertification.gov.au/, as updated from time to time.

'Notifiable Data Breach scheme' means the scheme under which any organisation or agency that the Privacy Act 1988 covers must notify affected individuals, relevant entities and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

'Third Party IT Services arrangement' means the arrangement between an Applicable Entity and a Vendor to provide Third Party IT services to the Applicable Entity to support the delivery of employment services by the Applicable Entity.

[2] Details of the current Accredited TPES Systems can be found at Accredited Third Party Employment and Skills (TPES) Systems - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au) or Schedule 2 [Scope of Accreditation] to the Vendor's Third Party IT Vendor Deed.

1. ESAF and RFFR Accreditation

The Department uses the External Systems Accreditation Framework (ESAF) and the Right Fit for Risk (RFFR)[3] assurance approach to assess and accredit Information Security Management Systems.

1.1 Vendor requirements

(Deed reference - clause 5.1(d))

1.1.1 Organisational requirements

In order to maintain Accreditation, a Vendor **must** comply with all requirements set out in the ESAF, these Guidelines and the Deed, including to:

- be registered with the Australian Business Register (ABR) and maintain a current Australian Business Number (ABN);
- be physically located within Australia and provide services from within Australia;
- advise the Department of any Change in Control and Change of Circumstance;
- develop and maintain a change management process which at a minimum defines the actions to be undertaken before and after standard, urgent and emergency changes are implemented; and
- comply with any additional condition of Accreditation set out in Schedule 2.

1.1.2 Personnel requirements

If the ESAF requires that any Personnel must complete specific Personnel vetting requirements for the purposes of Accreditation or reaccreditation, a Vendor **must:**

- ensure that its relevant Personnel successfully complete the required personnel vetting processes, and bear any costs associated with doing so;
- only allow its Personnel to engage in any duties associated, in any way, with the operation, support and management of the TPES System, or customer sales and support, after they have successfully completed the required personnel vetting requirements; and
- actively manage the ongoing Personnel vetting aftercare in accordance with the ESAF.

Note: The Department may sponsor any Australian Government security clearances if required.

1.2 RFFR Accreditation process

For RFFR Accreditation process and requirements to obtain and maintain accreditation, please see Right Fit For Risk Cyber Security Accreditation - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au).

[3] https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation

1.2.1 Variation requirements

(Deed reference – clause 5.1(e); definitions)

The environment within which Vendors operate is not static. Changes occur that are either external in origin or because of internal policy decisions. Some changes to a Vendor's circumstances or control may impact the Accredited TPES System's security profile.

In the context of the ESAF, a Change in Control of a Vendor and/or a Change of Circumstance to a Vendor's systems, processes or arrangements must be risk assessed by both the Vendor and the Department in terms of its impact on:

- the security of the Vendor's operations and the TPES System;
- the privacy of participant's personal information (in particular, any sensitive information); and
- the security of Departmental systems and data.

Changes in Control and material Changes of Circumstance **must** be Notified to the Department (clause 18 of the Deed). A Change of Circumstance may include for example a change of system architecture. Noting this is not an exhaustive list, changes to network design, encryption in transit and at rest, data plane and control plane, hosting arrangements, sub contractual arrangements, and authentication and authorisation may be considered material.

ALL details regarding any Changes in Control of a Vendor or Changes of Circumstance **must** also be documented in any application for reaccreditation or revised scope regardless of whether the Provider considers that they impact the TPES System's security profile.

1.2.2 Accrediting an additional TPES System

Vendors **must:**

- obtain accreditation for each separate TPES System they intend to offer to Applicable Entities for use in the delivery of Departmental programs.

The Department may amend Schedule 2 of the Deed to reflect the Accreditation of any additional TPES Systems by providing Notice to the relevant Vendor *(see clause 5.1(g) of the Deed*.

1.3 Access and information security assurance requirements for TPES Systems

1.3.1 Access to Department's IT Systems

(Deed reference – clause 5.2)

To be able to access the Department's IT Systems, Vendors **must** meet certain requirements under the Deed as described below**.**

1.3.2 Changes to Department's IT Systems

(Deed reference – clause 5.2(c))

During the Term of this Deed, the Department may make changes to the Department's IT Systems at any time. The Department will provide reasonable information about any changes to Vendors. These changes to the Department's IT Systems may affect an approved interface and the functioning of any TPES System.

