Australian Government

Department of Defence

RECORDS MANAGEMENT POLICY MANUAL

The *Records Management Policy Manual* (RECMAN) is issued for use by Defence personnel and is effective from the date of publication.

We have authorised this manual on advice from Deputy Secretary Defence Support and Reform as our principal adviser on all aspects of Record and Information Management by Defence personnel.

s22 [redacted] Brendan Sargeant Chief Operating Officer	s22 [redacted] Mark Binskin, AC Air Marshal Vice Chief of the Defence Force

Department of Defence
CANBERRA ACT 2600

19 May 2014

Sponsor:
Deputy Secretary, Defence Support and Reform

Sponsor contact:
Director, Records Management Policy

Effective Date: 19 May 2014

Review Date: 19 May 2019

Cancelled Documents:

Defence Records Management Policy Manual (POLMAN 3)

Defence Instruction (General) (DI(G)) ADMIN 27–2 *Access to Defence and Defence-related archival records under the Archives Act 1983* (also filed as DI(N) ADMIN 8–3, DI(A) ADMIN 4–1 and DI(AF) ADMIN 8–3)

DI(G) ADMIN 27–4 *Defence Records Management Policy* (also filed as DI(N) ADMIN 43–8, DI(A) ADMIN 91–1 and DI(AF) ADMIN 8–17)

Announcement statement—may be announced to the public.

Secondary release—may be released to the public.

All Defence information, whether classified or not, is protected from unauthorised disclosure under the *Crimes Act 1914*. Defence information may only be released in accordance with the *Defence Security Manual* as appropriate.

First edition 2014

Publisher

Defence Publishing Service
Department of Defence
CANBERRA ACT 2600

FOREWORD

1. RECMAN provides guidance for the management of Defence records and complying with the *Archives Act 1983*. It also supports the transition of records to a digital environment in accordance with the Government's Digital Transition Policy.

2. RECMAN establishes a clear, decisive and current records management policy for Defence personnel, and uses Australian and International standards for records and document management to ensure alignment with recognised best practices.

3. This Manual replaces *Defence Records Management Policy Manual* (POLMAN 3), Defence Instruction (General) (DI(G)) ADMIN 27–2 *Access to Defence and Defence-related archival records under the Archives Act 1983* and DI(G) ADMIN 27–4 *Defence Records Management Policy*.

AMENDMENT CERTIFICATE

Amendment		Effected	
No	Date	Signature	Date
AL1	28 May 2014		28 May 2014
AL2	23 December 2014		23 December 2014

CONTENTS

CHAPTER 1

RECORDS MANAGEMENT POLICY MANUAL

INTRODUCTION

1.1 The Department of Defence (Defence) generates an enormous quantity of key decisions and business activities. Defence is required by law to create and maintain full and accurate records as evidence of these decisions and business activities.

1.2 The *Archives Act 1983* imposes statutory obligations on Defence for the management of records, including the actions which must be taken to retain, destroy, store or otherwise deal with Commonwealth records. The *Freedom of Information Act 1982* requires Defence to publish a range of accurate, up-to-date and complete information to support a more open and transparent culture across government. Subsequent government reforms [1] have further raised the importance of effective and efficient information and record management policies and practices.

1.3 The *Records Management Policy Manual* (RECMAN) prescribes Defence's approach to records management and outlines the requirements that must be complied with to fulfil its lawful obligations under the *Archives Act 1983*. The content is consistent with the guidance provided by the National Archives of Australia (NAA) [2] and incorporates relevant Australian and international standards for records and document management.

POLICY STATEMENT

1.4 Defence is committed to information management and record keeping practices that comply with legislation and government policy, provide for public accountability, support decision-making and build on corporate memory including the preservation of historical information. To support this commitment, all Defence records must be created, captured, stored, managed, accessed and sentenced in accordance with the requirements as defined in RECMAN.

SCOPE

1.5 RECMAN applies to all records created as part of Defence decision-making or business activities. All Defence personnel and any individual or firm (including subcontractors) contracted by Defence must comply with RECMAN.

DEFINITIONS

1.6 A list of definitions that apply to this Manual is found in Annex A.

---

1 Attorney-General's Department—Freedom of information reforms.

2 The NAA is the agency responsible for defining all Commonwealth record keeping policies.

SPONSORSHIP AND AUTHORISATION

1.7 The following Defence personnel sponsor chapters of this Defence Manual:

Chapters	Primary Group/Service Sponsor	Group/Co-sponsor(s)
1	Deputy Secretary Defence Support and Reform	Not applicable
2		Chief Information Officer
3		Deputy Secretary Intelligence and Security and Chief Information Officer
4		Deputy Secretary Intelligence and Security and Chief Information Officer

1.8 The First Assistant Secretary Ministerial and Executive Coordination and Communication (FASMECC) is authorised to issue chapters two through to four of RECMAN. FASMECC will also amend the structure and content of RECMAN as necessary, upon assurance that relevant co-sponsor consultation has been undertaken and appropriate approval given.

ROLES AND RESPONSIBILITIES

1.9 The Associate Secretary Chief Operating Officer is the Secretary's principal advisor on all policy and administrative aspects of records management.

1.10 The Deputy Secretary Defence Support and Reform (DEPSEC DSR) is responsible for developing, providing advice on, and ensuring compliance with digital and physical records management policy. DEPSEC DSR delegates this responsibility to FASMECC and the Assistant Secretary Ministerial and Information Management (ASMIM), FASMECC provides advice to the Secretary and the Chief of the Defence Force (CDF), while the ASMIM is responsible for the day-to-day management and monitoring of compliance. DEPSEC DSR is also responsible for maintaining infrastructure and support services for physical records where the Defence Support and Reform Group has assumed ownership.

1.11 The Deputy Secretary Intelligence and Security (DEPSEC I&S) is responsible for providing records management advice and support services, to areas outside the Defence Intelligence Agencies, relating to records (physical or electronic) containing compartmented intelligence information (*see Defence Security Manual*, Part 2.30). DEPSEC I&S is also responsible for enterprise architecture, development, operation and maintenance of Defence records and document management systems on the Top Secret Network.

1.12 The Chief Information Officer is responsible for ensuring that Objective is available, reliable and accessible to staff when required; and ensuring new and existing business support systems comply with this policy and NAA's digital recordkeeping requirements. ASMIM, on behalf of the business owner, is responsible for providing digital business requirements to the Chief Information Officer.

1.13 All Group Heads and Service Chiefs are responsible for ensuring that this policy is complied with by their respective Group or Service and that specific Group or Service procedural guidance is available to support its implementation.

1.14 The Information Management Steering Committee is the high-level decision forum for improving information management in Defence in line with the Information Management Strategic Framework endorsed by the Defence Committee (now Secretary and CDF Advisory Committee).

STRUCTURE AND RELEASE DATES

1.15 The structure and release dates for RECMAN are detailed in Annex1B.

IMPLEMENTATION

1.16 RECMAN replaces the *Defence Records Management Policy Manual* (POLMAN 3) and supersedes Defence Instruction (General) (DI(G)) ADMIN 27–4 *Defence Records Management Policy* and DI(G) ADMIN 27–2 *Access to Defence and Defence-related archival records under the Archives Act 1983*.

1.17 Implementation of the policy will be supported by a range of detailed and practical guidance materials that will be available on the Records Management Policy intranet site.

1.18 All Groups and Services must ensure that appropriate local procedural guidance and adequate resources are in place to enable compliance with the requirements outlined in RECMAN.

GOVERNANCE AND COMPLIANCE

1.19 ASMIM has responsibility for monitoring Defence compliance with the requirements of RECMAN. Under ASMIM direction, the Directorate of Records Management Policy (DRMP) will undertake and coordinate monitoring, reporting and compliance activities to ensure that Groups and Services are complying with RECMAN.

1.20 These activities include:

a. reporting annually, as required by the NAA, on compliance with records and information management policies, standards and guidelines

b. requiring an annual Records Management Certificate of Compliance to be completed by each Group or Service

c. reporting to the Information Management Steering Committee on records management compliance levels and identified key risk areas.

1.21 Further information on governance and compliance is provided in Chapter 3 ‘Governance’.

SUPPORT AND ADVICE

1.22 DRMP is responsible for providing policy support and advice, including assisting Groups and Services to implement RECMAN in a manner appropriate to their business functions and activities. Further information on these support and advice activities is provided in Chapter 3 ‘Governance’.

1.23 Records management areas within the Australian Geospatial-Intelligence Organisation and Australian Signals Directorate are also responsible for providing support and advice when Defence Intelligence Agencies or compartmented intelligence records are involved.

Annexes

1A Glossary

1B Records Management Policy Manual structure and release dates

ANNEX 1A

GLOSSARY

1. **Access controls.** The scheme of non-hierarchical mechanisms, which may be applied to records and record plan entities, to prevent access by unauthorised users. They may include the definition of user access groups and ad hoc lists of individual named users.

2. **Access examination.** The process of examining records to identify any exempt information they may contain. The four main types of access examination are folio-by-folio, item sampling, title checking and full appraisal.

3. **Accession (1).** A group of records or archives from the same source taken into archival custody at the same time.

4. **Accession (2).** The process of formally accepting and recording the receipt of records into archival custody. Accessioning provides basic physical and intellectual control over material coming into archives.

5. **Active metadata.** Metadata available for use by an electronic document and records management system (EDRMS) to support or trigger automated records management processes.

6. **Active record.** A record that has not been closed and which is required for the day-to-day functioning of an agency or person.

7. **Activity.** An umbrella term covering all the functions, activities and transactions of an organisation and its employees. Business activity is used as a broad term, not restricted to commercial activity and including public administration, non-profit and other activities.

8. **Administrative Functions Disposal Authority (AFDA).** A general disposal authority that covers common administrative functions performed by most Australian Government agencies. The structure of the authority is based on the business classification scheme of the *Keyword AAA: Thesaurus of General Terms Commonwealth Version.*

9. **AFDA Express.** AFDA Express is a streamlined version of AFDA (above). It is an easier and quicker option for agencies to use, and includes functions such as finance, human resources, procurement and publications management.

10. **Admissibility.** The quality of being permitted to serve as evidence in a trial, hearing or other proceeding. Material admitted as evidence may be challenged as not authentic or as unreliable. Documentation to support evidence generally relies on the quality of the recordkeeping system creating and managing it.

11. **Appraisal.** The process of evaluating records to determine which are to be retained as archives, which are to be kept for specified periods and, which will be destroyed.

12. **Archives (1).** A building, room or storage area where appraised records are kept.

13. **Archives (2).** An organisation responsible for appraising, accessioning, preserving and granting access to archived records or collections.

14. **Audiovisual record.** A record that has sound and pictorial attributes. 'Audiovisual' is often used in a general sense to distinguish non-textual materials from written records.

15. **Audit trail.** Data that allows the reconstruction of a previous activity, or which enables attributes of a change (such as date, time or operator) to be stored so that a sequence of events can be determined in the correct chronological order. It is usually in the form of a database or one or more lists of activity data.

16. **Backup.** The activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. This is different from archiving information, which is preserving information with a view to its long-term value.

17. **Born digital.** Information that has been created in digital form rather than converted from physical to digital.

18. **Business information system (BIS).** An automated system that creates or manages information about an organisation's activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers eg ISIS, PMKeyS, ROMAN, etc. BIS that create or manage records should have the appropriate functionality for these tasks, or they should interface with other systems that manage the records.

19. **Capture.** The process of lodging a document or digital object into a recordkeeping system and assigning metadata to describe the record and place it in context, thus enabling the management of the record over time.

20. **Commonwealth record.** A record that is the property of the Commonwealth or of a Commonwealth institution; or a record that is deemed to be a Commonwealth record by virtue of a regulation under the *Archives Act 1983*, *but does not include a record that is exempt material or is a register or guide maintained in accordance with the Act.*

21. **Compression.** A process that reduces the amount of space necessary for data to be stored or transmitted. Compression is often used to describe the process of compacting and extracting the information, although the term can be used to distinguish the first phase from the second phase, which is called decompression. The digital image formats JPEG and GIF both use compression to minimise file size.

22. **Content.** That which conveys information, eg text, data, symbols, numerals, images, sound and vision.

23. **Contents date range.** The contents start date and contents end date, which are usually the dates on the first and last folios of a record.

24. **Context.** The background information that enhances understanding of technical and business environments to which the records relate, eg information on the application software, logical business models and the provenance of the record.

25. **Control record.** A record created and maintained to help identify and retrieve other records. Agency control records include such registry tools as record registers, movement registers, subject indexes and name indexes.

26. **Conversion.** The process of changing records from one medium to another or from one format to another. Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content). Examples include microfilming and digital imaging/scanning of paper records.

27. **Copying.** The production of an identical copy on the same type of medium (paper, microfilm or electronic), eg from paper to paper, microfilm to microfilm or the production of backup copies of electronic records (which can also be made on a different kind of electronic medium).

28. **Create (a record).** To make a record (evidence) of business transactions.

29. **Custody.** The responsibility for the care of records and archives, usually based on their physical possession. Custody does not necessarily include legal ownership.

30. **Data.** Data can be defined as facts represented as text, numbers, graphics, images, sound, or video. Data is raw material used to represent information, or from which information can be derived.

31. **Database.** An organised collection of related data. Databases are usually structured and indexed to improve user access and retrieval of information. They may exist in physical or digital format, and may or may not be recordkeeping compliant.

32. **Decrypted record.** A record that was subject to an encryption process but has since been successfully deciphered.

33. **Defence.** The Department of Defence, Australian Defence Force (ADF) and the Defence Materiel Organisation (DMO).

34. **Defence civilian.** Defence civilian, as defined in section 3 of the *Defence Force Discipline Act 1982* (DFDA), means a person (other than a Defence member) who:

a. with the authority of an authorised officer as defined in the DFDA, accompanies a part of the ADF that is outside Australia, or on operations against the enemy

b. has consented, in writing, to subject themselves to ADF discipline while so accompanying that part of the ADF.

35. **Defence employee.** A person employed in the Department of Defence under section 22 of the *Public Service Act 1999* (the Public Service Act).

36. **Defence personnel.** All Defence employees, Defence employees locally engaged overseas, Defence civilians, Defence members and the equivalents from other Defence organisations on exchange to Defence.

37. **Deletion.** The process of removing, erasing or obliterating recorded information outside the disposal process. Deletion does not meet the requirements for destruction of Commonwealth records as it may be possible to retrieve the deleted data before it is completely over-written and obliterated by the system.

38. **Description.** The process of recording information about the nature and content of records. The description identifies such features as provenance, arrangement, format, contents, and administrative and recordkeeping contexts, and presents them in standardised form.

39. **Descriptive metadata.** Metadata that is available for informational purposes only (such as comments and notes fields) and is not actively used by an electronic records management system to support or trigger automated records management processes.

40. **Destruction.** The National Archives issues disposal authorities for the disposal of Commonwealth records for the purposes of the *Archives Act 1983.* Destruction should be carried out by an approved method such as shredding or, in the case of electronic records, rendering them unreadable.

41. **Digital archive.** An archive which performs the same role in the digital world as traditional archives have in the paper world. It is broader than just a digital repository storing digital items. It ensures that digital records are professionally created, managed and preserved, while also ensuring access over time. A digital archive encompasses the technical infrastructure, standards, policies and procedures and support services for managing and providing access to digital objects and their associated metadata.

42. **Digital Asset Management System (DAMS).** Software responsible for the complete management of digital assets (including ingest, cataloguing, storage, audit, retrieval and distribution).

43. **Digital document.** A document created and/or maintained by means of digital computer technology.

44. **Digital folder.** A set of related digital records held in a tight-knit relationship and managed as a single object. It may also be referred to as a ‘container’.

45. **Digital preservation.** The series of managed activities necessary to ensure continued access to digital materials for as long as necessary. Digital preservation is defined very broadly as all of the actions required to maintain access to digital materials beyond the limits of media failure or technological change.

46. **Digital record.** A record created and/or maintained by means of digital computer technology. It includes records that are born digital or have undergone conversion from a non-digital format. Digital records are a subset of electronic records.

47. **Digital repository.** A device on which digital records and their associated metadata are stored.

48. **Digitisation.** The process of creating digital files by scanning or otherwise converting physical materials. The resulting digital copy is subject to the same retention and disposal requirements as the original.

49. **Disaster plan.** A written procedure setting out the measures to be taken to minimise the risks and effects of disasters such as fire, flood or earthquake, and to recover, save and secure the vital records should such a disaster occur.

50. **Disaster preparedness and response.** A range of activities aimed to reduce the risk of damage that might occur to records as a result of any disaster situation. Disasters can range in scale from minor flooding arising from leaking water pipes to major fire damage arising from a natural disaster. It encompasses planning, training, maintenance of relevant documentation, procurement of services, equipment and supplies, and salvage.

51. **Disposal.** The act of implementing a disposal action in accordance with a records authority and when the record is no longer required for business use. The National Archives authorises the disposal of Commonwealth records for the purposes of the *Archives Act 1983*. Generally this is achieved by issuing either a Commonwealth records authority (RA), or a Defence specific RA.

52. **Disposal action.** A ‘keep, destroy or transfer’ action stipulated in a record authority indicating the minimum retention period for a record and the event in relation to which the disposal date should be calculated.

53. **Disposal class.** A description of the activity documented in applicable records, and the appropriate disposal action for those records.

54. **Disposal freeze.** A ban on disposal action that applies to certain groups of records as designated by the National Archives of Australia. Records subject to a freeze must not be destroyed.

55. **Disposal trigger.** The point from which the disposal action is calculated. This can be a date on which action is completed or a date on which an event occurs. Examples include ‘Destroy 20 years after last action’ or ‘Destroy 75 years after date of birth’.

56. **Electronic document management system (EDMS).** An automated system that supports the creation, use and maintenance of electronically-created documents for the purpose of improving an organisation’s workflow. These systems do not necessarily incorporate recordkeeping functionality, and the documents may be of informational rather than evidential value (ie the documents may not be records). EDMS is a subset of business information systems whose primary purpose is to support creation, revision and management of digital documents.

