BUSINESS RULES
AIR FORCE PERSONNEL FILE – UNIT PERSONNEL RECORD

BUSINESS RULE CHANGES

BLUF: Previous versions of the Air Force Personnel File – Air Force Unit Personnel Record (AF UPR) Business Rules referred to procedures for the Defence Single Personnel File which was being trialled in 2016. At the conclusion of the trial, Defence was not in a position to introduce the Defence Single Personnel File so the AF UPR Business Rules are being amended to ensure they align with procedures suited to the current requirements of Air Force Personnel Files.

Please note that the AF UPR Management Team manages AF UPRs only, advice on Army, Navy and Civilian records is to be directed to the relevant agencies.

The current list of what is filed on the AF UPR is being withdrawn with the Business Rules. The principle of what is to be filed on the AF UPR is from the current digital records policy documents – AFIMMAN and Defence Records Management Policy. Unit administrators are requested to familiarise themselves with the policy documents to assist with determining if a document is to be stored on a member's AF UPR. AFIMMAN 3.6 details that Defence will protect official information in accordance with the expectations of the originator of the information. AFIMMAN 3.3 details the 'need to know' principle that is to be applied to documents and should be referred to by members filing information on AF UPRs to assist with determining what documents should be stored on the file.

The principles being adopted by the AF UPR Management Team for documents being filed on members' AF UPRs are:

- Unit-based decisions not stored on any other AFPF; example – General applications
- Applications generated by members (completed applications only)
- Documents that the member may require during their service; examples – Recognition of a De Facto Relationship, HQJOC Deployment Certifications etc.

Non example – Any documents generated outside the unit that are filed on another AFPF are not to be duplicated on the AF UPR.

This Business Rules are to be read in conjunction with the FAQs available on the AF UPR Management team webpage.

BUSINESS RULES

Introduction

Air Force Personnel Files (AFPF) are the primary record source for all personal documentation pertaining to a member's Service career.

Purpose

The purpose of this document is to outline the Business Rules (BR) associated with one component of AFPF only; which is the management of Air Force Unit Personnel Record (AF UPR).

There is over 20 file types under the overarching AFPF and are managed by the individual relevant stakeholders. The Air Force UPR Management Team manages AF UPRS only, which is an amalgamation of Unit Personnel Record (UPR), Aircrew Flying Service Record (AFSR) and Members Training Record (MTR).

A UPR is a centralised filing location for the management of records which pertain to a member's career at a unit level. The documentation within this file contains unit based decisions in the way of applications and forms that contain/contribute value to the member's career or that may be required for reference by the decision makers. The UPR then follows the member from posting to posting until they discharge and terminate their service. Once this has occurred, the file is then sentenced and retained by Archives for their required sentencing term.

Authority

The management of AF UPRs falls within the authority of Air Command Knowledge Management (ACKM), led by the Air Command Information Manager.

BUSINESS RULES

Creation of Air Force Unit Personnel Records (UPRs)

To minimise duplication and to mitigate incorrect processes, ACKM have authorised the following cells to create AF UPRs:

a. No 1 Recruit Training Unit (1RTU) – newly enlisted Air Force Personnel
b. Officer Training School (OTS) – newly appointed Air Force Personnel

In order to create an AF UPR, the above cells are to contact the AF UPR Management team and request a copy of “BLI 01 - Virtual UPR Creation”.

BUSINESS RULES

Air Force Personnel File Structure

All files and folders within the Air Force Personnel File structure (objective id: fR4850855) are maintained in one of the HQAC – Air Force UPR Management Group repositories.

The corporate file and AF UPR structure are two separate areas within Objective and should be treated as such. Retaining documentation relating to personnel on a corporate file is to ensure Defence records are easily accessible to those who have a need to access them, additionally it is to ensure a record is maintained as a corporate record where by a decision or outcome is being executed. Duplication of a document for the above reason is thereby authorised and is not deemed as unnecessary duplication IAW the Department of Defence Records Management Strategy.