Regardless of any changes to the Department's IT Systems, Vendors **must** ensure that Accredited TPES Systems are always consistent with the Department's IT Systems and **must** bear the cost and expense of doing so.

1.3.3 Department Data Sovereignty

Vendors **must** meet data sovereignty requirements as specified in the RFFR, that all data relating to the Services is not accessible from outside of Australia, and no data relating to the Services is transferred or stored outside of Australia, without prior written approval from the Department.

1.3.4 Hosting requirements

A Vendor **must** use a Hosting Service certified under the Digital Transformation Agency's Hosting Certification Framework[4].

[4] https://www.hostingcertification.gov.au/

2. Privacy, FOI and Protected Information

Supporting weblinks and documents relating to this Chapter

- Australian Privacy Principles (APPs)
- Privacy and the Department
- Provider Privacy Incident Report

2.1 Overview

Privacy is a fundamental consideration under the ESAF.

Vendors **must** comply with the *Privacy Act 1988* (Cth) (Privacy Act) which regulates the handling of personal information through minimum privacy standards known as the Australian Privacy Principles (APPs).

The APPs set out standards, rights, and obligations for the handling, holding, accessing and correction of personal information (including sensitive information).

This Chapter provides information for Vendors and their Personnel on their obligations in relation to handling personal and protected information about individuals, as well in relation to reporting privacy incidents.

2.2 The Australian Privacy Principles

'Personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, or is recorded in a material form or not[5].

Personal information includes an individual's name, signature, date of birth, address, telephone number, sensitive information, bank account details, employment information, and commentary or opinion about an individual. This kind of information may be shared verbally, contained in physical or digital files or documents, such as résumés or application forms provided by the individual, or in an email or text message, or recorded.

'Sensitive information' is a subset of personal information and includes information that relates to an individual's racial or ethnic origin, health status, genetics and biometrics, religious beliefs or affiliations, philosophical beliefs, sexual orientation, criminal record or membership of a political association, professional or trade association or trade union[6].

In delivering a TPES System for use by Applicable Entities, Vendors may, on their behalf, collect and store, personal information about individuals. In handling this personal information, Applicable

[5] See definition of personal information in section 6 of the Privacy Act 1988.

[6] See definition of sensitive information in section 6 of the Privacy Act 1988

Entities and Vendors are required under the relevant Deed to comply with the Privacy Act and the APPs as if they were agencies. The 13 APPs govern the standards, rights, and obligations around:

- governance and accountability (APP 1);
- collection, use and disclosure of personal information and government related identifiers (APP 2, 3, 4, 5, 6, 7, 8 and 9);
- quality and protection of personal information (APP 10 and 11); and
- the rights of individuals to access and correct their personal information (APP 12 and 13).

The APPs are principles-based law. Vendors must consider their own situation and the Deed provisions and implement procedures and policies to ensure compliance with the relevant APPs.

Vendors are directed to the APP Guidelines which can be found on the OAIC website for further direction.

2.3 Privacy Incidents and the Notifiable Data Breach Scheme

Vendors are required under the Notifiable Data Breach scheme to notify Applicable Entities and affected individuals, the Department and the OAIC about eligible data breaches. An eligible data breach occurs when:

- there is unauthorised access to, or disclosure of, personal information held by an entity, or information is lost in circumstances where unauthorised access or disclosure is likely to occur
- it is likely to result in serious harm to any of the individuals to whom the information relates, and
- the entity has been unable to prevent the likely risk of serious harm with remedial action.

Vendors should refer to Notifiable data breaches - Home (oaic.gov.au) for further information.

Vendors **must:**

- comply with any directions, guidelines, determinations, rules, or recommendations of the Australian Information Commissioner;
- notify the Department and any Applicable Entities as soon as possible following becoming aware of any unauthorised access to, use or disclosure of, personal information, or a loss of personal information they hold using the Provider Privacy Incident Report (PPIR). This applies to all privacy incidents, whether they are an eligible data breach or not, in line with the Department's Breach Management Approach[7];
- promptly assess all privacy incidents to determine whether an eligible data breach has occurred and, if required, notify affected individuals and the OAIC;
- provide the Department with a copy of any notification of an eligible data breach made to OAIC and any subsequent correspondence with OAIC; and

[7] Breach Management Approach (ecsnaccess.gov.au)

- take all reasonable steps to ensure that this assessment is completed within 30 calendar days of becoming reasonably aware that there may be an eligible data breach. By responding quickly, Vendors can substantially decrease the impact on affected individuals, and reduce the costs associated with dealing with the privacy incident, including reputational costs.