57. **Electronic document and records management system (EDRMS).** A system used to:

ensure the authenticity, reliability, usability and integrity of records

support the conduct of Defence business

support compliance with the regulatory environment

provide accountability.

58. **Electronic messages.** Any personal or business communication using an electronic system for the conduct of official business. Common examples include email, instant messaging and SMS (short messaging services).

59. **Electronic messaging systems.** Applications used by agencies or individuals for sending and receiving, as well as storing and retrieving, electronic messages. These systems generally do not possess recordkeeping functionality. Example: Outlook.

60. **Electronic record.** A record created, communicated and/or maintained by electronic means. Although this term can refer to analogue materials (eg videotapes), it generally refers to records held in digital form on magnetic or optical computer storage media.

61. **Electronic transaction.** A packet of data transmitted in the course of conducting business online, whether in the form of a, automated transaction or other type of digital communication.

62. **Embargo.** A temporary restraint on the disposal of records, including transfer or destruction. In the content of RECMAN, the term embargo is used to refer to internally-mandated injunctions on records disposal set by Defence, as distinct from freezes imposed by the NAA. (*see* Freeze).

63. **Export.** An access or transfer process whereby copies of a digital record (or group of records) are passed with their metadata from one system to another, either within the organisation or elsewhere.

64. **External service provider.** External service provider means an organisation or individual engaged by Defence that:

a. represents a business resource and is subject to direct management by Defence or

b. is an organisation or individual engaged by Defence to undertake a consultancy that meets the criteria for reporting consultancies on AusTender as defined by the Department of Finance and Deregulation:

(1) the services to be provided involve the development of an intellectual output that assists with Defence decision-making and

(2) the output will reflect the independent views of the consultant and

(3) the output is the sole or majority element of the contract, in terms of relative value and importance.

Individuals engaged as APS or ADF employees are not included.

65. **File (1).** An organised unit of records kept together because they relate to the same subject, activity or transaction.

66. **File (2).** The process of capturing records by placing them on a file.

67. **File census.** A stocktake of all an organisation's files stored in a designated area. A file census or muster is usually carried out to gather data to update the organisation's file tracking system.

68. **File muster.** A stocktake of all an organisation's files stored in a designated area. A file muster or census is usually carried out to gather data to update the organisation's file tracking system.

69. **File part.** A part of a file (or item) that has no independent existence or control apart from the other part(s) of the file. File parts should be retained together, and may not be independently destroyed.

70. **Folder.** A container used to organise records within a file, or files within a system.

71. **Folio (1).** A leaf of paper or page in a file, usually numbered on one side only.

72. **Folio (2).** To assign a number to a leaf or page.

73. **Format.** The physical form (such as paper or microfilm) or computer file format in which a record is maintained.

74. **Freeze.** A temporary restraint on the disposal or transfer of records. In the context of RECMAN, freeze is used to refer to externally mandated disposal bans, usually imposed by the National Archives of Australia. Occasionally, prominent or controversial issues or events, or judicial proceedings have implications for the management of records held by agencies. In such cases, the Archives may support compliance requirements or an identified need to suspend Archives' records destruction permissions by issuing a records disposal freeze or retention notice. Generally, these state that agencies must not destroy any relevant records. (*see* Embargo).

75. **Full and accurate record.** A record that is:

- compliant with the recordkeeping requirements arising from the regulatory and accountability environment in which the organisation operates
- adequate for the purposes for which it is kept
- complete—containing not only the content, but also the structural and contextual information necessary to document a transaction
- meaningful—containing information and/or linkages that ensure the business context in which the record was created and used is apparent

- comprehensive—documenting the complete range of the organisation's business for which evidence is required
- accurate—to reflect the transactions that it documents
- authentic—enabling proof that it is what it purports to be and that its purported creators did indeed create it
- inviolate—securely maintained to prevent unauthorised access, alteration or removal.

76. **Function.** Functions represent the major responsibilities that are managed by the organisation to fulfill its goals. They are high-level aggregates of the organisation's activities.

77. **General records authority (GRA).** A records authority that covers functions common to all or most government agencies, usually produced by the National Archives on behalf of the Australian Government.

78. **Handheld Imagery (HHI).** Imagery derived from devices that are carried and operated personally recording either still frame or video. It includes, but is not limited to:

- negatives, photographic prints and slides
- video stills, digital video files and analogue tapes
- cassettes or compact discs
- scanned images.

79. **Hierarchical relationship.** A relationship based on degrees or levels of superordination and subordination, where the superordinate term represents a class or whole and the subordinate terms refer to its members or parts. A relationship between terms that is based on a ranking or order from a superior to a subordinate position.

80. **High value records.** High value records are those that are useful, important, in the national interest, or have significant historical value.

81. **Hybrid file.** A set of related digital and physical records that are linked by metadata and managed as a single file.

82. **Image format.** The specification under which an image has been saved to disk or in which it resides in a computer memory. There are many commonly used digital image formats including TIFF, DIB, GIF and JPEG. The image format specification dictates what image information is present and how it is organised in memory.

83. **Import.** To receive digital records and associated metadata into one system from another, either from within the organisation or from elsewhere.

84. **Important records.** Important records are those that provide legal and regulatory evidence of activities and decisions containing information about people,

events, issues, places and times. The effective management of these records improves the quality, timeliness and transparency of decisions. Important records usually have a temporary retention period from eight to 130 years. They must be assessed prior to disposal and can only be disposed of using a Records Authority.

85. **Inactive record.** A record that is not required to be readily available for the business purposes of a department or agency and may therefore be transferred to intermediate storage, archival custody or be destroyed subject to applicable records authorities.

86. **Information.** Data in context. Without context, data is meaningless. Context includes:

a. the business meaning of data and related terms

b. the format in which data is presented

c. the timeframe represented by the data

d. the relevance of the data to a given usage.

The value of ‘information’ can be measured by its ability to affect behaviour, influence a decision, or determine an outcome.

87. **Inherit.** To take on a metadata attribute from a parent entity.

88. **Inherited record.** A record that has been passed from one agency to another when responsibility for the relevant function is transferred or one agency is absorbed by another, including when state agencies are absorbed by Australian Government agencies.

89. **Instance.** A version of a digital record in a particular format or at a particular point in time. For example, one instance of a record may be in its native format while another instance is a rendition. Instances may be created as a product of migration or conversion processes.

90. **Integration.** A tight-knit relationship between an electronic records management system and another application or mechanism. Integration implies data being shared between systems and a common look and feel suggesting a single application.

91. **Interface.** A mechanism whereby data can be exchanged between applications.

92. **Legacy record.** A record that is not covered by a records authority or a general records authority. These records can be in Archives or agency custody and can be of any age or any format.

93. **Lossless (image compression).** Image compression may be described as lossless and lossy. Lossless compression ensures that the uncompressed version is identical to the original—no information has been lost. The GIF file format incorporates a compression algorithm that is lossless for images that contain fewer than 256 colours; images with more colours are reproduced with a limited palette.

The JPEG format can, in theory, be configured to have varying degrees of loss, including a lossless option.

94. **Lossy (image compression).** Image compression may be described as lossless and lossy. Lossy compression results in some difference between the original and an uncompressed version. In general, lossy compression may produce a smaller file size. The JPEG format can, in theory, be configured to have varying degrees of loss, including a lossless option.

95. **Low value records.** Low value records only need to be retained for as long as they are in use, unless they are subject to an embargo or freeze. Once they have been superseded or are no longer required they can be destroyed under Normal Administrative Practice (NAP).

96. **Magnetic tape.** A plastic, paper or metal tape that is coated or impregnated with magnetisable iron oxide particles on which information is stored as a pattern of polarised spots. These are read using magnetic tape drives.

97. **Magneto-optical disk.** A disk that combines the use of magnetic and optical technologies. To record data, elements of the crystal structure of the substrate are aligned by using a laser to heat the element in the presence of an applied magnetic field. When the magnetic field is aligned one way, a ‘1’ is recorded; when the magnetic field is reversed, a ‘0’ is recorded. The data is read by reflecting a lower-intensity laser beam off the surface; the polarisation of the reflected light varies according to the crystal alignment of the element of the substrate.

98. **Maintain.** To retain and preserve records in identifiable recordkeeping systems over time in accordance with disposal decisions. Records that are required to be maintained should remain accessible, their integrity should be protected and, where necessary, they should meet the conditions or requirements identified in order to satisfy business needs, organisational accountability and community expectations. This may include the migration of records across successive systems and other preservation strategies.

99. **Metadata.** Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. Metadata is attached to records when they are created and added to as a result of different processes such as transfer, sentencing and disposal.

100. **Migration.** The act of moving records from one system to another while maintaining their authenticity, integrity, reliability and usability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another.

101. **Motion imagery.** Imagery:

- using sequential or continuous streams of images that enable observation of the dynamic behaviour of objects within a scene
- whose temporal rates, nominally expressed in frames per second, must be sufficient to characterise the dynamic behaviours being observed

- that includes metadata and nominally begins at frames rates of 1 Hz (1 frame per second) within a common field of regard
- that is platform based.

102. **Native format.** The format in which the record was created or in which the originating application stores records.

103. **Natural language.** Normal language that is flexible, variable and fluid. Natural language is the language of thought and conversation. It is the language used in free text titling.

104. **Normal administrative practice (NAP).** Normal Administrative Practice refers to business processes under which material of ephemeral value is destroyed when it is no longer required to support business goals. The Archives Act 1983 allows agencies to destroy material which does not constitute a record, or which is of no lasting value, through Normal Administrative Practices without reference to a Records Authority. The Normal Administrative Practice for low value records generated on Operations is documented in CJOPS Directive 64/12 *Information and Records Management for Operations*. Normal administrative practice is specific to the context of an individual agency.

105. **Off-site storage.** A general term describing location arrangements for records. The storage might be leased by the agency or held by a storage provider. The agency contracts the storage provider to care for the records on their behalf.

106. **Outsourced Service Provider.** An organisation or individual delivering specific services or supplies, usually against pre-defined milestones and deliverable requirements. The provider of the outsourced service is not subject to direct management by Defence.

107. **Physical record.** A record in hardcopy form, such as a folio, paper file, bound volume, photograph or artefact. Physical records must be managed by an approved recordkeeping system.

108. **Preservation.** The processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. Preservation encompasses environmental control, security, creation, storage, handling, and disaster planning for records in all formats, including digital records.

109. **Record.** A Defence record is any document or object, in any form, that contains information relating to Defence activity, and is created, captured, managed or stored by any Defence personnel or external service provider in order to provide evidence of that activity.

110. **Record type.** The definition of a record object that specifies particular management requirements, metadata attributes and forms of behaviour. Specific record types are deviations from the norm, which allow an organisation to meet regulatory requirements (such as privacy or data matching) for particular groups of records. The default record type in Defence is ‘Corporate record’. Other record types include Personnel records, Financial records, etc.

111. **Recordkeeping.** The making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes the creation of records in the course of business activity, the means to ensure the creation of adequate records, the design, establishment and operation of recordkeeping systems and the management of records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration).

112. **Recordkeeping metadata.** Structured or semi-structured information that enables the creation, management and use of records through time and across domains in compliance with relevant legislation. Recordkeeping metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them.

113. **Recordkeeping system.** A framework to capture, maintain and provide access to evidence of transactions over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include:

- both records practitioners and records users
- a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices
- policy statements, procedures manuals, user guidelines and other documents that are used to authorise and promulgate the policies, procedures and practices
- the records themselves
- specialised information and records systems used to control the records
- software, hardware, other equipment and stationery.

114. **Records authority.** A records authority is an instrument issued by the National Archives of Australia to give its approval to Australian Government agencies or other organisations or persons to keep, destroy or transfer Commonwealth records. Records authorities state which classes of records are to be retained as part of the archival resources of the Commonwealth. Records authorities that permit destruction generally specify the minimum length of time that Commonwealth records must be retained. Some authorities may include other conditions. General records authorities (GRAs), such as the Administrative Functions Disposal Authority (AFDA), apply to all Commonwealth institutions.

115. **Records management.** The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

116. **Repository.** A structured physical or digital space set aside for storing records and their associated metadata. Archival repositories are often constructed to meet specific standards designed to ensure the longevity of the records.

117. **Retain as national archives (RNA).** The disposal action for Commonwealth records appraised as having archival value. This means that the records should be transferred to the National Archives when they are no longer required for business use.

118. **Retention period.** The minimum length of time after the disposal trigger that a record must be maintained and accessible before the disposal action can be implemented.

119. **Review.** A disposal process where a folder or group of records is examined to consider the allocation of a disposal class or whether any disposal action can take place.

120. **Security controls.** A scheme of protective markings that may be allocated to users, digital records and files to restrict access in accordance with the *Australian Government Security Classification System* (AGSCS). It may include a hierarchical security category, possibly in conjunction with a non-hierarchical qualifier.

121. **Sentencing.** The process of identifying the disposal class a record belongs to and applying the disposal action specified in the relevant records authority. Sentencing is the implementation of decisions made during appraisal.

122. **Sentencing on creation.** The process of allocating a disposal class to a file as soon as it has been created. Sentencing on creation is more likely to occur with records in a digital recordkeeping system. Review dates may be added as a quality control measure.

123. **Software obsolescence.** Software being rendered obsolete because newer versions are not ‘backward compatible’ (able to read older versions of that software), and the software is no longer used and has been superseded by other software, or it cannot function with newer equipment or software.

124. **Source record.** A document or record that has been copied, converted or migrated or will be the input for such a process. A source record may be an original record or it may be a reproduction that was generated by an earlier copying, conversion or migration process.

125. **Storage.** A set of processes to ensure that records are protected, accessible and managed in a cost-effective manner for as long as they are needed. This includes facilitating retrieval and use.

126. **Storage facility.** Any building, equipment or system that houses records, including commercial storage facilities, in-house storage facilities and archival storage facilities.

127. **Structure.** The appearance and arrangement of a record’s content, eg the relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices.

128. **Structured data.** A record created from data that has been collated and managed in a structured environment, often in a database-type business information system. The captured data is highly-structured, predictive and repetitive.

129. **System administrator.** A user role with designated responsibility for configuring, monitoring and managing a system and its use. This role may exist at different levels of seniority and be associated with a variety of permissions to undertake system administration functions and some records management processes.

130. **Taxonomy.** The classification of entities in an ordered system that indicates natural relationships.

131. **Thesaurus.** A classification tool comprising an alphabetical presentation of a controlled list of terms linked together by semantic, hierarchical, associative or equivalence relationships. In a thesaurus, the meaning of a term is specified and relationships to other terms are shown. A thesaurus should provide sufficient entry points to allow users to navigate from non-preferred terms to preferred terms adopted by the organisation.

132. **Top numbering.** The practice of applying an additional file number (or other identifiers) to files when their control is transferred from one recordkeeping system to another, to bring them into line with the new control system.

133. **Transfer (of custody).** The transfer of custody of a Commonwealth record is subject to section 24 of the *Archives Act 1983*. It involves transferring the duty of care for the ongoing physical management of records from one custodian to another. Transfer also involves the imposition of intellectual control in preparation for transfer of custody. It does not include transfer of legal ownership or intellectual property rights over the record. This duty of care may include responsibility for the record's:

- the record's physical storage and protection
- making its existence known
- making it accessible
- preserving its authenticity
- protecting it from unauthorised access, theft or disposal
- accounting for its management.

134. **Transfer (of ownership).** The transfer of ownership of a Commonwealth record is subject to section 24 of the *Archives Act 1983*. It involves one party relinquishing physical, legal and, in certain instances, intellectual property rights over the record to another party.

135. **Transformation.** A digital migration in which there is an alteration to the content information (CI) of an archival information package (AIP), eg changing ASCII codes to UNICODE in a text document being preserved.

136. **Unauthorised destruction.** In the case of Commonwealth records, destruction that is not carried out in accordance with:

- a current records authority
- a valid NAP

- a legal requirement to destroy.

In addition, destruction may be unauthorised if it is done in spite of a disposal freeze or embargo, or without the consent of the Commonwealth institution to which the record belongs (in practice, the head of the institution or their delegates). Unauthorised destruction may place staff in breach of the Archives Act 1983, the Crimes Act 1914, the Public Service Act 1999, or the Defence Force Discipline Act 1982.

Similar factors apply to unauthorised disposal, transfer of custody or ownership, damage, alteration or addition of or to records.

137. **Uncontrolled record.** Records that have not been documented or brought under a system of control or arrangement. For example, documents on network or local drives are uncontrolled records.

138. **Unsentenced record.** A record for which a value has not been determined and which consequently, has not been sentenced using a current records authority.

139. **Unstructured data.** Data not managed in a structured database. The term refers to narrative and contextual data such as word-processed documents, emails, presentations and web pages. To be managed as a record, this data needs to be captured into a system with recordkeeping functionality.

140. **Useful records.** Useful records are those that enable Defence to perform more efficiently and effectively. The effective management of these records improves the quality, timeliness and transparency of decisions. Useful records usually have a temporary retention period of up to seven years and must be assessed prior to disposal. Useful records can only be disposed of using a Records Authority.

141. **Version control.** A process which allows a record’s data to be edited and revised while retaining the history of the changes. Version control functionality allows for older versions of the record to be recalled if necessary.

142. **Vital records.** Vital records are those that are essential to the operations of Defence or the achievement of its required outcomes, particularly in the event of disaster and the re-establishment of core business functions and activities. These records may be permanent or temporary, active or inactive, and originals or copies.

143. **Workflow.** The automation of a business process, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules. A participant may be a system user, business work group or software application.

ANNEX 1B

RECORDS MANAGEMENT POLICY MANUAL STRUCTURE AND RELEASE DATES

STRUCTURE

The *Records Management Policy Manual* (RECMAN) chapters have been structured to reflect the life-cycle of a record and provide guidance on the records management framework.

Chapter 2—Records Management Context describes the records management framework that Defence needs to operate in, providing an understanding of the Commonwealth policies and legislative frameworks that apply and of the external agencies responsible for administering these. It also outlines the records management environment within Defence mandating the Defence-wide records management systems and associated policies such as gaining access to the Defence records management system.

Chapter 3—Governance details the Defence approach to governance and compliance, discussing the corporate approaches to governance through compliance assurance, reporting and communication. This chapter also details the training and advice available to support Groups and Services in complying with this policy.

Chapter 4—Records Management provides policy on how to identify, describe and manage records throughout their life, including creation, capture, storage and disposal.

Table 1B.1: RELEASE DATES

The release dates for the RECMAN chapters are as follows:

CHAPTER(S)	RELEASE DATE	REVIEW DATE
1	May 2014	May 2019
2	December 2014	December 2019
3	December 2014	December 2019
4	December 2014	December 2019

CHAPTER 2

RECORDS MANAGEMENT CONTEXT

INTRODUCTION

2.1 Effective records management will support Defence in maintaining authoritative information that has integrity and is accessible, auditable, accurate, reliable, complete, and of high quality.

2.2 To implement a successful records management policy, it is important to understand the environment in which it operates. This includes understanding the administrative, legislative, regulatory, and operational context. There are also a number of significant internal and external influences which are applicable to the conduct of effective records management.

2.3 In accordance with guidance provided by the National Archives of Australia (NAA) and the Australian Government, Defence must actively manage its records management processes and practices to ensure delivery is compliant with policy. This chapter details Defence's records management context by considering the legislative and regulatory environment, as well as the historical and technical factors and stakeholders that affect Defence's records management requirements.

LEGISLATIVE CONTEXT

2.4 This policy enables Defence to operate in compliance with a broad range of Commonwealth legislation. The key Acts and their application to Defence are described in brief below. Additional information about supporting legislation is provided in Annex A.

Archives Act 1983

Under the *Archives Act 1983* (Archives Act), the NAA is responsible for overseeing Commonwealth recordkeeping, determining standards and providing advice to Commonwealth agencies.

2.5 The NAA administers access to all Commonwealth records in the Open Access period, including all Defence records. Before the NAA releases records for public access, NAA staff examine them to ensure the information does not fall into one of the exemption categories contained in the Archives Act. Where the records contain national security related material, the NAA may seek Defence advice on any enduring sensitivities that may require exemption under the Act. The NAA makes the final decision on exemptions.

2.6 Under the Archives Act, anyone has a right of access to Commonwealth government records that are in the Open Access period, including those held by Defence, unless the record contains information that falls into certain exemption categories defined in section 33 of the Act. Following amendments to the Act, the open access period for Commonwealth records begins after 20 years instead of the previous 30 years. The changes to the open access periods for Commonwealth records took effect from 01 January 2011 and will be phased in over a 10-year period, as outlined on the NAA website.

2.7 Sections 24 and 26 of the Archives Act outline the penalties which may be directed at any individual who engages in conduct that result in the transfer, alteration, damage or destruction of Commonwealth records including Defence records, except where done in accordance with the conditions identified in the Act (20 penalty units per offence, a penalty unit is $170 under s4AA of the *Crimes Act 1914*). Offences against these sections of the Act are strict liability offences.

2.8 The NAA develops Records Authorities (RAs), in cooperation with Australian Government agencies including Defence. Defence's RAs give Defence permission under the *Archives Act 1983*, for the destruction of the temporary records described after the minimum retention period has expired. Retention periods for these temporary records are based on: an assessment of business needs; broader organisational accountability requirements; and community expectations, and are approved by the National Archives of Australia on the basis of information provided by the agency.

Electronic Transactions Act 1999

2.9 The *Electronic Transactions Act 1999* (Electronic Transactions Act) facilitates digital enterprise by ensuring that electronic transactions are not invalidated because of their format. Defence conducts most of its business through the use of electronic transactions; this Act recognises these transactions and the importance of digital information to the future economic and social prosperity of Australia.

2.10 Sections 8-12 of the *Electronic Transactions Act* validate electronic communications for a range of transactions including the production, communication and retention of written documents and signatures.

Evidence Act 1995

2.11 The *Evidence Act 1995* defines what documents, including records, can be used as evidence in Australian courts. Defence records are evidence of organisational decisions and actions. These documented business and operational practices will be required to withstand scrutiny in the event that they are required to be produced as evidence in legal proceedings.

Freedom of Information Act 1982

2.12 The *Freedom of Information Act 1982* (FOI Act) gives individuals the legal right to access documents held by Australian Government ministers, departments and most agencies. The FOI Act.

- enhances the transparency of policy making, administrative decision making and government service delivery
- allows individuals to see what information government holds about them, and to seek correction of that information if they consider it wrong or misleading
- enables the community to be better informed so as to participate more effectively in the nation's democratic processes
- allows information gathered by the government at public expense to be made available more widely to the public.

2.1 The Department can refuse access to some documents, or parts of documents that are exempt. Exempt documents may include those relating to national security, documents containing material obtained in confidence and Cabinet documents, or other matters set out in the FOI Act.

2.2 The FOI Act also requires government agencies to publish specified information, under the Information Publication Scheme, about their structure and activities.

2.3 The Australian Signals Directorate (ASD), Defence Intelligence Organisation (DIO), and Australian Geospatial-Intelligence Organisation (AGO) are specifically exempt from the operation of the FOI Act. This exemption includes any document that has originated with, or has been received from, these agencies.

Privacy Act 1988

2.4 The *Privacy Act 1988* (Privacy Act), through the *Australian Privacy Principles* (APPs), regulates how Australian Government agencies and organisations (collectively known as APP entities) collect, deal with, maintain the integrity of, and provide access and correction to personal information. The rights to access and amend personal information under the Privacy Act are in addition to rights provided under the FOI Act.

2.5 For privacy purposes, 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; and whether the information or opinion is recorded in a material form or not'.

2.6 Photographs and other pictorial representations of a person are a type of record, and therefore all images showing identifiable people must be handled in accordance with this legislation.

2.7 The Defence Intelligence agencies, AGO, ASD and DIO, are specifically exempt from the operation of the Privacy Act. However, as a matter of policy, these agencies apply the Privacy Act to certain non-intelligence records.

2.8 In relation to records management, the APPs require that personal information that is not contained in a Commonwealth record, and that is not reasonably necessary for, or directly related to, one or more of Defence's functions or activities, must be destroyed as soon as practicable, but only if it is lawful and reasonable to do so.

STANDARDS

Australian and International

2.9 All Defence records must be managed in accordance with *Australian Standard (International Organisation for Standardisation) AS ISO 15489*. The NAA has endorsed this standard as the minimum standard for Commonwealth records management practices. The standard is supported by *ISO 26122: Work process analysis for recordkeeping* (formerly AS5090) and *AS 5044 AGLS Metadata Standard*.

2.10 All Defence records must comply with the metadata standards described in the *Australian Government Recordkeeping Metadata Standard 2.0 (AGRkMS)*. This standard is also compliant with the Australian Standards on Metadata for Records (AS ISO 23081). The Metadata Standard sets out the type of information that Defence should capture in a structured way to describe the identity, authenticity, content, structure, context and essential management requirements of records.

2.11 With the transition to digital information and recordkeeping, NAA has endorsed *ISO 16175 Functional requirements for records in electronic office environments*, to complement AS ISO 15489. ISO 16175 includes fundamental principles for the management of digital records, and provides guidelines and functional requirements for digital records management systems and records held within other business systems.

2.12 All physical Defence records must be stored in accordance with the *Standard for the Physical Storage of Commonwealth Records* disseminated by the NAA. This Standard represents a code of best practice for the storage of Defence records.

Defence

2.13 The *Defence Security Manual (DSM)* provides the appropriate controls for Defence to protect its information and assets, at home and overseas. The governance arrangements and core policies in the *Protective Security Policy Framework* describe the higher level protective security outcomes and identify mandatory requirements. Defence complies with the mandatory requirements and has core policies which cover Information Security and Physical Security.

2.14 Clear guidance on information and records management requirements whilst deployed to an area of operations or exercise is contained in Joint Operations Command CJOPS directives and instructions.

2.15 All Handheld Imagery, regardless of source, must be managed in compliance with all records management policy and standards as well as

- DEF(AUST) 7100 GEO Part A – Handheld Imagery Metadata
- DEF(AUST) 7100 GEO Part B – Handling Procedures for Defence Handheld Imagery.

2.16 All Motion Imagery, regardless of source, must be managed in compliance with all records management policy and standards as well as

- DEF(AUST) 7101 GEO Part A – Motion Imagery Handling Procedures
- DEF(AUST) 7101 GEO Part B – Motion Imagery Metadata.

2.17 Personal information that is ‘sensitive information’ attracts more stringent requirements in accordance with APP 6.2(a)(i). Due to the protected nature of clinical and diagnostic information, clinical images should be considered part of a member’s health record, and therefore should be treated with the same considerations of confidentiality, privacy and security as any other part of their Defence health record. Health records will be managed in accordance with Joint Health Command policy.

AUSTRALIAN GOVERNMENT DIGITAL TRANSITION POLICY

2.18 In 2011, the Australian Government, in conjunction with the NAA released the Commonwealth *Digital Transition Policy* which *'requires agencies to move to digital information and records management and away from paper-based records management.'* This means that the majority of Defence's records must be created, stored and managed digitally by 2017, and where practicable, paper records should also be digitised. This will provide a number of efficiency and other benefits including improved corporate governance and cost effective business processes.

2.19 Defence has identified a large number of paper records which could be digitised and stored electronically. This would improve the accessibility and searchability of records currently held in paper format, and significantly reduce existing paper stockholdings, reducing the management and maintenance effort required for ongoing use of these records.

DEFENCE CONTEXT

Historical

2.20 Australia has maintained military forces and records since Federation. Not long after Federation, the Australian Army and Commonwealth Naval Force were established. In 1911, the Government established the Royal Australian Navy and in 1912, the Australian Flying Corps was established. The services were not linked by a single chain of command, as they each reported to their own separate Minister and had separate administrative arrangements. This led to the creation of discrete records repositories, and for different establishments. In 1976, the Government made a strategic change and established the Australian Defence Force to place the services under a single headquarters. Over time, the degree of integration has increased and tri-service headquarters, logistics and training institutions have replaced many single-service establishments.

2.21 The introduction of computer-based information and records management in the 1990's has changed the way in which Defence creates and manages records. Prior to this period, the majority of Defence records were in physical format. The growth of Defence establishments has affected archival arrangements for physical records, resulting in some repositories becoming full or difficult to access. This has lead to outsourcing of records storage and the digitisation of physical records.

2.13 The transition to digital information creation has made it easier for anyone to create a record. A corresponding reduction in specialist records management roles and an immature understanding of Defence records management and access has generated a records management environment that is uncoordinated, unstructured, and not well understood. This policy will assist Defence to address these challenges by more clearly articulating records management roles and responsibilities, and providing clear principles that enable a flexible and pragmatic approach to achieving compliance across all Groups and Services.

Technical

2.14 In November 2009, *Objective* was endorsed by the Defence Committee as the mandatory enterprise document and records management system. *Objective* is available on both the Defence Restricted Network and Defence Secret Network, and by mid 2015 all Group and Service rollouts of the application will be complete. The AGO, ASD and DIO maintain separate recordkeeping systems on the Defence Top Secret Network.

ACCESS CONSIDERATIONS

2.15 **High Sensitivity** – In addition to the conduct of operations, Defence provides a critical capability to Government in the areas of military security, intelligence, cyber security, and information security. While intelligence information and product is created to service the needs of Defence, and other Commonwealth agencies, it may also be shared with allies and coalition partners. Much of this information is highly sensitive, and must be managed with due care for the security, access, and disposal requirements of those stakeholders.

2.16 **Public Interest** – Some Defence information is of direct interest to members of the public, the media, Defence industry, and a wide range of special interest groups. In managing its records, Defence must balance the need for maintaining operational and commercial security with the requirement for transparency and accountability to the Australian public.

2.17 **Defence Community** – Records management in Defence must meet the varied operational and business needs of the Australian Defence Force, civilian and contract staff by improving the accessibility of authoritative information. Records must be a trusted resource that has integrity and are accurate, auditable, reliable, complete and high quality, without being onerous.

Annex:
2A Additional Legislation Summaries

ANNEX 2A

ADDITIONAL LEGISLATION SUMMARIES

1. Additional legislative considerations of the Defence records management policy are provided below.

Australian Information Commissioner Act 2010

2. The *Australian Information Commissioner Act 2010* established the Office of the Australian Information Commissioner (OAIC). The Australian Government announced as part of the 2014–15 Budget that the Office of the OAIC will be disbanded from 31 December 2014. Until it is disbanded, the OAIC has three primary functions:

- privacy functions, conferred by the *Privacy Act 1988* (Privacy Act) and other laws
- freedom of information functions, in particular, oversight of the operation of the *Freedom of Information Act 1982* (FOI Act) and review of decisions made by agencies and ministers under that Act
- Government information policy functions.

3. The changes announced by Government mean that from 01 January 2015:

- the *Privacy Act 1988* will continue to be administered by the Privacy Commissioner and supporting staff from a new office based in Sydney
- freedom of information (FOI) policy advice, guidance and annual statistics will be administered by the Attorney-General's Department
- the right to external merits review of FOI decisions by government agencies and Ministers will be the responsibility of the Administrative Appeals Tribunal (AAT)
- complaints about FOI administration by government agencies will be referred to the Commonwealth Ombudsman
- unresolved FOI review applications and complaints before the OAIC will be transferred to the AAT and the Commonwealth Ombudsman.

Copyright Act 1968

4. All information (including imagery) captured on behalf of the Department of Defence is the property of the Commonwealth and copyright belongs to the Commonwealth. This includes copyright made in pursuance of employment, under the direction or control of the Commonwealth, or due to agreement between parties including the Commonwealth. Guidance on the application of copyright to Australian Government intellectual property is detailed in the Intellectual Property Manual, published by the Attorney-General's Department.

Crimes Act 1914

5. The *Crimes Act 1914* outlines crimes against the Commonwealth. Section 70 prohibits Commonwealth officers (which include public servants, members of the Defence Force, or anyone working for the Australian Government) from publishing or communicating facts, documents or information which they gain access to through their work unless they have permission to do so. Many Defence records contain sensitive information and the release of these records in an uncontrolled way could have major implications for the Commonwealth and Australia.

Criminal Code Act 1995

6. Part 10.7 of the *Criminal Code Act 1995* describes computer based crimes. According to Division 477 and 478 any unauthorised access, modification or impairment of data or access to data held on a computer or other telecommunications device is illegal. All Defence employees have an obligation to actively control access to Defence records.

Defence Act 1903

7. The Australian Defence Force's command arrangements are specified in the *Defence Act 1903* and subordinate legislation. This Act states that the Minister of Defence 'shall have the general control and administration of the Defence Force' and that the Chief of the Defence Force, the Secretary of the Department of Defence and the Chiefs of the three Services must act 'in accordance with any directions of the Minister'. The leaders of Defence are also responsible to the junior Ministers who are appointed to manage specific elements of the Defence portfolio. The Minister may also delegate his or her authority via a delegation instrument.

Defence Force Discipline Act 1982

8. The *Defence Force Discipline Act 1982* relates to the discipline of the Defence Force and related purposes. A relevant record under this Act means any part of a record that is kept by any means under a law of the Commonwealth and relates to a person's service as a member of the Defence Force. Defence Force records serve as evidence of the rights and obligations of individuals and document activities which may serve as admissible evidence in a court of law.

Intelligence Services Act 2001

9. The *Intelligence Services Act 2001* establishes the functions of Defence and Australian Signals Directorate. It also imposes limitations on the activities of these agencies.

Military Rehabilitation and Compensation Act 2004

10. The *Military Rehabilitation and Compensation Act 2004* details the basic rights and entitlements to compensation and rehabilitation for current and former members of the Australian Defence Force, as well as Cadets, Cadet Officers and Instructors who are injured in the course of their duties on or after 01 July 2004. The Act also provides compensation to the dependants of those members and former members who die or are severely injured or ill due to their service on or after 01 July 2004. Defence has an obligation to retain accurate records to ensure all Service personnel receive the appropriate entitlements under the Act.

Public Governance, Performance and Accountability Act 2013

11. The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) establishes a coherent system of governance and accountability across Commonwealth entities. In addition to establishing a performance framework across Commonwealth entities, the Act requires Defence to:

a. meet high standards of governance, performance and accountability

b. provide meaningful information to the Parliament and the public

c. use and manage public resources properly

d. work cooperatively with others to achieve common objectives.

12. To comply with this legislation, Defence has an obligation to manage its records effectively.

Public Service Act 1999

13. The *Public Service Act 1999* provides for the establishment and management of the Australian Public Service (APS), including the APS values, employment principles and code of conduct. These values include open accountability for actions, and responsiveness in providing frank, honest, comprehensive, accurate and timely advice and in implementing the Government's policies and programs. Defence has an obligation to hold staff accountable for their actions, and to ensure that records are honest, comprehensive, accurate and timely.

Safety, Rehabilitation and Compensation Act 2004

14. The *Safety, Rehabilitation and Compensation Act 2004* details the basic rights and entitlements to compensation and rehabilitation for all employees of the Commonwealth who are injured in the course of their duties. This Act is superseded by the *Military Rehabilitation and Compensation Act 2004* for members of the Australian Defence Forces who are injured on or after 01 July 2004. Defence has an obligation to retain accurate records to ensure all personnel receive the appropriate entitlements under the Act.

Veterans Entitlements Act 1986

15. The *Veterans Entitlements Act 1986* provides for the payment of pensions, allowances and medical treatment for qualifying veterans and their dependants. Defence has an obligation to retain accurate records to ensure all ex-Service personnel receive the appropriate entitlements under the Act.

Work Health and Safety Act 2011

16. The *Work Health and Safety Act 2011* (WHS Act) provides a framework to protect the health, safety and welfare of all workers in the workplace. It also protects the health and safety of all other people who might be affected by the work.