Vendors **must** also immediately Notify the Applicable Entity and the Department if they become aware:

- of a breach or possible breach of any of the obligations contained in, or referred to in, the Deed(s) by any Personnel or Subcontractor;
- that a disclosure of personal information may be required by law; or
- of an approach to the Vendor by the Australian Information Commissioner or by an individual claiming that their privacy has been interfered with.

Vendors **should** be aware that the Department monitors Personnel access to Records in the Department's IT Systems. Where a clear business reason for access to a Record or Records is not identified, the Department may require further information or investigation by a Vendor and may take action against individuals.

2.4 Privacy complaints

An individual who considers that their privacy has been interfered with can contact the Department, an Applicable Entity, and/or the OAIC to make a complaint. It is unlikely that a complaint will be received by a Vendor. Complaints under the Privacy Act should be directed to the relevant Applicable Entity in the first instance. Applicable Entities are required to respond to any privacy complaints within 10 Business Days and in accordance with the PPIR where a privacy incident has been identified.

For further information and alternative contact details, please refer to the Department of Workplace Relations' Privacy Policy.

2.5 Awareness and Training Expectations

Vendors **must:**

- adopt practices to ensure that its Personnel are aware of their obligations under the Privacy Act, the Deed, and this Chapter; and
- ensure that Personnel who handle or will handle personal information while delivering services to Applicable Entities under the Deed understand their obligations.

Vendors **should:**

- ensure their internal privacy practices, policies and procedures are proactively reviewed, consider compliance with new laws or updated information handling practices, and ensure that they are responsive to new privacy risks; and
- ensure that Personnel undertake privacy and fraud training on an annual basis.

2.6 Personnel Compliance

Vendors **must** monitor and annually self-audit that Personnel have completed privacy training.

The Department may request details of a Vendor's self-audit at any time or may conduct its own audit of a Vendor's compliance with the requirements in this Chapter.

It is recommended that Vendors put in place their own processes to audit the compliance of their Personnel with privacy obligations more generally.

2.7 Freedom of Information requests

(Deed reference: clause 12)

Under the Deed, Vendors are required to assist the Department in processing requests under the *Freedom of Information Act 1982 (Cth)* (the FOI Act) by providing Records (digital or physical) in their possession that are relevant to a request. An individual seeking to access documents containing their personal information may submit a request for access under either the Privacy Act or the FOI Act. However, where the document being sought does not contain the individual's own personal information, access is not available under the Privacy Act as the Privacy Act only allows an individual to access their own personal information.

Requests under the FOI Act should be directed to the Department's Information Law Team at FOI@dewr.gov.au.

2.8 Protected Information

(Deed reference: clause 8.5)

Protected Information is relevantly defined in section 23 of the *Social Security Act 1991* as information about a person that was obtained by an officer under the social security law and is held or was held in the records of the Department or Services Australia. Protected information includes information to the effect that there is no information about a person held in the records of the Department or Services Australia. Protected information may also be personal information under the Privacy Act.

For example, if an individual receives a social security benefit or payment, that individual's information (including their name, date of birth and contact details) will likely be both personal and Protected Information.

2.9 Offences related to Protected Information

(Deed reference: clause 8.5)

It is an offence under the *Social Security (Administration) Act 1999* for a person to intentionally obtain, make a record of, disclose to any other person, or otherwise use, Protected Information if the person:

- is not authorised by or under the social security law to do so, and
- the person knows, or ought reasonably to know, that the information is Protected Information.

This means Vendors' Personnel may commit a criminal offence if they:

- search for, or access, Protected Information not required for their duties
- make copies of Protected Information where not authorised
- disclose Protected Information to other staff or third parties who do not need to know that information, or
- otherwise use Protected Information where not permitted.

2.10 Consent

Vendors may make a record of, use or disclose Protected Information where the person to whom the information relates provides consent to that recording, use or disclosure.

2.11 Subpoenas or notices to produce

If Vendors receive a subpoena or a notice to produce from a court which requires disclosure of Protected Information, they must ensure that they comply with all relevant laws, as well as the requirements of the Deed and guidelines, in responding to that subpoena or notice to produce.

In particular, Vendors should have regard to section 207 of the *Social Security (Administration) Act 1999* in determining whether Protected Information can be disclosed.