17. All workers and visitors to a workplace are protected by the Act. This includes employees, contractors, subcontractors, outworkers, apprentices and trainees, work experience students, volunteers and employers who perform work. The WHS Act also provides protection for the general public so that their health and safety is not placed at risk by work activities.

18. Records must be kept in relation to all WHS incidents, irrespective of whether an incident is notifiable to WorkCover.

CHAPTER 3

GOVERNANCE

Introduction

3.1 This chapter documents the governance arrangements for the management of records in Defence, including compliance monitoring and reporting, roles and responsibilities, training, and support.

COMPLIANCE

3.2 All Defence personnel must comply with RECMAN. External service providers must comply with RECMAN where compliance is a condition of their engagement.

3.3 Members of the Australian Defence Force (ADF) Cadets, including but not limited to Australian Army Cadets, Australian Navy Cadets and Australian Air Force Cadets, must comply with RECMAN.

3.4 Where an individual or Group does not operate in accordance with RECMAN, the National Archives of Australia (NAA) may apply its enforcement powers under the *Archives Act 1983*. Those powers include seeking various civil penalties. NAA has the power to pursue penalties against Defence and individuals.

Monitoring and reporting

3.5 Each year the Secretary of the Department of Defence submits a Certificate of Records Management Compliance to the Minister of Defence and the NAA. The Certificate focuses on Defence's compliance during the previous calendar year with the:

- *Archives Act 1983*
- Australian Standard (International Organisation for Standardisation) AS ISO 15489
- ISO 16175 - Functional requirements for records in electronic office environments
- SA/SNZ TR ISO 26122:2012: Work process analysis for recordkeeping
- AS 5044 AGLS Metadata Standard
- Australian Government Recordkeeping Metadata Standard 2.0 (AGRkMS).

3.6 The Certificate of Records Management Compliance includes details of all instances of non-compliance, detailing remedial measures that are being taken to improve compliance.

3.7 The Directorate of Records Management Policy (DRMP) coordinates Certificate of Records Management Compliance reports from the Records Stewards (Group Heads and Service Chiefs) into a single annual Certificate of Records Management Compliance for the Department.

3.8 The internal and external reporting requirements and process are provided on the Records Management website.

3.9 DRMP may perform a records management compliance audit at any time. Any work area wishing to perform an internal records management compliance audit may consult with DRMP for assistance and support.

GOVERNANCE FRAMEWORK

3.10 All Defence records are owned by the Department of Defence. Everyone has a responsibility for Defence records.

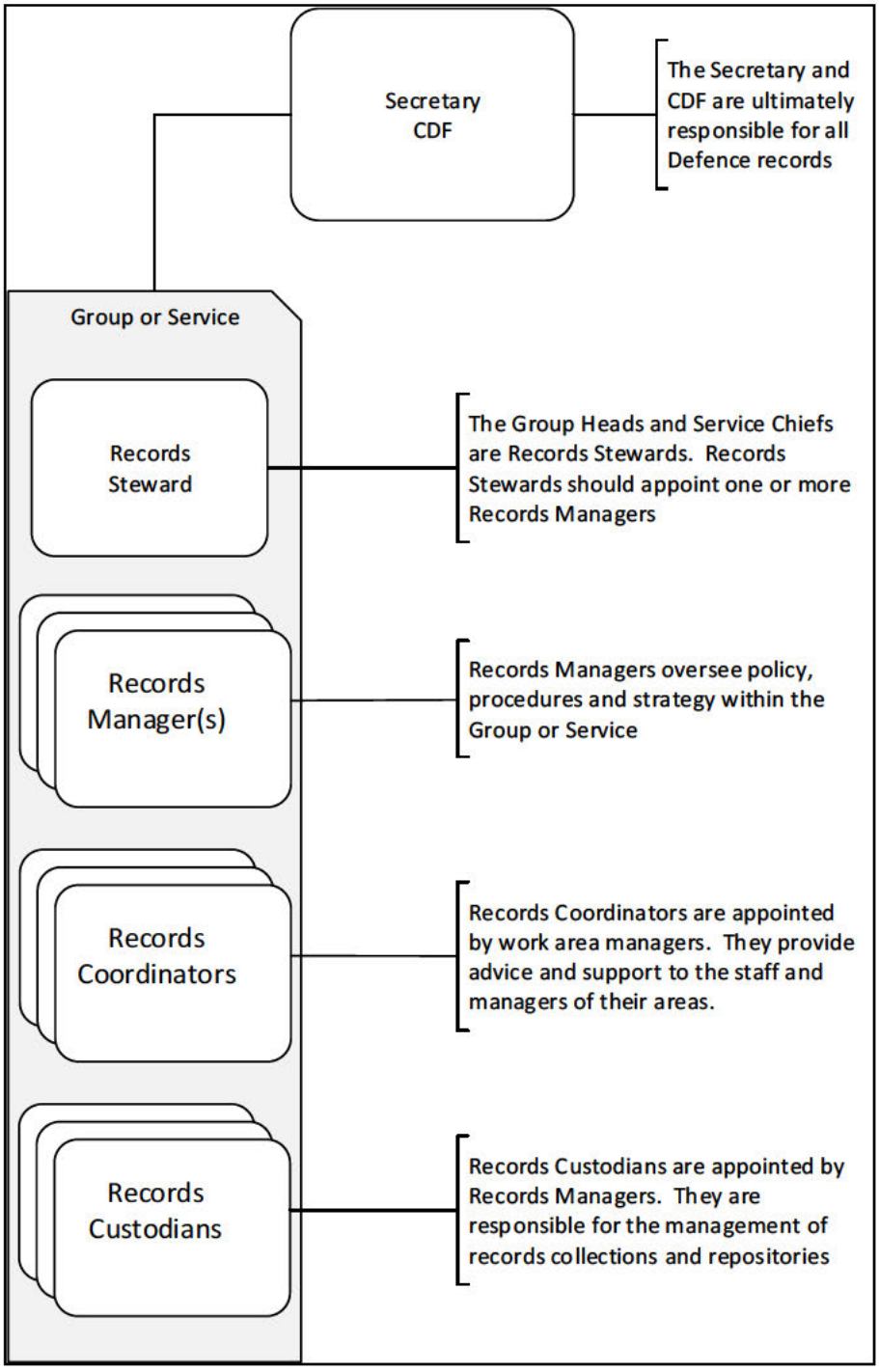


Figure 1: Records Management Governance Framework

3.11 The Secretary and the Chief of Defence Force are ultimately accountable for all Defence records.

Records Stewards

3.12 The Defence Records Stewards are the Group Heads and Service Chiefs.

3.13 The Surgeon General ADF is the Records Steward for the health records of all current serving members.

3.14 Records Stewards are accountable for ensuring that records management is adequately resourced and prioritised, and records are managed to a standard within their area of responsibility.

3.15 Records Stewards, or their delegates, should appoint and manage one or more Records Managers. The Records Steward should determine the position levels for personnel, and resources necessary to fulfil the Records Manager roles within their Group or Service. This will vary according to the complexity, sensitivity, and volume of records managed within the area.

Records Managers

3.16 Records Managers are responsible for:

a. Ensuring that all standards, policies, procedures and instructions within their Group/Service are consistent with, promote compliance with, and do not duplicate, Defence records management policy.

b. Providing the vital records strategy for their Group/Service.

c. Approving record and file title conventions for use across their Group/Service, promoting consistency across all Defence.

d. Determining which of their Group/Service's legacy record collections should be digitised.

3.17 Records Managers may conduct audits of records management performance within their Group and Service, either independently or on behalf of DRMP. This includes coordinating the Group or Service's response to the Records Management Certificate of Compliance audit.

3.18 The Records Managers for each Group are identified on the Records Management website.

3.19 Records Managers should appoint and manage Records Custodians. The Records Manager should determine the position levels for personnel, and resources necessary to fulfil the Records Custodian role(s) within their work area. This will vary according to the complexity, sensitivity, and volume of records managed within the area.

Records Coordinators

3.20 Work area managers should appoint Records Coordinators. Work area managers should determine the position levels for personnel, and resources necessary to fulfil the Records Coordinator role within their work area. This will vary according to the complexity, sensitivity, and volume of records managed within the area. It is the work area manager's responsibility to ensure that personnel assigned records coordination responsibilities complete relevant training.

3.21 Records Coordinators provide records management advice and support to the staff and managers of their work area. They are also responsible for:

a. Ensuring work area records are managed effectively and in accordance with Defence records management policy and relevant Group/Service specific instructions.

b. Ensuring work area staff have appropriate records management training.

c. Managing user authorisation for access and privileges in approved records management systems.

d. Drafting records management related Standard Operating Procedures, instructions and Standing Orders, as appropriate for activities unique to their local work area.

e. Managing the vital records strategy for their work area (if required).

f. Liaising with Records Managers and Custodians and the DRMP on behalf of the work area.

g. Search and discovery of records.

h. Executing sentences on the work area's records, with regard to the relevant records authorities, freezes, and embargoes.

i. Maintaining proper facilities for the storage and preservation of onsite physical records (*see* Chapter Four).

j. Managing the transfer of records into, and out of, the work area, ensuring procedures comply with classified document registration requirements.

Records Custodians

3.22 Records Custodians are responsible for the management of record collections and repositories in accordance with current records management policy and the standards, policies and procedures specified by the Records Manager, including:

a. Ensuring their repositories and systems are approved by DRMP and comply with the recordkeeping standards specified in this policy. Approval of records management systems is delegated to the Records Manager for each of the Intelligence Agencies (Defence Intelligence Organisation (DIO), Australian Signals Directorate (ASD), and Australian Geospatial-Intelligence Organisation (AGO)).

b. Ensuring maintenance of proper facilities for the storage and preservation of physical and digital records.

c. Controlling access to and transfer of physical and digital records into and out of their repositories and systems, managing compliance with classified document registration procedures where applicable.

3.23 Records Custodians include physical and digital repository managers and recordkeeping system administrators. Records Custodians provide a service, and do not have any decision making authority with regard to the records in their collections unless specifically granted it by a Records Manager.

3.24 Defence Support and Reform Group is the Records Custodian for all closed physical records (other than audio/visual material) held within Directorate Defence Archives repositories.

3.25 The Records Custodians for approved recordkeeping systems are registered on the Records Management website. Defence Intelligence Agencies (including AGO, ASD and DIO) will maintain a register of Records Custodians within their respective agencies.

All personnel

3.26 All Defence personnel, and external service providers, are responsible for creating, capturing, managing, using and appraising records as a part of their operational and administrative duties, in accordance with Chapter Four of this policy. External service providers are responsible for records management tasks where this has been documented in the conditions of their engagement.

Information Management Steering Committee

3.27 The Information Management Steering Committee (IMSC) is the high-level decision forum for improving information management (including records management) in Defence in line with the Information Management Strategy and Framework endorsed by the Defence Committee.

3.28 The functions of the IMSC are to:

a. Set the whole-of-Defence direction for information management (including records management) through:

   (1) defining strategic policies

   (2) establishing governance frameworks.

b. Determine information management priorities and drive implementation of information management initiatives, including allocation of funding and resources.

c. Resolve information management issues and risks on a whole-of-Defence basis.

d. Monitor performance against information management priorities.

e. Report to the Chief Operating Officer and Secretary and Chief of the Defence Force Advisory Committee on Information Management decisions.

Directorate of records management policy

3.29 DRMP is responsible for:

a. Developing and communicating records management policy.

b. Providing corporate records management procedures for all Defence records.

c. Promoting implementation of records management compliant policies and practices within Defence.

d. Managing Defence records management related specifications and standards (eg standards for contemporaneous and retrospective digitisation, digitisation metadata specifications, recordkeeping systems standards).

e. Approving and monitoring the compliance of recordkeeping systems and managing the register of approved recordkeeping systems for the Defence Restricted Network (DRN) and Defence Secret Network (DSN). This authority is delegated to the specified Records Manager for each of the Defence Intelligence Agencies (DIO, ASD, and AGO).

f. Managing the records management competency framework.

g. Providing policy input and advice to business units who are considering additional records management training programs.

h. Promulgating advice on freezes and embargoes on records destruction throughout Defence.

i. Writing and administering Records Authorities and participating in the revision of Commonwealth Records Authorities on behalf of Defence.

j. Reporting on Defence records management to external authorities, including collating Defence's response to the Senate Standing Order #12 (the 'Harradine Report') and responding to NAA Check-Up surveys.

k. Managing Control Records. Control records created by the Defence Intelligence Services (ASD, DIO and AGO) are managed by their parent agency.

l. Liaising with the NAA, including:

(1) Records management policy

(2) Revision or creation of Records Authorities

(3) Approving the transfer of sentenced records which are classed as Retain as National Archives to the NAA

(4) Approving the destruction of Commonwealth records and maintaining a portfolio of all Defence Control Records on behalf of the NAA. This authority is delegated to the specified Records Manager for each of the Defence Intelligence Agencies (AGO, ASD and DIO).

3.30 DRMP is the business owner of the primary recordkeeping systems on the DRN and DSN. The business owners of approved supplementary recordkeeping systems will be identified in the register of approved recordkeeping systems. The Intelligence Agencies (DIO, ASD, and AGO) maintain a separate register of approved systems within their own agencies.

TRAINING

Records Management Training and Support

3.31 Records Stewards are responsible for the records management competency of their personnel.

Records Management Competency Framework

3.32 DRMP is responsible for developing and maintaining the Defence Records Management Competency Framework. Defence records management training is designed by DRMP and the National Sentencing Team (NST).

3.33 Records Coordinators should ensure all personnel in their work area receive role appropriate training within three months of commencement, and refresher training as required.

All personnel

3.34 All Defence personnel and external service providers (for whom compliance is a condition of their engagement) should complete as a minimum:

- Responsible Recordkeeping (CAMPUS).

3.35 This course is a prerequisite for all other records management training.

3.36 All Defence personnel and external service providers who are granted access to an approved Defence records management system should complete training specific to the use of that system, appropriate to the access privileges assigned to them.

Recordkeeping system training

3.37 Design and delivery of training specific to individual recordkeeping systems is the responsibility of the Records Custodian for that system. Details are available on the Records Management website.

Records Custodians

3.38 There is no additional training required for Records Custodians beyond the minimum required for all personnel.

3.39 Defence personnel and external service providers who are assigned responsibility as Records Custodians will be invited to join the Defence Records Management Community of Practice (DRMCoP). Members will receive regular records management updates, have access to additional training, and receive invitations to records management events.

Records Coordinators

3.40 The Records Coordinator competency is obtained by successfully completing the following training, in addition to the minimum required of all Defence personnel:

- Records Coordination in Defence (CAMPUS)
- Sentencing Defence Records (CAMPUS).

3.41 DRMP recommends that Defence personnel complete the NAA course '*Practical Sentencing in a Digital Environment*' prior to commencing the CAMPUS 'Sentencing Defence Records' course where it is practical to do so.

3.42 Defence personnel who successfully obtain the 'Records Coordinator' competency will be invited to join the Defence Records Management Community of Practice (DRMCoP). Members will receive regular records management updates, have access to additional training, and receive invitations to records management events.

Deployed records coordinators

3.43 Deployed records coordinators face additional challenges and should receive additional training prior to deployment. The Deployed Records Coordinator competency is obtained by successfully completing the following training:

- Records Coordination in Defence (CAMPUS)
- Sentencing Defence Records (CAMPUS)
- Records Management on Operations (CAMPUS).

Records Managers

3.44 The Records Manager competency is obtained by successfully completing the following training:

- Records Management Strategy (classroom).

3.45 Details of course dates, locations and prerequisites are available on the Records Management website.

Records Stewards

3.46 Records Stewards may request a records management briefing from DRMP during normal business hours. DRMP can provide an on request executive support service to assist Records Stewards and their delegates in their records management decision making functions.

Senior executives

3.47 Senior executives may request records management training and support from DRMP during Canberra business hours.

SUPPORT

3.48 A wide range of supporting records management standards, templates, documents and information is available on the Records Management website.

Records Management advice

3.49 Records Management advice should be sought in writing in the first instance from DRMP.

CHAPTER 4

RECORDS MANAGEMENT

INTRODUCTION

4.1 This chapter defines a record in Defence and sets out the policy for how records should be managed.

DEFENCE RECORDS

4.2 A Defence record is any document or object, in any form, that contains information relating to Defence activity that is created, captured, managed or stored by any Defence personnel or external service provider in order to provide evidence of that activity.

4.3 Records are not restricted by format and include structured and semi-structured data, raw and processed data, documents, images, audio and visual digital media, handheld imagery and motion imagery, emails, web pages, social media posts, medical documentation and imagery, technical drawings and physical objects (such as art work and artefacts). The format and security classification of a record do not affect its value as a record, but do affect the handling procedures for the record.

4.4 Records constitute the ‘memory’ of Defence by documenting decisions, actions, events, policies and processes. As such, records strengthen current and future decision making capability, inform stakeholders, and support litigation and regulatory compliance. To achieve these outcomes, records must be created, managed, retained, accessible and appropriately preserved and/or destroyed.

4.5 Defence records include both core records that relate to Defence operational activities, and administrative records that relate to the administration of the Department.

Material which is not a record

4.6 A document or object is not a record if it does not relate to Defence activities, has no unique content or is only momentarily useful.

4.7 Documents or objects relating to Defence activity are not records if they are:

a. copies of blank forms, templates, or form letters

b. copies of material retained for convenience or reference purposes only

c. facilitative, transitory or short-term items

d. rough working papers

e. drafts not intended for further use or reference – whether in paper or electronic form –including documents that have minor edits for grammar and spelling and do not contain significant or substantial changes or annotations.

4.8 All materials subject to litigation, embargo or freeze must be managed as records (*see* Freezes and embargoes).

Personal documentation

4.9 Personal documentation is created by individuals for non-work purposes, rather than as part of their role as Defence personnel. Personal documents are not records and may be deleted as long as they do not contain evidence of Defence activity, or evidence which could be used in any legal action by, or against, Defence.

4.10 Personal documentation includes:

a. personal or conversational email

b. personal correspondence

c. personal photographs and videos

d. personal social media interactions.

4.11 Personal information that does constitute a record includes any information that:

a. Discusses or makes reference to a Defence activity

b. Provides evidence of allegations of abuse which can include but is not limited to: sexual and physical assault – including threats; harassment – including of a sexual nature; bullying, intimidation and other such unacceptable behaviour; discrimination; hazing or initiation; mismanagement of complaint handling; other criminal and non-criminal offences, which may result in personal physical or mental injury

c. Provides evidence of a breach of human rights legislation

d. Is relevant to an investigation or Commission of Inquiry

e. Provides evidence of unauthorised release of sensitive information.

Storage of non records

4.12 In accordance with Defence workplace agreements, some personal or other documents that are not Defence-related may be stored on the Defence Restricted Network (DRN) or Defence Secret Network (DSN) in accordance with the Defence Fair Use of Defence Resources policy.

4.13 All electronically stored media and all personal information created, processed, transmitted or stored on Defence assets is the property of the Commonwealth and is subject to Commonwealth legislation, regardless of whether or not it is a Defence record.

Access

4.14 All Defence records and all electronically stored material created, processed, transmitted or stored on Defence assets are subject to the access provisions of the *Archives Act 1983* (Archives Act) and the *Freedom of Information Act 1982* (FOI Act) and are subject to the *Evidence Act 1995* (Evidence Act). Records containing personal information are also subject to the *Privacy Act 1988* (Privacy Act). However, the Defence Intelligence agencies (Australian Geospatial-Intelligence Organisation, Australian Signals Directorate and Defence Intelligence Organisation) are specifically exempt from the operation of the FOI Act and the Privacy Act (*see* Chapter 2).

VALUE OF RECORDS

4.15 Records have value, and should be managed and retained according to that value.

4.16 When assessing the value of a record Defence personnel should consider the following contexts:

- **Operational –** Does the record support or directly relate to the command and control, planning, conducting, supporting, monitoring and evaluation of a campaign, operation or activity for the Defence of Australia and its national security?
- **Corporate Administration –** Does the record contribute directly to the administration of Defence personnel, support and logistics, health and welfare, capability and acquisition, science and technology, estate, facilities, infrastructure or the environment?
- **Financial –** Does the record relate to financial resources, budgets, accounting, assets management, fraud control, delegation powers and audits?
- **Legal –** Does the record relate to legal matters, claims, compensation, Military Police or the Provost Marshal?
- Historical – Is the record of historical significance?

4.17 Some records have very high value at certain points in their useful life, but very low value at other times. Some records have the potential to serve multiple purposes other than the purpose for which they were originally created or captured. Records should always be managed according to their greatest current or predicted future value.

4.18 A simple guide to evaluating the value of a record is to consider, ‘How serious would it be if this record went missing, was stolen, was disseminated to the wrong people, or was inadvertently or purposefully destroyed? How important would its recovery be if there was an accident or disaster that rendered it inaccessible?’

4.19 The security classification of a record is important to the management of the record, but does not have any direct impact on its value as a record, and may change over the life of the record.

4.20 All records must be appraised and disposed of using a Records Authority RA). The Defence Records Authorities are owned by the National Archives of Australia (NAA), but are managed by Directorate of Records Management Policy (DRMP) (*see* Chapter Three).

Business continuity records

4.21 **Business continuity records** are those that are essential to the operations and survival of Defence, particularly in the event of disaster and the re-establishment of core business functions and activities. These records may be permanent or temporary and originals or copies.

4.22 **Vital records** are those necessary to preserve:

- delegations of authority
- operational readiness
- operational policies and procedures
- Defence's financial position
- Defence's legal position
- evidence related to current or potential litigation
- the business interests of Defence
- the claims and rights of Defence personnel and stakeholders
- plans for infrastructure.

4.23 Business continuity records must be managed in accordance with both Defence records management policy and the *Continuity of Defence Operations policy*. Records Managers should determine whether a vital records strategy is required for their Group/Service.

CREATING AND CAPTURING RECORDS

4.24 Defence records must be managed in an approved recordkeeping system.

4.25 An approved recordkeeping system is an integrated suite of technology, processes and procedures that meets the Defence records management standards for the management of Defence records.

4.26 DRMP is the sole authority for the approval of Defence recordkeeping systems on the DRN and DSN. DRMP will manage a register of approved recordkeeping systems. This register will contain details of all approved recordkeeping systems in Defence, including the types of records approved for management in that system and the business owner of the system.

4.27 *Objective* is the primary recordkeeping system for Defence. However, it is often not the primary source for structured information stored in Defence's business and operational systems (eg personnel information is managed in PMKEYS). Some digital records are better managed for part or all of their life in a suitably configured and managed information system that meets recordkeeping standards or integrates with an approved recordkeeping system. Where this is the case, approval must be sought for registration of the primary source system as an approved recordkeeping system.

4.28 All approved recordkeeping systems must be compliant with *ISO 16175 - Functional requirements for records in electronic office environments*, and will be subject to compliance checks every two years. Records Custodians are responsible for ensuring that the systems they manage are configured and managed in such a way as to comply with ISO 16175 at all times. A checklist is available on the Records Management website to assist system owners in determining whether their system may be suitable for assessment and approval. ISO 16175 is endorsed by the NAA for use by Australian Government agencies. Compliance with ISO 16175 is usually dependent on specific installation, configuration, and ongoing management decisions.

4.29 DRMP has delegated their authority to approve Defence recordkeeping systems on the Defence Top Secret Network to the Records Manager of each Defence Intelligence agency. These systems are subject to this policy and must comply with the standards specified by DRMP. Each Defence Intelligence agency will maintain its own register of approved Defence recordkeeping systems, to the standard specified by DRMP.

4.30 Personnel should always create or capture records as close as possible to the relevant event, action or decision. The closer to an event that a record is created the greater its usefulness, reliability and evidentiary value.

4.31 Records are created and captured to support effective administration and operation, and as evidence of actions, events, decisions or decision making processes. The more important an action, event or decision, the greater the requirement to ensure accurate and comprehensive records are created and captured, to provide evidence of the decision making process.

4.32 All records should be managed in the context within which they are most meaningful. Some records have very low individual value, but much greater value within their business context.

4.33 All personnel are responsible for creating and capturing records.

Digital recordkeeping

4.34 Defence records must be created and managed in digital form unless it is not legal or practical to do so.

4.35 Digital records are records created, communicated and/or maintained by means of computer technology. They may be 'born digital' (first created in electronic format) or they may have been converted into digital form from their original format (eg scans of hardcopy documents).

4.36 Digital records include emails, word processed documents, spreadsheets, multimedia, web forms, websites and online transactions. Digital records can also be found in many systems throughout the Department including databases and business information systems.

4.37 It is Australian Government policy to use digital recordkeeping to improve accessibility and reduce costs. Digital recordkeeping means that the majority of Defence records must be created, stored and managed digitally. Where possible, incoming paper records should be scanned so that new paper files are not created. Standards for scanning documents are detailed in RECMAN Annex 4A. Optical character recognition is best practice and should be used for all documents containing text unless there is a specific business case against it.

4.38 Citizenship and migration documents are exempt from the *Electronic Transactions Act 1999,* which does not permit them to be created or managed in digital form.

Electronic Transactions

4.39 Electronic transactions enable individuals to quickly authorise and approve documents and/or perform transactions online that provide a legally binding record of an action or decision capable of being electronically retrieved. Common examples of this in Defence are emails, signals, PMKEYS, ROMAN, and the ‘review and approve’ and workflow functions available in Objective.

4.40 The *Electronic Transactions Act 1999* declares that ‘…a transaction is not invalid merely because it is carried out in one or more electronic communications’. Electronic transactions are legally binding so long as both parties consent to the electronic form. The following requirements imposed under a law of the Commonwealth can be met in electronic form:

a. to give information in writing

b. to provide a signature

c. to produce a document

d. to record information

e. to retain a document.

4.41 To be legally binding, an electronic transaction must be consented to by all involved parties and meet criteria for authenticity, reliability, usability and integrity.

4.42 The *Electronic Transactions Act 1999* applies to all laws of the Commonwealth unless they are specifically exempted by the *Electronic* Transactions *Regulations 2000.*

Electronic Signatures

4.43 An electronic signature is a method of producing an identifiable and authenticated signature or equivalent on an electronic document which indicates the provenance and intent of the signatory regarding the information contained within the document.

4.44 The deliberate act of typing a signature is considered evidence of an intention to authorise, but an automated signature block is not. Email headers are considered proof of the originator, but are not considered an electronic signature for this purpose.

Digital Signatures

4.45 Digital signatures use Public Key Infrastructure to provide assurances of the evidence of a transaction, the identity of the transaction participants and acknowledgement of approval by a signatory. Digital signatures should be used where additional authentication is required for a high risk transaction and for transactions with parties outside Defence. More information about digital signatures can be found on the Chief Information Officer Group website.

Describing records

4.46 Defence records must have a meaningful title, subject, or label, and must be registered on a file or stored in databases endorsed by DRMP as compliant with ISO16175.

4.47 A file may include any collection of related records, regardless of format. Files are required for the purpose of ensuring that records are managed in context-the value of a file is greater than the sum of the value of its records. Folders may be used within files to group information for the purpose of convenience. For example, a file about procurement of a new weapon system may include a folder containing the digital specifications, a folder for each series of test reports, and details of a physical prototype.

4.48 The title of a file should indicate the nature and purpose of the core business, activity, transaction or decision of the records collated in the file. Specific standards and agreed best practice conventions apply to the titles of some audio, imagery and scientific records. Records and file title guidance can be found on the Records Management website. Record and file title conventions are the responsibility of Records Managers.

4.49 Records are also described using metadata – ‘data about data’. Metadata is used to provide context and descriptive information about records over time ‘so that people know what the records are about, understand their context and purpose and can find them easily.’ Metadata includes information such as title, author and creation date.

4.50 The higher the value of the record being created, the more detail should be added to the metadata fields. A richer set of metadata makes a record easier to find, use, share, protect, classify and sentence.

4.51 All digital Defence records must comply with the metadata standards described in the *Australian Government Recordkeeping Metadata Standard 2.0 (AGRkMS)*.

4.52 Records captured through the digitisation of physical documents must comply with *Annex 4A – Scanning Standards* and the *Defence Digitisation Metadata Standards*.

4.53 Recordkeeping systems should automate the capture of metadata wherever possible. The *AGRkMS Implementation Guide* and ISO 16175 provide guidance on best practice in capturing metadata in business and recordkeeping systems.

4.54 Imagery records must comply with the metadata standards and handling procedures described in *Annex 4B – Defence Imagery Standards*.

Correspondence (including emails)

4.55 **Internal.** For correspondence originating within Defence, the author is responsible for storing the record in an approved records management system.

4.56 **External.** For correspondence originating outside Defence, the first Defence person (or external service provider to Defence) on the 'To' or 'Addressee' list is to capture the record.

4.57 Additional convenience copies of correspondence may be captured, but are not considered Defence records.

4.58 **Email.** Email records must include both the email body and any attachments. Where an email 'trail' is captured retrospectively, only the last email in the trail (containing all the previous emails in the conversation) should be captured. If another email thread is started containing only some of the initial email threads then the subsequent threads should also be captured even if there is some duplication of content..

4.59 Legal responsibility for retaining and archiving correspondence belongs with the originating organisation. However, where Defence receives correspondence from an external source that requires any Defence action or decision or is formal correspondence of thanks, congratulations or advice, this correspondence becomes a Defence record and responsibility for its management resides with the recipient of the correspondence.

RECORDS STORAGE

4.60 Defence records must be stored in a way that preserves their authenticity, reliability, discoverability, accessibility, quality, usability, and security for as long as needed.

4.61 Failing to maintain records in an accessible state may be deemed to be an act of destruction under s24(5) of the *Archives Act 1983* and may be an offence. The requirement for 'accessibility' in this context refers to the ability of authorized persons to retrieve the records, rather than to the records' compliance with standards for accessible content in accordance with the *Disability Discrimination Act 1992*.

Physical records storage

4.62 Physical files must be indexed in an approved digital recordkeeping system, and made accessible in accordance with the *Archives Act 1983*, *Freedom of Information Act 1982*, *Evidence Act 1995* and *Privacy Act 1988*.

4.63 General information on storing physical records can be accessed via the NAA website. This advice forms the minimum standard for preservation of physical records in Defence, including but not limited to paper documents and artworks, microfiche, gramophone discs, and magnetic media.

Digital records storage

4.64 Digital records must be stored in an approved recordkeeping system and accessible for access requests under the *Archives Act 1983* and *Freedom of Information Act 1982*. Records must not be stored on uncontrolled or unapproved systems which include email, personal or network drives.

4.65 How and where digital information is stored affects its viability over time. Digital records required for long-term retention (ie important, high value and RNA records), or identified as high risk, need particular care. When storing digital records, Records Custodians should:

a. **Store records in non-proprietary format.** Where possible, digital records stored for long periods should be stored in non-proprietary formats to protect them against changes to software that may prevent them from being read in the future. More information on suitable storage formats is available from the Records Management website.

b. **Actively manage systems.** Systems management strategies and standard operating procedures compliant with this policy should be approved by the Records Manager and used to ensure that systems are managed effectively over time.

c. **Backup regularly.** Digital storage devices deteriorate with time and use and may lose records without visible signs of damage. Records Custodians should maintain and replace storage media in line with manufacturer's recommendations.

d. **Conduct regular integrity checks.** Integrity checks are important to ensure that there has been no inadvertent change, deterioration or data loss. This should be a routine part of testing your business continuity plan.

e. **Store devices in appropriate conditions.** Magnetic and optical storage devices, including computer hard drives, tablets, thumb drives and optical or magnetic media and other peripheral computing hardware must be managed and maintained. The facilities housing them must appropriately protect the records and make them accessible. Digital storage devices are susceptible to dust and fluctuations in humidity, temperature and radiation, and it is important to ensure that stable environmental conditions are maintained.

f. **Refresh storage devices.** Computer hardware and digital storage media can become obsolete rapidly. Software changes may also require format conversion to ensure that information remains readable and accessible.

Custodians should continuously monitor digital records and refresh the media as needed, while maintaining the integrity of the records.

g. **Perform health checks.** When storage devices are replaced or upgraded, Custodians should check that all records that need to be refreshed or migrated are included. It is also an excellent opportunity to sentence records that are due for disposal in accordance with a relevant RA.

DIGITISING RECORDS

4.66 Some records originally created or captured in physical format are more effectively stored and managed in digital format. Defence is required to comply with the *Australian Government Digital Transition Policy,* under which physical records will be digitised wherever it is cost-effective to do so.

4.67 An NAA-approved set of minimum standards is available from DRMP for use when scanning paper documents into a records management system. All scanned paper records must meet these minimum specifications described in *Annex 4A – Scanning standards*.

4.68 After scanning and quality checking:

- electronic records must be managed in an approved recordkeeping system
- the new electronic records become the primary records and are subject to sentencing and disposal under relevant records authorities, either Australian Government Disposal Authorities (such as Administrative Function Disposal Authority (ADFA) Express) or Defence RAs
- the physical source records become copies which may be able to be destroyed (in accordance with General records authorities (GRA) 31 below).

Digitisation projects

4.69 A digitisation project (also known as ‘retrospective scanning’) is used to digitise a large collection of existing physical records, or files. All digitisation projects must register their project with DRMP before commencing scanning in order to ensure that records are being digitised in accordance with government legislation and the *Defence Digitisation Metadata Standards* for scanned paper documents. Failure either to register a digitisation project, or submit a subsequent business case to DRMP may result in non-compliance with the Australian Government Digital Transition Policy or a more serious breach of the *Archives Act 1983*. The digitisation business case template can be obtained from the Records Management website.

4.70 It is possible for business areas to apply to the DRMP for an exemption from complying with the normal technical digitisation specifications; this exemption will only be accorded in exceptional circumstances, and will be subject to strict conditions.

Destroying original documents after digitisation

4.71 General Records Authority 31 (GRA 31) is the legal instrument which authorises the disposal of source records, following successful copying, conversion or migration, in accordance with the *Archives Act 1983*[1]. Specifically, GRA 31 authorises the destruction of all agency records created on, or after, 01 January 1995 and all non-RNA records created before 1995, subject to some exclusions and conditions.

4.72 Defence may not destroy original source records after copying, conversion or migration if:

- the record is identified as RNA or Retain Permanently and is pre-1995 (these records must be transferred to NAA in original format)
- there is a legal requirement to retain the record in its original format or a specific format
- there is a government policy, Executive Directive, NAA disposal freeze or Defence imposed embargo to not destroy the record
- the record may be required as evidence in a current judicial proceeding or a future judicial proceeding that will be commenced, or will likely be commenced
- the record is subject to a current application for access under the *Freedom of Information Act 1982*, *Archives Act 1983* or other legislation
- NAA has issued a notice that specifically requires retention of the record in its original format or a specific format
- the record is on loan from the care of NAA.

4.73 Establishing the authenticity and reliability of a digital record may depend on the accuracy of the digitisation process, the system used to produce the record, the source of the information in the record, the method of its preparation, and the controls used to manage the record (including metadata about the record).

4.74 Defence must be able to ensure that business practices, records management systems and digitisation processes can stand up to the scrutiny of the courts, parliament, the Ombudsman and relevant auditors.

RECORDS DISPOSAL – KEEP, DESTROY OR TRANSFER?

4.75 Defence records must be retained, preserved and accessible for as long as they are legally required. They may be retained for a longer period if they are useful and do not contain personal information which must be destroyed or de-identified in accordance with the *Privacy Act 1988*.

[1] Section 24(2)(b) of the *Archives Act 1983*

Sentencing

4.76 Sentencing is the process of examining the information contained on a file to determine the value of the decision or activity that has been documented, and using a Defence specific Records Authority, or a Commonwealth GRA to decide whether to retain, destroy or transfer the file. The disposal of records after sentencing is authorised by the *Archives Act 1983*.

4.77 Records within a file must be sentenced together, and the file must be retained in accordance with the highest value record within the file.