3. Records Management

(Deed reference: clauses 10, 11, 12, 13)

Supporting Documents for this Chapter

- General advice on management of Records
- The Office of the Australian Information Commissioner Guide to securing personal information
- Privacy Incident Report

3.1 Overview

This Chapter specifies Vendors' obligations with regards to the creation, management, retention, storage, transfer, and disposal of Records created or used by Vendors and Applicable Entities under relevant Applicable Agreements, and access to those Records by both Vendors' Personnel and Subcontractors.

Vendors **must** create and maintain true, complete, and accurate Records in the connection with the delivery of its obligations under, and in accordance with, the Deed.

General advice on the management and storage of records, information and data is available on the National Archives of Australia (NAA) website.

3.2 Records Framework

Under the Deed, 'Records' means documents, information and data stored by any means (including electronically) and for any purpose and all copies and extracts of the same and includes Deed Records and Relevant Records.

Records includes 4 categories

CATEGORY	DESCRIPTION
Commonwealth Records	Any Records provided by the Department to: • the Vendor for the purposes of this Deed; or • an Applicable Entity under an Applicable Agreement which is Accessed by the Vendor pursuant to the relevant Applicable Agreement, the Third Party IT Services arrangement and this Deed, and includes Records which are copied or derived from Records so provided.

CATEGORY	DESCRIPTION
Deed Records	Any Records • developed or created or required to be developed or created as part of or for the purpose of performing the Deed; • incorporated in, supplied, or required to be supplied along with the Records referred to in the point above, or • copied or derived from Records referred to in the above points, and • includes all Reports.
Vendor Records	All Records, except Commonwealth Records, in existence prior to the relevant Deed Commencement Date: • incorporated in; • supplied with, or as part of, or • required to be supplied with, or as part of, the Deed Records.

3.3 Management of Records

(Deed reference: clause 10.1, 10.2)

Management of Records **must** be in accordance with the "digital by default" approach set out in the Australian Government's Building trust in the public record: managing information and data for government and community policy (effective 1 January 2021).

Vendors **must:**

- wherever possible and consistent with the Deed, and other applicable legal requirements, create and manage Records in a digital format;
- ensure that any Record in a digital format is created, stored and operated in accordance with the Deed requirements, and other applicable legislative provisions, including the *Electronic Transactions Act 1999 (Cth)*;
- ensure that Records in a digital format containing sensitive information as defined in the Privacy Act are kept secure. The Office of Australian Information Commissioner (OAIC) website provides information on keeping personal information secure;
- ensure that Personnel and Subcontractors do not access, copy, disclose or use any:
    - Record containing any information about any participant in any employment services program or skills program; or
    - Record in the Department's IT Systems containing any information about any individual (including individuals who are not participants in any employment services or skills program),

  unless such access, copying, disclosure or use is for the purpose of:
    - providing services to an Applicable Entity under the relevant Applicable Agreement; or
    - otherwise complying with the Deed;
- not access, copy, disclose or use any Record unless such access, copying, disclosure or use is for the purpose of assisting an Applicable Entity to comply with their Applicable Agreement.

Storage requirements

Vendors **must:**

- store all Records in accordance with this Chapter, the Department's Security Policies, and where relevant, its Privacy Act obligations;
- store Records securely either on their own premises or off-site using a records storage facility in compliance with legislation covering the management of Commonwealth/Deed Records, including the Privacy Act*;*
- take such steps as are reasonable in the circumstances to protect Records that contain Protected Information and/or personal information for the purposes of the Privacy Act – in accordance with Australian Privacy Principle 11 – from misuse, interference, and loss, and from unauthorised access, modification, or disclosure:
    - The guide to securing personal information can be found on the OAIC website and provides guidance on the reasonable steps entities are required to take under the Privacy Act to protect the Personal Information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure;
    - Vendors **must** particularly take reasonable steps to protect their systems storing personal information from hacking attacks;
- ensure that the Department can access Records by retrieving Records (including, if stored digitally, by retrieving the digital copy and if relevant printing it) and providing it to the Department or any Applicable Entity (as relevant) upon request;
- ensure physical Records are protected from:
    - storage environment damage (e.g. for paper Records, damp from a cement floor or fire damage);
    - unauthorised addition, alteration, removal, or destruction;
    - use outside the terms of the relevant Deed;
    - for Records containing Personal Information, privacy incidents; and
    - unauthorised access including inappropriate 'browsing' of Records.
- ensure that physical Records containing sensitive information, as defined in the Privacy Act*,* are kept in lockable cabinets with appropriate access management procedures maintained.