4.78 Records Coordinators are responsible for sentencing and disposal of their records. Sentencing training and advice is available from the National Sentencing Team.

4.79 Guidance on information and records management requirements whilst deployed to an area of operations or exercise is contained in Joint Operations Command CJOPS directives and instructions. These directives must be utilised in the all operational and exercise phases, including conduct in the areas of operations by all personnel with no exceptions. The directives include responsibilities for the repatriation of records.

Normal Administrative Practice (NAP)

4.80 The Normal Administrative Practice (NAP) provision of the Archives Act gives Defence permission to destroy certain material without formal authorisation from the NAA. NAP is to be used as a legal tool to assist in identifying material which may be destroyed without sentencing, and without creation of a control record.

4.81 NAP may be used to destroy any material that is not a record (*see* paragraphs 0 and 4.7).

4.82 NAP may be used to destroy cancelled files that have been created in error and that have never had records placed on them. These files may contain materials that are not records, such as blank templates or convenience copies.

4.83 NAP must not be used to destroy records that have mandatory retention periods under a Records Authority.

4.84 NAP must not be used for documents covered by disposal freezes, Defence disposal embargoes or other potentially significant records such as evidence of harassment, breach of Human Rights legislation, or those relevant to an investigation or Commission of Inquiry.

4.85 NAP must not be used to destroy a closed file that contains records. Closed files must be disposed of in accordance with a disposal authority.

4.86 There is a specific NAP Policy in place for use on Operations. This has been reviewed by the NAA and can be found in Annex A of *CJOPS Directive 64/12 Information and Records Management on Operations*.

Records Authorities

4.87 A Records Authority is a legal instrument issued by the NAA, which outlines the mandatory requirements of Australian Government agencies for retaining, transferring or disposing of records. These Authorities contain information about the classes of records that must be retained, how long they must be retained, and other conditions.

4.88 Records Authorities usually apply to the records of a single agency while General Records Authorities generally apply to all Australian Government agencies.

4.89 Defence uses both General Records Authorities and Defence Records Authorities for retention and disposal of all records. Where a given record falls within the scope of both a General Records Authority and a Defence Records Authority, it must be managed in accordance with whichever Authority sets the longer retention period.

Administrative Function Disposal Authority (AFDA) and AFDA Express

4.90 AFDA and AFDA Express are general records authorities that cover common administrative functions performed by most Australian Government agencies. However, they do not cover Defence core business records, or records which document the Defence military combat function or the management of Defence military personnel, and must not be used to sentence these records.

4.91 **General Records Authorities:** are used for functions common to all or most government agencies. For example, GRA 31 is used to dispose of records after digitisation and GRA 25 provides requirements for recordkeeping when functions and activities are outsourced to contractors. Other commonly used GRAs are AFDA Express and GRA 21 – Intelligence. GRAs are written by the NAA in consultation with all Australian Government agencies.

4.92 **Defence Records Authorities:** are used for functions specific to the core business of Defence. These RAs are prepared by DRMP in consultation with business areas and the NAA using templates and guidelines provided by the NAA. RAs are assessed and validated by NAA before being authorised and issued by the Director-General of the NAA under Section 24(2)(b) of the Archives Act. Defence RAs can only be developed or modified by DRMP and must be authorised by the NAA. Information about extant and proposed Defence RAs is available on the Records Management website.

Control records

4.93 Control records contain metadata about files that have been sentenced. All sentenced files must be recorded on a control record to document the disposal process prior to execution of the sentence (retain, destroy or transfer). Control records for the destruction of electronic records should be automatically generated and maintained by the approved recordkeeping system used to store and destroy the records (eg Objective). Control records describing the destruction of physical records must be manually created and maintained by the sentencing business unit, and provided to DRMP. This replaces the requirement to notify the NAA, or use a Notification of Records Destroyed (NAS 45) form. DRMP is responsible for keeping a copy of all Defence control records, and reporting destroyed records to NAA.

4.94 Control records are classified RNA, and must contain the following details as a minimum:

a. file number/unique id

b. classification eg unclassified, confidential etc

c. file title/object label

d. content to (open date) and content from (closed date)

e. disposal authority and class

f. status eg Destroy, Destroy Later, or Retain as RNA

g. destruction year if required.

4.95 The *Control Record template* is available from the Records Management website.

Freezes and embargoes

4.96 A records disposal freeze suspends the destruction of all relevant records held by Defence or other agencies that relate to a nominated prominent or controversial issue, event, or judicial proceeding. Records disposal freezes are usually issued by the NAA.

4.97 Records that are subject to a disposal freeze can be sentenced but cannot be changed, destroyed or transferred until the NAA either lifts the freeze or issues new instructions on disposal actions.

4.98 A Defence records embargo is a Defence imposed ban on the disposal of particular subject matter records or information due to impending policy changes, litigation (including court-issued discovery orders), public controversy or community interest. Embargoes must be requested by the relevant Records Manager. Embargoes, like freezes, halt any disposal action until the embargo is lifted.

4.99 All current records disposal freezes and embargoes are clearly indicated on the Records Management website.

TRANSFER OF RESPONSIBILITY

4.100 Every Defence record must have a Records Steward. Active records must have a Records Coordinator.

Resignation or transfer

4.101 On resignation or transfer from a business area or unit, all personnel must transfer all physical and electronic records under their control to either the person who will be assuming their duties or the unit Records Coordinator. They must ensure that the person assuming their duties, and/or the Records Coordinator, has full access to all physical and electronic records under their control. Their existing records access permissions must then be cancelled, or revised to reflect their new role.

Transfer of function

4.102 When a function is transferred to a new unit or work area, access to all records pertaining to that function should be transferred to the new Records Coordinator by their current Records Coordinator.

Cessation of function

4.103 On cessation of a function, all affected personnel must ensure that all outstanding electronic records are filed and closed and sentenced in an approved recordkeeping system. All physical files must be digitised or transferred to an appropriate repository with their control records. The Records Coordinator is responsible for ensuring sentencing is carried out and that control records are created.

Transfer of records between agencies

4.104 Records may be transferred between Defence and other Australian Government agencies as a result of a transfer of function, and in accordance with the Archives Act. Where this happens, the agency transferring the records must provide a list of all records supplied, and any records that may be held by the NAA or external service providers. Details of the records received or despatched must be updated in the relevant EDRMS within Defence.

Lost records

4.105 Lost records are records that have been accidentally destroyed or that are no longer accessible or recoverable. All lost records must be reported to their Records Coordinator and Records Manager. Lost records must also be reported to DRMP as lost records are required to be reported to NAA.

Discovered records

4.106 Discovered records are those that are found, but whose existence or location was not previously known to their Records Coordinator and/or Steward. Discovered records include any records not registered in an approved recordkeeping system (eg documents stored on C:, G: or P: drives). Upon discovery, records should immediately be captured in an approved recordkeeping system and reported to the unit Records Coordinator and DRMP so that control records can be updated and an update provided to NAA if required.

Abandoned records

4.107 Abandoned records are those records that are not being actively managed as the owner or unit responsible for their day-to-day management is no longer active. Abandoned records should be reported to their Records Manager for allocation to a new Records Coordinator, and DRMP so that control records can be managed and NAA notified if required.

Annexes:

4A Annex 4A – Minimum technical scanning specifications
4B Annex 4B – Defence Imagery Standards

ANNEX 4A

MINIMUM TECHNICAL SCANNING SPECIFICATIONS

1. These minimum specifications are required for all post-1995 records and pre-1995 temporary records.

2. Destruction of physical records that have been digitised may only be performed in accordance with General Records Authority 31 (GRA 31). Records excluded by GRA 31 must not be destroyed, even after digitisation. Pre-1995 source records which are Retain National Archives or Retain Permanently in agency must not be destroyed.

3. The NAA recommends use of the highest specifications that are practical and possible when digitising.

4. Optical character recognition (OCR) is best practice and should be used for all documents containing text unless there is a specific business case against it. OCR must be used where records are to be accessible in accordance with the requirements of the *Disability Discrimination Act 1992*. The OCR rendition of a record should be captured and managed in addition to, but not instead of the scanned images.

Table 4A.1: Records types and standards

Record Type	Standard		Quality Check
For clean, high contrast documents with text or graphics, for which colour is either not present or not essential, and for any images that are line art, Defence must produce images conforming to these specifications or higher. Generally this specification for documents may be used unless any of the following conditions apply: The document contains colour information that must be retained to preserve the meaning; The document has a low contrast (eg faded text, browning paper, or coloured paper); or The document includes photographs, is a photograph or a negative. **Please Note:** documents with coloured letterheads, wet signatures (unless they have	Format	JPEG 2000, PDF/A, TIFF	Testing of the images to ensure that the minimum requirements listed in these technical specifications have been met.
	Multi page format	PDF/A	
	Resolution	300 dpi	
	Scanning ratio	100%	
	Type of image	greyscale	
	Bit-depth	8 bit	
	Compression	lossy	
	Searchability	OCR Recommended	

Record Type	Standard		Quality Check
intrinsic value) and documents containing 'penned' notes in margins do not constitute the requirement to scan in colour unless the business area deems this necessary.			
For documents where colour is present and is important, or for documents with low contrast (eg faded text, coloured background) or for graphics, technical drawings and maps, Defence should produce images conforming to the following specifications or higher:	Format	JPEG 2000, PDF/A, TIFF	Testing of the images to ensure that the minimum requirements listed in these technical specifications have been met.
	Multi page format	PDF/A	
	Resolution	300 dpi	
	Scanning ratio	100%	
	Type of image	colour	
	Bit-depth	24 bits RGB	
	Colour management	embedded ICC colour profile	
	Compression	lossy	
	Searchability	OCR Recommended	

Notes:

(a) ISO PDF/A is defined in ISO 19005-1:2004. It is a constrained version of PDF Reference 1.4 with various proprietary fonts and formats removed. It provides a mechanism for representing electronic documents in a manner that preserves their visual appearance over time, independent of the tools and systems used for creating, storing or rendering of the files (ISO 19005-1:2004). It is commercially available in Adobe 8 and above. ISO 19005-2 was issued in 2011 and addresses newer features. It is considered appropriate as a standard for use in this context.

5. Defence has a scanning metadata capture specification which meets metadata requirements regarding process and methodology for records used in evidence. If scanning directly into Objective the metadata will be automatically captured, and tested using the Objective Desktop Scanning Tool. If scanning into a database or different medium, the metadata capture specification that must be used can be obtained from Directorate of Records Management Policy. Chief Information Officer Group is responsible for managing the additional metadata script required for all digitisation projects on the Defence Restricted Network and Defence Secret Network.

6. All digitisation projects involving Handheld Imagery must be done in consultation with the Intelligence and Security Group which holds and maintains all HHI policy and metadata requirements in accordance with legislation and whole of government standards. *See* Annex 4B – Defence Imagery Standards.

ANNEX 4B

DEFENCE IMAGERY STANDARDS

1. Once collected, imagery has the potential to serve many purposes other than the original purpose for which it was collected. To ensure that all Defence imagery maintains the highest possible value it must be controlled by standardised handling procedures and tagged with appropriate metadata.

HANDHELD IMAGERY

2. Hand Held Imagery (HHI) is imagery derived from image capture/recording devices carried on and operated by personnel. It is a key product capability for Defence and serves intelligence, operational, training, evidentiary and public affairs requirements. Defence collects, stores, protects, utilises, retrieves, shares, disseminates and, when legally appropriate, can dispose of HHI. These processes require a coordinated method of standardising metadata and ensuring that recordkeeping requirements are put into practice.

Handheld Imagery Standards

3. Guidance for the management of Defence HHI, including legacy HHI, is found in DEF(AUST) GEO 7100. It comprises two parts: PART A defines the metadata standards for HHI and PART B describes the handling procedures for HHI.

Handheld Imagery Metadata

4. DEF(AUST) GEO 7100 PART A defines the metadata standard for HHI. This metadata provides information relating to specific attributes of the image. The creator or originator of the image is responsible for capturing the specific metadata attributes.

5. The Defence HHI metadata schema defines specific metadata requirements, which provide precise information relating to imagery attributes such as subject description, security classification, image location, originator details and creation date. Capturing metadata related to an image is achieved through the use of an image log or Defence approved Digital Asset Management software such as Fotostation. The elements which provide the basis of the Defence HHI metadata schema are internationally defined through the International Press Telecommunication Council's IPTC standard, Adobe's XMP specification, ISO 15836:2009 Dublin Core metadata element set and JIETA's EXIF specification.

Handheld Imagery Handling Procedures

6. The Handling Procedures for HHI found in DEF(AUST) GEO 7100 PART B are based on the concept of three types of Imagery and are managed according to three separate workflows. They are:

- **Type One Imagery** (Evidentiary) – the purpose of imagery collection at the time of capture, is to record potential evidence by a visual medium.

- **Type Two Imagery** (Imagery with value) - includes daily Defence business activities such as (but not limited to) operational deployments, training

exercises, intelligence collection, public affairs, estate management, assets identification and defect photography.

- **Type Three Imagery** – (Specialist/Ephemeral) - Acquired for specific purposes, within a defined environment, by a small team. This imagery usually has limited use and a short expiry date. *Type Three imagery is not for dissemination beyond its initial creation environment. If dissemination is required, the imagery is to be managed as Type Two with metadata applied. Type Three HHI assessed as having no value may be disposed of under the provision of Normal Administrative Practice when it is no longer required.*

Handheld Imagery Management Systems

7. DEPSEC I&S is accountable for the standards and specifications used to administer HHI. Business areas that create HHI are responsible for the management of the HHI in accordance with Defence Standard DEF(AUST) GEO 7100. Business areas are also responsible for correct storage and archive of HHI into an approved records management system with the exception of:

a. HHI captured for intelligence or operational purposes is to be sent to Australian Geospatial-Intelligence Organisation HHI Manager s47E(d)

b. HHI captured for public affairs purposes is to be sent to Corporate Communication Branch, Multimedia Directorate s47E(d)

8. To facilitate correct management of HHI, all asset management databases must be able to implement appropriate imagery management in accordance with the prescribed metadata standards and handling procedures in DEF(AUST) GEO 7100 and be able to satisfy one of the following criteria:

a. ability to comply with *ISO 16175 Functional requirements for records in electronic office environments*

b. ability to integrate with an approved recordkeeping system to facilitate compliant recordkeeping.

9. Where there is no capability to have a recordkeeping metadata schema that allows for sentencing under the *Archives Act 1983* or the ability to integrate with one, the database must be catalogued in an approved recordkeeping system. In addition to standard recordkeeping data, the catalogue entry for the HHI file must contain, as a minimum, metadata regarding the location, custodianship and accessibility of the HHI and a synopsis of the types of HHI the file contains.

MOTION IMAGERY

10. Motion Imagery (MI) is imagery utilising sequential or continuous streams of images that enable observation of the dynamic behaviour of objects within the scene. It is a key product capability for Defence and serves intelligence, operational, training, evidentiary and public affairs requirements. Defence collects, stores, protects, utilises, retrieves, shares, disseminates and when legally appropriate can

dispose of MI. These processes require a coordinated method of standardising metadata and ensuring that recordkeeping requirements are put into practice.

Motion Imagery Standards

11. Guidance for the management of Defence MI, including legacy MI, is found in DEF(AUST) GEO 7101. It comprises two parts: PART A describes the handling procedures for MI and PART B defines the metadata standards for MI.

Motion Imagery Handling Procedures

12. Handling procedures guidance for Defence MI found in DEF(AUST) GEO 7101 PART A falls into two (2) main categories:

a. General Guidance - handling procedures applicable to all MI records, including requirements for naming conventions, storage, time zone and location information.

b. Specific Guidance - handling procedures applicable to a specific MI record including details of MI format, type, category and components.

13. The standard covers the MI records obtained from the following types of sensors:

a. Moving sensor, moving Field of View (FOV):

(1) Integrated systems - for example a sensor or system attached to an unmanned aerial vehicle/system, land vehicle and fixed or rotary wing aircraft. These systems are usually fitted with sensors to track sensor and platform orientation, and other information feeds required to comply with this guidance.

b. Fixed sensor, fixed FOV

(1) For example a Closed Circuit Television (CCTV) camera fixed to or within a building, or a remotely placed fixed camera with no pan, tilt or zoom and.

c. Fixed sensor, moving FOV

(1) CCTV, or remotely placed fixed camera with a pan, tilt or zoom function.

14. The Handling Procedures for MI are based on the concept of four (4) types of Imagery and are managed according to separate workflows. They are:

- **Type One Imagery** (Evidentiary) – the purpose of imagery collection at the time of capture, is to record potential evidence in a visual medium.
- **Type Two Imagery** (Imagery with value) – includes daily Defence business activities such as (but not limited to) operational deployments, training exercises, intelligence collection, public relations, and estate management.
- **Type Three Imagery** (Scientific/Research Purposes) – MI for the purpose of research and development conducted by the Defence Science and Technology Organisation.

- **Type Four Imagery** (Specialist/Ephemeral) – Acquired for specific purposes within a defined environment by a small team. This imagery usually has limited use and a short expiry date. *Type Four imagery is not for dissemination in any form beyond its initial creation environment. If dissemination is required the imagery is to be managed as Type Two or Type Three MI.*

Motion Imagery Metadata

15. DEF(AUST) GEO 7101 PART B defines all elements that collectively enable MI to be discovered, shared and managed throughout Defence. The standard should be used when acquiring new MI systems to ensure that they can comply with the information needs of Defence.

16. All sensor platforms capturing MI are to record accurate metadata. Where available, metadata elements should be automatically populated as part of the collection process, but may include elements generated in post processing. The method of metadata capture is dependent on the category of the MI. These categories are described in DEF(AUST) GEO 7101 PART B. PART B also lists the 32 Defence MI Core Metadata elements which, as a minimum, must be recorded.

Motion Imagery Management Systems

17. DEPSEC I&S is accountable for the standards and specifications used to administer MI. Until a whole of Defence MI repository is operational, all business areas and parent organisations having one or more collecting functions remain responsible for the centralised management and storage of all MI records they capture in accordance with the guidance in DEF(AUST) GEO 7101.

18. To facilitate correct management all MI, all asset management databases must be able to implement appropriate imagery management in accordance with the prescribed metadata standards and handling procedures in DEF(AUST) GEO 7101 and be able to satisfy one of the following criteria:

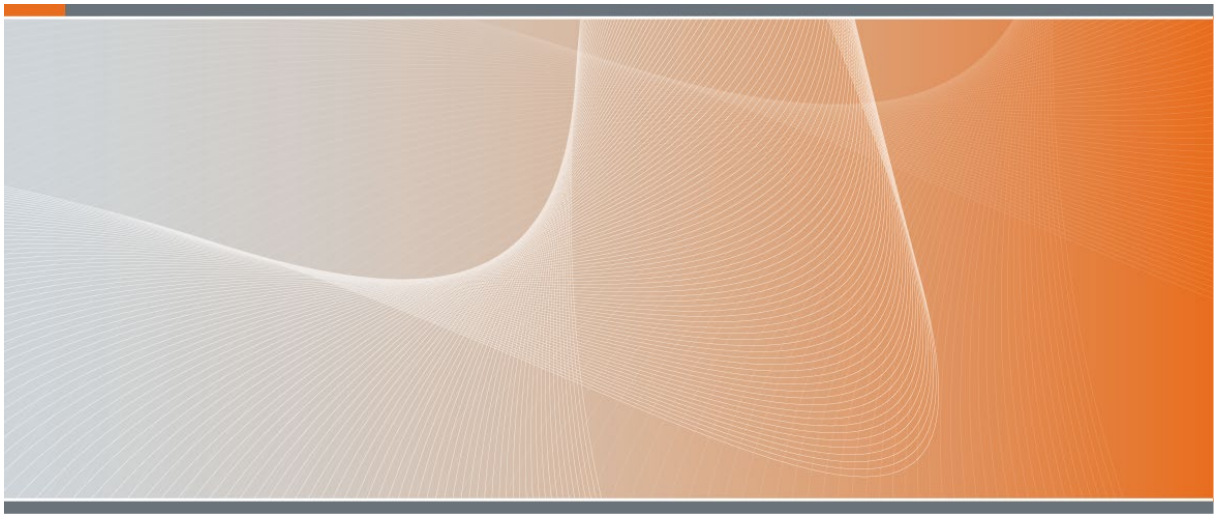
a. ability to comply with *ISO 16175 Functional requirements for records in electronic office environments*

b. ability to integrate with an approved recordkeeping system to facilitate compliant recordkeeping.

19. Where there is no capability to have a recordkeeping metadata schema that allows for sentencing under the *Archives Act 1983* or the ability to integrate with one, the database must be manually catalogued in an approved recordkeeping system. In addition to standard recordkeeping data, the catalogue entry for the MI file must contain, as a minimum, metadata regarding the location, custodianship and accessibility of the MI and a synopsis of the types of MI the file contains.

Australian Government
Department of Defence

DEFENCE RECORDS MANAGEMENT POLICY



s22

Dr Tom Clarke
First Assistant Secretary Enterprise
Transformation and Governance

Department of Defence
CANBERRA ACT 2600

22 December 2021

DEFENCE RECORDS MANAGEMENT POLICY

Issued by:	The Records Management Policy (RMP) has been issued by the First Assistant Secretary Enterprise Transformation and Governance with the authority of the Associate Secretary.
Purpose:	The RMP describes the agreed approach for achieving compliance with legislation and whole of government policy. The Department of Defence (Defence) generates an enormous quantity of key decisions and business activities. Defence is required, by law, to create and maintain complete and accurate records as evidence of these decisions and business activities. The RMP directs all Defence personnel to manage their obligations when creating, capturing, controlling and disposing of Defence records across business environments and systems. It is supported by products located on the Enterprise Records Management[1] website that enable Defence personnel to meet the intended policy outcomes. They should be read in conjunction with this policy.
Scope and applicability:	RMP is an administrative policy framework document. It applies to all Defence personnel. The terms of a relevant contract may extend the application of this policy to a person/s engaged under a contract. Defence Instruction – Administrative policy[2] should be read in conjunction with this policy. In accordance with Defence Instruction – Administrative policy[3], the Secretary and the CDF expect Defence personnel to comply with this policy. Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include the requirement to comply. If so, include such terms in the contract.
Management:	The RMP will be reviewed three years from its date of issue. A review may occur sooner to ensure it continues to meet the intended policy outcome/s.
Availability:	The latest version of the RMP is only available on the Defence Publications[4] website. Its currency cannot be guaranteed if sourced from other locations. It is available for public release.

s47E(d)

s47E(d)

s47E(d)

s47E(d)

Policy domain:	Administration and Governance.
Accountable officer:	Associate Secretary.
Policy owner:	First Assistant Secretary Enterprise Transformation and Governance.
Policy contact:	Directorate of Enterprise Records Management.
Cancellation:	Records Management Manual – RECMAN.
Definitions:	Definitions that apply to RMP are at Annex 1A.

DEFENCE RECORDS MANAGEMENT POLICY

POLICY STATEMENT

1.1 Defence must manage its records[5] in a way that:

a. complies with legislation, standards and government policy;

b. provides for public accountability;

c. supports decision-making; and

d. preserves corporate memory and historical information.

1.2 To meet this requirement, all Defence records are:

a. created to support business and meet obligations;

b. captured in digital format and described;

c. made accessible and disclosed where required; and

d. appraised, retained and disposed of in accordance with the principles in this policy.

1.3 Records captured in digital format enable the systematic and consistent application of records management practice. Physical processes should only be used where digital systems are not available.

1.4 The Enterprise Records Management (ERM) Directorate provides the enterprise level policy, guidelines and products for records management in Defence. Defence personnel must comply with the enterprise level records management policy.

1.5 Groups and Services may establish supplementary records management guidelines where specific business requirements exist that are not catered for through the application of the enterprise level products. These supplementary records management guidelines must not be inconsistent with enterprise level policy. ERM can support Groups and Services to establish these supplementary guidelines. Business units may use these supplementary guidelines where applicable in accordance with the enterprise level records management policy.

1.6 Groups and Services will report against the expected outcomes of this policy and on the maturity of records management in Defence, which will inform external reporting obligations and identify areas for business improvement.

s47E(d)

PRINCIPLE 1: CREATING RECORDS

1.7 Records will be created to enable business, and preserve the corporate memory and historical information related to Defence events, activities, decisions and personnel.

RATIONALE

1.8 Records are required to be complete, reliable and fit for purpose enabling Defence to:

a. meet operational, legal and legislative obligations;

b. provide accurate and adequate evidence of Defence functions, policies, procedures, decisions and transactions; and

c. support lessons learnt and better decision-making in the future.

EXPECTED OUTCOMES

1.9 When records are created appropriately Defence will:

a. meet specific legislative requirements concerning the creation of records;

b. have evidence that certain actions, decisions or events occurred; and

c. have a collection of historical events acting as knowledgebase to inform future actions and decisions.

1.10 Additional products supporting the implementation of Principle 1 Creating Records[6] are located on the Enterprise Records Management website.

PRINCIPLE 2: CAPTURING AND DESCRIBING RECORDS

1.11 Defence records will be captured in systems that ensure they are adequately described, organised and stored for as long as they need to be kept.

RATIONALE

1.12 Descriptive information is used to identify, authenticate and contextualise the record and the people, processes and systems that create, maintain and use it. Without this information records have no context, making them difficult to find, retrieve and use.

1.13 Information needs to be structured in a way that enables Defence personnel to determine where to store their records and find information when they need it.

1.14 Appropriate preservation techniques ensure the records remain accessible and usable for as long as required.

EXPECTED OUTCOMES

1.15 When records are adequately described Defence personnel will be able to:

a. easily discover and retrieve records; and

b. have confidence in the authenticity and integrity of the records.

1.16 Structured information will be fit for purpose and organise records in a way that:

a. uses recognisable and understood terminology;

b. enables Defence personnel to know where they need to store records;

c. enables Defence personnel to navigate to the records they need; and

d. enables specialist records management activities including retention and disposal.

1.17 Defence systems will incorporate preservation activities that will ensure that records remain accessible and usable. For digital records this will include consideration of software, infrastructure and process requirements. For physical records this will include a controlled storage environment and the establishment of careful handling, transport and display procedures.

1.18 Additional products supporting the implementation of Principle 2 Capturing and Describing Records[7] are located on the Enterprise Records Management website.

PRINCIPLE 3 – ACCESSING AND DISCLOSING RECORDS

1.19 Access to Defence records will be managed in a way that ensures they are both available when needed and protected when required.

RATIONALE

1.20 Defence has an obligation under the *Archives Act 1983*[8], *Freedom of Information Act 1982*[9] and *Privacy Act 1988*[10] to enable external (public) access to Defence records. The Archives Act provides some exemptions for intelligence agencies.

1.21 Internal access to records will only be restricted when required by legislation, business requirement or in accordance with Defence security policy for the Classification and Protection of Official Information[11].

1.22 Incorrectly applied access control can make records unavailable to Defence personnel, inhibiting their ability to conduct business.

EXPECTED OUTCOMES

1.23 Defence will meet its obligations to provide access to the public.

1.24 Defence personnel will be able to locate and access the records they need to conduct Defence business.

1.25 Criteria for restricting access to records will be documented and consistently applied.

1.26 Additional products supporting the implementation of Principle 3 Accessing and Disclosing Records[12] are located on the Enterprise Records Management website.

PRINCIPLE 4 – APPRAISING, RETAINING AND DISPOSING OF RECORDS

1.27 Defence records will be disposed of when:

a. all legal retention requirements have been met in accordance with the relevant Records Authority; and

b. the records are no longer required for business or historical purposes.

[8] https://www.legislation.gov.au/Series/C2004A02796

[9] https://www.legislation.gov.au/Series/C2004A02562

[10] https://www.legislation.gov.au/Series/C2004A03712

[11] http://ibss/PublishedWebsite/LatestFinal/%7B49C4B82E-8C6E-4943-AEEF-6A51196C5127%7D/Item/%7B35F8B979-01BF-4D7B-A829-A5085122C478%7D

s47E(d)

RATIONALE

1.28 The legal requirements to retain records are mandated by legislation.

1.29 Records can be kept for longer than the minimum legal requirement if there is a business or historical need.

1.30 Records that are no longer required should be disposed of to:

a. enable the efficient and effective use of current records; and

b. reduce the cost of record management practice.

EXPECTED OUTCOMES

1.31 Records will be appraised to identify and document:

a. the legal retention requirements; and

b. the business and historical retention requirements.

1.32 Once records are identified as no longer required to be retained, the relevant transfer or disposal action is undertaken.

1.33 Additional products supporting the implementation of Principle 4 Appraising, Retaining and Disposing of Records[13] are located on the Enterprise Records Management website.

KEY ROLES, FUNCTIONS AND RESPONSIBILITIES

1.34 Responsibility for records management activity is delegated to the following key roles. Additional information regarding records management Roles and Responsibilities[14] is located on the Enterprise Records Management website.

1.35 **Group Heads and Service Chiefs** are responsible for ensuring records are managed appropriately within their Group or Service. Group Heads and Service Chiefs, together with Division Heads where appropriate, are accountable for ensuring records governance and assurance is adequately resourced and prioritised.

1.36 **Functional Commanders and Division Heads** are responsible for:

a. ensuring that records governance and assurance is adequately resourced and prioritised.

s47E(d)

s47E(d)

b. approving local records management guidelines that meet business and functional requirements.

1.37 **Records Management Advisors** are responsible for providing records governance and assurance activities within the respective Group, Service or Division and provide leadership and coordination required to:

a. assist the Group Heads and Service Chiefs, Functional Commanders and Division Heads to make records management related decisions.

b. marshal expertise to identify records management requirements and develop local records management guidelines.

c. support Records Management Specialists to complete their role.

1.38 The designated Records Management Advisor (RMA) are personnel at the executive level 2 or senior military rank 06. They act as the authorised point of contact and action delegate appointed by the Group Head, Service Chief or Division Head. The RMA are the delegated Group/Service or Division member of the Records Management Advisory Board (RMAB).

1.39 **Records Management Specialists** are responsible for managing and providing Defence expertise for records and content management activities including:

a. the creation of information structures within Enterprise Records Management systems to organise records, files and information.

b. building the security models in the business systems for providing access to and protection of information.

c. recordkeeping administration for storing, updating, accessing and preserving records, files, information, and artefacts.

d. advanced search, discovery and transfer activities.

1.40 The Records Management Specialist role commonly works within the Job Families profile of Information & Knowledge Management and requires relevant specialised records management training.[15]

1.41 For deployed and operational environment, see Commander Joint Operations Information Management handbook for Operations and Joint Exercises.

1.42 **Work Group Coordinators** are nominated by managers or supervisors to support work area personnel by:

a. managing access controls to folders and files by applying permissions within the Enterprise Records Management system, Objective.

b. assisting and providing guidance on the use of records management functionality in Objective.

c. providing general advice on identifying documents and artefacts that require records management.

1.43 The Work Group Coordinator role requires relevant specialised Objective training.[16]

1.44 **All Defence Managers and supervisors** are responsible for:

a. identifying where specialist records management resources are required.

b. ensuring Records Management Specialists are given support to complete records management activities, including policy and systems training.

1.45 **All Defence personnel** are responsible for:

a. identifying information, documents and artefacts that need to be captured as a Defence record.

b. storing records with appropriate naming conventions determined by the Group, Service or Division.

c. storing records with the appropriate security controls including applying permissions in the Enterprise Records Management system, Objective.

d. following the approved local records management guidelines

1.46 For deployed and operational environment, see Commander Joint Operations Information Management handbook for Operations and Joint Exercises.

1.47 All Defence personnel are required to complete records management training[17] relevant to their role.

s47E(d)

s47E(d)

ANNEX A

DEFINITIONS

The following list of terms are defined in Defence Instruction – Administrative policy.

The definitions are intended to apply to their use in administrative policy framework documents:

Accountable officer

Administrative policy

Australian Public Service employee

Commander

A person/s engaged under a contract

Defence

Defence civilian

Defence locally engaged employee

Defence member

Defence personnel

Defence-wide administrative policy framework document

Framework documents

Manager

Policy domain

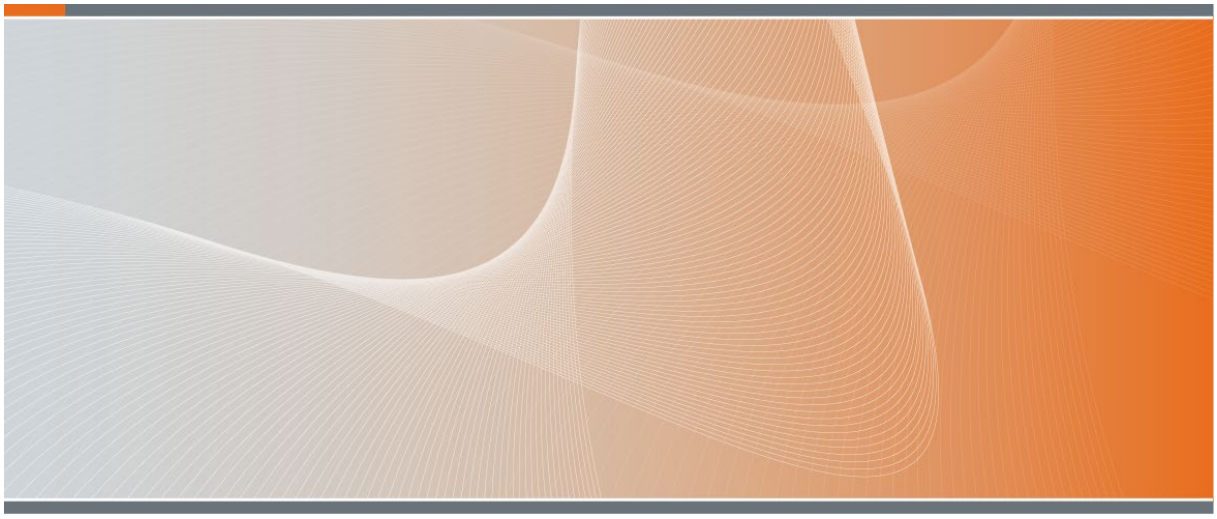
Policy owner

Supervisor

Australian Government

Defence

DEFENCE RECORDS MANAGEMENT POLICY



s22

Dr Paul Robards
Chief Data Integration Officer

Department of Defence
CANBERRA ACT 2600

30 June 2024

AMENDMENT CERTIFICATE

Amendment number	Amendment	Effective date
AL1	Major Amendments **Principle 1**: *Creating Records* and **Principle 2:** *Capturing and Describing Records* have been combined into *Creating and Capturing Records*. This is a more accurate reflection of the process wherein most records are simultaneously captured upon creation. **Principle 2** *In Life Records Management* is a new principle created to instruct on the importance of effectively protecting records and the hygiene activities that need to take place over time from creation to archiving. **Principle 3** changes from *Accessing and Disclosing Records* to *Archiving Defence Records* as this accurately reflects the next step in the records lifecycle. This principle provides advice to Defence personnel on how to correctly sentence and preserve Defence records for future retrieval or disposal. **Principle 4** is renamed *Access and Control of Records* previously *Appraising, Retaining and Disposing of Records* now covered in Principle 3. This change reflects the requirements of the *Archives Act 1983* for public access to Defence records, once a record reaches its Open Access Period.	04 Aug 2023
AL2	Update to the Objective Workgroup Coordinator role. Update to the All Defence Personnel role. Correction of spelling error	30 June 2024

DEFENCE RECORDS MANAGEMENT POLICY

Issued by:	The Defence Records Management Policy (this policy) has been issued by Chief Data Integration Officer with the authority of the Associate Secretary.
Purpose:	This policy describes the agreed approach to achieving compliance with legislation and whole of government policy. The Department of Defence (Defence) generates an enormous quantity of key decision and business activities. Defence is required, by law, to create and maintain complete and accurate records as evidence of these decisions and business activities. The Defence Records Management Policy directs all Defence personnel to manage their obligations when creating, capturing, controlling and disposing of Defence records across business environments and systems. This policy is supported by a range of products that enable Defence personnel to meet the intended outcome/s. They should be read in conjunction with this policy.
Scope and applicability:	This policy has been issued in accordance with *The Defence Instruction – Administration of the Australian Defence Force and Defence (Defence)* (AG1). The Secretary and the Chief of the Defence Force expect Defence personnel to comply with this policy. The terms of a relevant contract may extend the application of this policy to a person/s engaged under a contract. In accordance with AG1, Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include the requirement to comply. If so, include such terms in the contract. The Defence Instruction (including AG1) should be read in conjunction with this policy. In accordance with AG1, Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include the requirement to comply. If so, include such terms in the contract.
Management:	This policy has been developed, and will be maintained, in accordance with the Administrative Policy Arrangements. It will be reviewed within five years from its date of issue. A review may occur sooner to ensure it continues to meet the intended policy outcome/s.
Availability:	This policy is available at Defence documents. Its currency cannot be guaranteed if sourced from other locations. It is not available for public release.
Accountable officer:	Associate Secretary

Policy owner:	Chief Data Integration Officer
Policy contact:	Enterprise Records Managemen s47E(d)
Cancellation:	Defence Records Management Policy AL1
Definitions:	Definitions that apply to the Defence Records Management Policy are at Annex A.