General advice on the management and storage of Records is available on the NAA website.

Access to documents and Records

(Deed reference – clauses 11, 12 and 13)

Vendors **must:**

- be able to locate and retrieve Records about a participant if requested by the Department or by an Applicable Entity (for example, where the Department has received a Freedom of Information Act request for Access to a document created by, or in the possession of the Vendor or any Subcontractor);
- where a participant/individual directly requests a Vendor to provide access to Records, including their own information, in the first instance, direct the request to the relevant Applicable Entity. If the participant/individual does not have a relevant Applicable Entity, the request should be referred to the Department, those responsible for Vendor management under RFFR approach;

- inform the Department if they become party to legal action in relation to their previous or current Third Party IT services arrangement, so that arrangements for the appropriate retention of Records can be organised; and
- store Records in such a way that all Records relevant to a request under the FOI Act are able to be located and retrieved efficiently. This includes being able to retrieve email Records and Records created by, or sent to, individuals who have ceased working for Vendors and/or Applicable Entities.

Records Register

(Deed reference: clauses 10.2 and 10.3)

Vendors **must** maintain a register of Records held by them and make this register available to the relevant Applicable Entity to whose Applicable Agreement it relates, and the Department on request.
The register of Records must be created and managed in a digital format (ideally Microsoft Excel or equivalent or a comma or tab limited format) that the Department's IT Systems can read.

Vendors **may** wish to identify on the Records register whether Records are:

- Priority – pertaining to current or pending legal action, Complaint, injury, or possible claim for compensation
- Active – pertaining to current participants
- Inactive – pertaining to former participants
- Damaged – e.g. paper Record affected by water
- Destroyed (whether authorised or accidental) – e.g. paper Record burnt or shredded
- Transferred – participant and Record transferred to another Applicable Entity
- Returned – have been returned to the Department.

3.4 Movement of Records

(Deed reference – clause 10.5)

Vendors **must not**, and **must** ensure that its Personnel do not:

- remove any Records relating to the Deed or the services provided by an Applicable Entity with whom Vendors have a Third Party IT Services arrangement, or allow any Records relating to the services provided by an Applicable Entity with whom a Vendor has a Third Party IT Services arrangement to be removed, from their premises, except to the extent necessary to enable the delivery of the services by that Applicable Entity, or
- take, transfer, transmit or disclose any Records relating to the services provided by an Applicable Entity with whom they have a Third Party IT Services arrangement, or allow any Records relating to the services provided by an Applicable Entity with whom they have a Third Party IT Services arrangement to be taken, transferred, transmitted, accessed, or disclosed, outside of Australia,

without the Department's prior written consent.

Further, the obligation set out above applies in respect of taking, transferring, transmitting, accessing, or otherwise disclosing any Records relating to the services provided by an Applicable Entity with whom Vendors have a Third Party IT Services arrangement, outside of Australia:

- to individuals within their own organisation, and
- to any third party, including to any Subcontractor.

3.5 Transfer of Records between Vendors

(Deed reference: clause 10.5)

Records (digital or physical) must only be transferred between Vendors in accordance with these Guidelines, and where it is required to continue providing services to Applicable Entities under a Third Party IT services arrangement. Records must be transferred securely, as soon as possible and in any case within 20 Business Days of a request by an Applicable Entity to transfer Records. A list of all Records being transferred between Vendors should be provided to the Applicable Entity with whom the receiving Vendor has a Third Party IT services arrangement.

The transfer of Records containing personal information and Protected Information must be undertaken in accordance with the Privacy Act and the *Social Security (Administration) Act 1999* (Cth).

When a Vendor is transferring Records between its Sites, to another Vendor for storage or secure destruction or to the Department, the sending Vendor's **must** ensure that the Records are secure during the transfer process.

3.6 Data Migration

Data migration is the process of transferring data from one application or format to another. It may be required when implementing a new application, which may require data to be moved from an incompatible proprietary data format to a format that can be integrated with new applications.

Vendors must ensure that any migration activities include validation of the migrated data quality to ensure that no data (or Records containing the data) is lost or corrupted, and the data and Records continue to be fit for the intended purpose.

When migrating information, Vendors **must** ensure:

- the migration is planned, documented, and managed;
- pre and post migration testing proves that authentic, complete, accessible, and useable Records can and have been migrated; and
- source Records are kept for an appropriate length of time after the migration to confirm that the migration has been successful. Determination of the specific retention period must be based on an organisational risk assessment.