POLICY STATEMENT

1.1. Defence must manage its records in a way that:

a) complies with legislation, standards and government policy;

b) provides for public accountability;

c) supports decision-making;

d) preserves corporate memory and historical information; and

e) adheres to the Defence Security Principles Framework and under the guidance of the Defence Good Administrative Decision-Making Manual.

1.2. Records management encompasses all activities involved in the management of records over the course of the records lifecycle. The lifecycle includes the creation, capture, in life management and archiving of records. In addition, Defence has a legislative requirement to manage and enable access to our records, whilst exercising and enforcing appropriate controls over the handling of those records.

1.3. Defence records are Commonwealth records and must be managed to the standards expected by the Commonwealth. Our records must be authentic, reliable and defensible. Our Records Management practices must be undertaken with integrity. Records Management decisions must be robust, defensible and transparent while being accountable to other relevant government agencies (such as the National Archives of Australia or the Australian National Audit Office) and the Australian public.

1.4. A record is any information, object or artefact, regardless of form or format (document, video, picture, audio, emails, web pages, technical drawings, social media posts etc.) that preserves the memory or knowledge of Defence events, activities, decisions and personnel. Records are a Defence asset and must be maintained, managed and protected.

1.5. All Defence records must be captured and managed in digital systems capable of meeting the record keeping requirements of the *Archives Act 1983*. Records captured in digital format enable the systematic and consistent application of records management practices whilst simultaneously ensuring that information is discoverable and accessible. Physical processes should only be used where digital systems are not available.

1.6. The Defence Records Management Policy is an inclusive policy and must be implemented in association with other relevant Defence policies. For example, the Defence Security Principles Framework, Defence Privacy Policy, Information and Communication Technology Policy, and Defence Data Policy must be considered when handling and managing records.

1.7. Defence engages with a broad and diverse range of risk across the organisation to achieve its objectives. Effective recordkeeping required considered judgements to determine risk management, cost and strategic value. Engaging with specialist risk areas in Defence management, will ensure managing Commonwealth records are complementary to other legislative requirements.

1.8. Some specialist areas in Defence have specific requirements for risk management including legislative obligations.

1.9. The Enterprise Records Management (ERM) team provides the enterprise level policy within the Defence Records Management Policy Framework. Defence personnel must comply with the enterprise level records management policy.

1.10. Groups and Services may establish supplementary records management guidelines where specific business requirements exist, for example in the use of military capability. These supplementary guidelines must not be inconsistent with legislative requirements or the Defence Records Management Policy. ERM can support Groups and Services to identify and develop supplementary guidelines, making them available to other areas of Defence.

1.11. Group and Services will report against he expected outcomes of this policy and on the maturity of records management in Defence, to inform external reporting obligations and identify areas for business improvement.

1.12. The Defence Records Management Policy is the capstone document in the Defence Records Management Policy Framework. Additional products supporting the implementation of this policy are available on the Enterprise Records Management Intranet site.

PRINCIPLE ONE – CREATING AND CAPTURING DEFENCE RECORDS

1.13. Defence records are created whenever there is a business need, legal requirement or expectation. The creation of Defence records supports accountability and transparency of Defence business by providing evidence of activities. Creation of records supports quality delivery of services, informs decision-making, and assists in meeting organisational goals.

1.14. Defence records will be captured in systems that ensure they are adequately described, organised and stored for as long as required under the *Archives Act 1983*. Without processes and tools to capture records, Defence is unable to meet its legislative obligations, whole of government reporting requirements and business needs.

RATIONALE

1.15. The legal requirement for Commonwealth agencies to retain records are mandated under the *Archives Act 1983*.

1.16. Record are to be complete, reliable and accurate, enabling Defence to:

a) Meet operational, legal and preservation obligations;

b) Provide adequate evidence of Defence functions, policies, procedures, decisions and transactions;

c) support business intelligence for robust decision-making; and

d) record the collective memory of Defence activities.

1.17. Descriptive information is used to identify, authenticate and contextualise the record and the people, processes and system that create, maintain and use it.

Without this information records have no context, making them difficult to find, retrieve, authenticate and use.

1.18. Information needs to be structured in a way that enables Defence personnel to determine where to store their records and find information when they need it.

1.19. Information needs to be structured in a way that enables it to be managed in accordance with the information security requirements under the Defence Security Principles Framework or other relevant security doctrine.

1.20. Information structures must be fit for purpose and consider:

a) usability for the business area;

b) appropriate groups with regards to management and disposal of source records after they have been appraised; and

c) the business requirement to share and access information, whist also maintaining security controls where needed.

1.21. Physical record holdings must be registered in an electronic record keeping system capable of fulfilling Commonwealth record keeping requirements to enable capture of contextual information, through life management, discoverability and access to the records. When physical records are not registered into an electronic system, Defence is unable to meet our legislative requirements, the records are unable to be leveraged for strategic purposes and non-compliant records management practices are more likely to occur.

EXPECTED OUTCOMES

1.22. Defence creates accurate, complete and reliable records that:

a) support a business function;

b) meet legislative requirements;

c) provide evidence of Defence decisions, activities, events or personnel; and

d) preserve the memory or knowledge of the Defence organisation.

1.23. Defence captures records into systems that:

a) adequately describe the records to enable identification, authentication and contextualisation;

b) have documented and defined processes;

c) structure the information to enable discoverability, retrieval and access;

d) structure the information so that it is fit for use by the user and can meet all information management requirements;

e) can manage the record through the entirety of the record lifecycle;

f) ensures information security requirements under the Defence Security Principles Framework (and other relevant doctrine) are met; and

g) incorporates preservation activities that will ensure that records remain accessible and usable. For digital records this will include consideration of software (including software obsolescence), infrastructure and process requirements.

1.24. Where a physical record holding exists, those physical records are registered into an electronic record keeping system to enable capture of contextual information, through life management, discoverability and access.

PRINCIPLE TWO – IN LIFE RECORDS MANAGEMENT

1.25. Defence records must be managed through all stages of the records lifecycle. Defence have record holdings that will need to be retained, in some cases, for multiple decades or in perpetuity. These records must be actively managed over this time to ensure the Defence is meeting our legislative obligations.

RATIONALE

1.26. Records will often outlive the organisational construction under which they are created. In life records management ensure that records are owned, managed, accounted for and protected. Defence needs to have mechanisms in place for the duration of the records life, to ensure ongoing accessibility and preservation of any inherited archival resources of the Commonwealth.

1.27. Digital records must be stored in system capable of meeting all records management requirements over the life of the record. Further, digital records must be protected against obsolescence in terms of both file formats and ICT systems and infrastructure. A failure to appropriately plan for through life management of records creates legacy systems. This may result in records that are inaccessible or undiscoverable.

1.28. Defence records are an asset. As an asset they must be maintained, managed and protected through their lifecycle. Even inactive records require management. Where records are not maintained, managed and protected Defence is unable to meet our legislative requirements, and we are unable to leverage our records for strategic advantage.

EXPECTED OUTCOMES

1.29. Defence records are managed at all stages of the records lifecycle between creation and disposal.

1.30. Defence knows where all records are stored (both digitally and physically)

1.31. Systems that contain records have established preservation standards to ensure the integrity and authenticity of records contained within, including obsolescence management and business continuity plans.

1.32. Systems that contain records have documented processes and procedures in place to maintain system compliance with record keeping requirements.

1.33. Physical records are stored in physical conditions that do not degrade the physical quality or intrinsic value of the record.

1.34. All Defence records have a custodian who is responsible for managing those records, including any risks associated with the record holding.

1.35. Record holding are monitored for compliance with record keeping requirements.

1.36. Record holdings are monitored to identify lost or damaged records. Any loss or damage of records is formally investigated, remediation actions are implemented and outcomes are reported to Enterprise Records Management to facilitate reporting to the National Archives of Australia in line with legislative requirements.

1.37. Defence is able to identify vital records to enable business continuity and to re-establish functions in the event of a disaster. Vital records are those that protect the assets and interest of Defence as well as those of its partners and clients.

1.38. Defence has documented processes and procedures in place to:

a) manage record transfers as a result of personnel movement;

b) manage information transfer between external service providers and Defence;

c) manage the commencement and ceasing of functions by the Department;

d) manage legacy record holdings;

e) manage information security requirements;

f) manage digitisation program; and

g) report on data breaches

PRINCIPLE THREE – ARCHIVING DEFENCE RECORDS

1.39. Archiving is the process by which inactive records, data or information, in any format, is security stored and preserved until the end of its retention schedule under the *Archives Act 1983*.

1.40. Archiving must ensure that inactive records are retained in an appropriate manner that is:

a) accessible for future business use; and

b) accessible to meet legislative requirements and managed in accordance with record keeping obligations

1.41. Archiving in Defence is broken down into three broad categories:

a) Appraisal

b) Sentencing

c) Disposal

1.42. An archive is a secure digital or physical repository where Defence stores its records between the end of their active life and the records disposal.

RATIONALE

1.43. The mechanisms that Defence can use to dispose of Commonwealth records are mandated under the *Archives Act 1983*.

1.44. Undertaking ongoing and consistent archiving processes not only ensures that Defence is managing is records through the record lifecycle, but that the department is managing our resources and risks.

1.45. The benefits of regularly undertaking archiving include:

a) Maintaining an awareness of what records are held

b) Responding quickly to discovery orders or access requests

c) Reducing liability and risk of holding information that could be destroyed

d) Reducing legacy holding of hard copy records

e) Identifying and managing high-value records

1.46. Defence records will be disposed when:

a) all legal retention requirements have been met in accordance with the relevant Records Authority; and

b) the records are no longer required for business or historical purposes.

1.47. Records are disposed to:

c) Meet legislative requirements under the Archives Act 1983;

d) Improve information security by reducing the holdings that may be subject to data breaches and leaks;

e) Reduce storage space and costs (either physically or digitally); and

f) Improve search-ability of systems by reducing volume.

1.48. Disposal of Defence records must be undertaken in an accountable, transparent and traceable manner.

EXPECTED OUTCOMES

1.49. Defence records are appraised to determine what legal disposal actions are available to use.

1.50. Defence sentences our records capturing those sentences in an electronic record keeping system to:

a) Identify legal retention requirements;

b) Monitor and manage the records over its retention period; and

c) Risk manage record holdings by identify high value records.

1.51. Defence disposes of our records using processes that:

a) meet legislative requirements under the Archives Act 1983;

b) capture all mandatory disposal information into systems that are searchable;

c) are accountable and transparent;

d) are defensible to other government agencies and the Australian public;

e) meet information security requirements under the Defence Security Principles Framework (or other relevant Security Doctrine); and

f) are strategically appropriate.

1.52. Where records are kept beyond their legal retention requirements, such retention is risk managed, documented and reviewed at regular intervals.

PRINCIPLE FOUR – ACCESS AND CONTROL OF DEFENCE RECORDS

1.53. Access to Defence records will be managed in a way that ensure they are both available when needed and protected when required.

1.54. Control over Defence records describes the mechanisms that govern the behaviour of those individuals who have a right to access or a need to access Defence records.

1.55. All Defence personnel are obligated to report and respond to a suspected privacy data breach within their work area using the Privacy Data Breach Form (AF100). In accordance with the *Privacy Act 1988* and under the Notifiable Data Breach (NDB) scheme, in the event of unintended or unauthorised disclosure or loss of personal information. Defence must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) about an eligible data breach.

RATIONALE

1.56. Access to Defence's records is managed for two distinct groups;

a) Defence personnel; and

b) the public

1.57. The *Archives Act 1983* establishes the public's right to access Commonwealth records. Defence's business requirements establish the need for Defence personnel to have access to records. Access to records must be managed to ensure that personnel can access records needed to fulfil their role on behalf of Defence.

1.58. Internal access to records will only be restricted where required by legislation, Defence's business requirement or in accordance with Defence Information Security Requirements.

1.59. Incorrectly applied access controls can make records unavailable to Defence personnel, inhibiting their ability to conduct business, strategically leverage our information and manage the record through life.

EXPECTED OUTCOMES

1.60. Defence meets its obligations to provide access to Defence records to the public in accordance with the requirements of the *Archives Act 1983*.

1.61. Defence systems that contain records have governance arrangements that document the management of security restrictions, access and controls for accessibility and discovery of records required.

1.62. Change controls are in place for the management of systems that contain Defence records.

1.63. A security matrix is in place that identified what each system user is able to do and mechanisms are in place to ensure users have been deactivated from the system when they cease employment or change Defence employment types.

KEY ROLES, FUNCTIONS AND RESPONSIBILITIES

1.64. **Group Heads and Service Chiefs** are responsible for ensuring records are managed appropriately within their Group or Service. Group Heads and Service chiefs, together with Division heads, where appropriate, are accountable for ensuring records governance and assurance is adequately resources and prioritised.

1.65. **Division Heads** are responsible for:

a) ensuring that records governance and assurance is adequately resourced and prioritised; and

b) approving Group, Service or Divisional specific records management guidelines and instructions where required. These must not conflict with the Defence Records Management Policy.

1.66. **Enterprise Records Management Directorate (ERM)** is responsible for providing policy, procedures and guidance to better inform and support enterprise records management.

1.67. **Records Management Advisors (RMA)** are personnel at the Executive Level 2 or Senior Military Rank 06. They act as the authorised point of contact and action delegate appointed by the Group Head, Service Chief or Division head. The RMA are the delegated Group, Service or Division members of the Records Management Advisory Board (RMAB). Records Management Advisors are responsible for providing records governance and assurance activities within the respective Group, Service or Division and provide leadership and coordination.

1.68. **Records Management Specialists (RMS)** are personnel that commonly work within the Job Families profile of Information & Knowledge Management and require relevant specialist records management training.

1.69. **Objective Workgroup Coordinators (WGC)** are APS or ADF personnel nominated by managers or supervisors to support work area personnel, and are responsible for:

a) Managing access controls to folders and files by applying permissions within Objective;

b) Assisting and providing guidance on the use of records management functionality in Objective;

c) Providing general advice on identifying document and artefacts that require records management; and

d) Carrying out maintenance and assurance activities across their Objective Workgroup.

1.70. Managers and Supervisors must not appoint a consultant, contractor, or external service provider as an Objective Workgroup Coordinator.

1.71. If a business unit determines there is an operational requirement for a consultant, contractor, or external service provider to undertake the duties of an Objective Workgroup Coordinator exists, a business case and risk assessment must be undertaken. The Approval Authority to appoint a non-Commonwealth official into a WCG role is at the SES1 / 1 Star level.

1.72. **Defence Record Sentencing Officers** are nominated by managers or supervisors to sentence Defence records on behalf of that business unit. A sentencing officer must be trained to undertake sentencing, with the proficiency recorded in PMKeyS. They are responsible for:

a) Appraising and sentencing Defence records; and

b) Monitoring record holdings for execution of sentences.

1.73. All **Defence Managers and Supervisors** are responsible for:

a) Identifying where specialist records management resources and Objective Workgroup Coordinators are required and maintaining these roles within their unit; and

b) Ensuring Records Management Specialists and Objective Workgroup Coordinators are given support to complete records management activities, including policy and systems training.

1.74. **All Defence personnel** are responsible for:

a) identifying information, documents and artefacts that need to be captured as a Defence record;

b) storing records with appropriate naming conventions determined by the Group, Service or Division;

c) storing records with the appropriate security controls including applying permissions in the Enterprise Records Management system, Objective;

d) following approved local records management guidelines, where applicable;

e) transferring custodianship of records to an appropriate custodian prior to position movement (including transfer, resignation or termination); and

f) completing records management training relevant to their role.

ANNEX A

DEFINITIONS

The following list of terms are defined in The Defence Instruction. The definitions are intended to apply to their use in administrative policies.

Accountable officer
Administrative policy
A person/s engaged under a contract
Australian Public Service employee
Commander
Defence
Defence civilian
Defence locally engaged employee
Defence member
Defence personnel
Directions
Manager
Personal information
Policy owner
Provision
Supervisor
Technical authority

For the purpose of the administrative policies described in this document, the following definitions apply:

Record: any information, object or artefact, regardless or form or format (document, video, picture, audio, emails, web pages, technical drawings, social media posts etc.) that preserves the memory or knowledge of Defence events, activities, decisions and personnel.

Records Management: the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining formation about business activities and transactions in the form of records.

Archiving: The processes by which inactive records, data or information, in any formation is securely stored and preserved until the end of its retention schedule under the *Archives Act 1983*.

Archive: A security digital or physical repository where Defence stores its records between the end of their active life and the records disposal.

Disposal: Under the *Archives Act 1983*, disposal of Australian Government information means either its destruction, transfer of its custody of ownership or damage or alteration.