These requirements are in line with the Archives Act 1983 (Cth) and Archives Regulations. However, if future processes include destroying source Records, it is recommended that Vendors seek independent legal advice to ensure that there is no legal requirement to maintain them.

Migrated business information **must** be at least functionally equivalent to the source record for business, legal and archival purposes. General Records Authority 31 (NAA) permits the destruction of information and records after they have been successfully migrated from one system to another.

Vendors **should** note that information transferred to the Department will be imported into the Department's official recordkeeping system and appropriate classification will be applied at the time of import.

3.7 Data Security Considerations

(Deed reference: clause 5.7)

Vendors **must:**

- if required, ensure that those Personnel or Subcontractors who access sensitive, or security classified information have an appropriate security clearance and a need to know that information;
- ensure that Access to (including remote access) to supporting ICT systems, networks, infrastructure, and applications is controlled;
- ensure that Information in systems is continuously safeguarded from cyber threats; and
- ensure that administrative privileges, such as logon and administrator privileges, are restricted.

Vendors **should** refer to the digital Information Assurance / IT Security Compliance guide on the Department's website and ACSC for more information.

3.8 Decommissioning of Systems

When decommissioning any system, Vendors **should** ensure that they have considered the value of the Records and any ongoing need by the Department or Applicable Entities to access it. If the information is no longer required, the Vendor **must** obtain authorisation from the relevant Applicable Entity to legally destroy that information.

The NAA provides authorisation to destroy Australian Government Records in the form of records authorities.

Digital preservation requires a proactive program to identify records at risk and take necessary action to ensure their ongoing viability. To achieve this, Vendors **must** consider the lifecycle of the information versus the lifecycle of the system and have plans in place to preserve information as needed. Regular and planned migration helps avoid obsolescence and ensures information will continue to be accessible and useable by Applicable Entities.

3.9 Breaches and Inappropriate Handling of Records

(Deed References: clauses 5.8, 13)

Reporting Requirements

Vendors **must** report all incidents involving unauthorised access, damage, destruction, loss or theft of Records to the Department and to the relevant Applicable Entity. Where the Records contain or possibly contain personal information of participants, Vendors must follow the privacy incident reporting process set out in the Chapter 2 Privacy, FOI and Protected Information.

Rectification Requirements

For all incidents involving the misuse, interference, loss, unauthorised access, unauthorised use, unauthorised disclosure, damage, destruction, loss or theft of Records (digital or physical), Vendors **must:**

- immediately make every effort to recover lost or damaged Records (e.g. retrieving or photocopying Records), including if required, arranging and paying for the services of expert contractors (e.g. disaster recovery or professional drying services);
- not destroy damaged Records without prior authorisation from the Department;
- inform Applicable Entities if any Personal Information has been lost or is at risk of being publicly available, i.e., a data breach which may or may not be notifiable;
- inform Applicable Entities if any Protected Information is at risk of being publicly available; and
- review relevant policies and procedures to ensure their adequacy in future.

The Department may make recommendations to the Vendor to mitigate the risk of recurrence of an incident.

3.10 Retention of Records

(Deed reference: clause 10.6)

All Records must be retained by Vendors for a period of no less than 6 years after the creation of the Record, unless otherwise specified in these Guidelines or by the Department. Vendors **must** also meet the requirements of relevant Applicable Entities with respect to Record retention.

Digital Records

Where Vendors are in possession of Records as a result of the provision of services to an Applicable Entity under a Third Party IT services agreement, they **must** only dispose of those Records in accordance with the retention period specified in the Deed and with prior agreement of the Applicable Entity.

For purposes of determining the applicable retention period, a scanned version of a paper Record must have the same creation date as the original source document.

Information in the Department's IT Systems will be retained by the Department for the appropriate retention periods.

Physical Records

Vendors **must** retain relevant paper Records according to the minimum retention periods specified in the Deed and must only dispose of those Records in accordance with the retention period specified in the Deed and with the prior agreement of the Applicable Entity.

3.11 Disposal of Records

(Deed Reference: clause 10.7)

Vendors **must** work with Applicable Entities to dispose of Records as and when requested by the Department.

Methods of destroying Records

When Vendors destroy Records, they **must** use a method that ensures the information is no longer readable and cannot be retrieved.