BUSINESS RULES

Members File Privileges

Members will have 'See' and 'Open' access to all folders within their own UPR with the exception of:

- Training – Up to 'Edit' access
- Discipline and Adverse Admin Action - No access.

Information on how to locate your own UPR is located on the FAQ tab on the AF UPR Management Team's webpage.

Units are NOT to apply their own privileges to AF UPRs or to any of the mandated folder in the structure, nor are they to request ICT to do this for them. The UPR Management Team are the only authorised cell to apply privileges.

User Groups

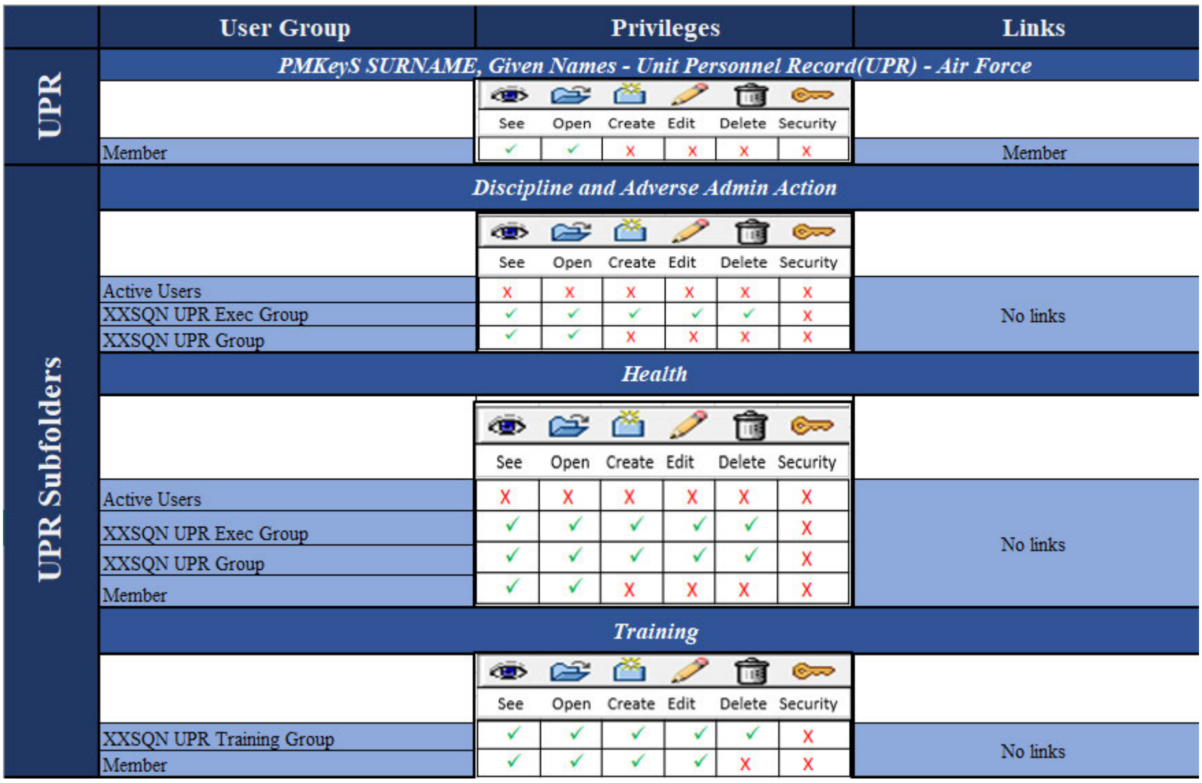
The UPR Management Team is responsible for the application of the below 3 listed standardised user groups on an AF UPR and manages the level of privileges assigned to each user group.

UPR Group
UPR Exec Group
UPR Training Group

Unit Work Group Co-ordinators (WGC) are responsible for managing the above user groups and maintaining the correct user access as deemed appropriate by them or the Unit Executives for the unit.

AF UPRs are not a working area, nor are they accessible by those whom do not have a business reason to do so due to their Sensitive: Personal markings.

Need to Know and Need to Share principles apply and will be actively audited through the provisions provided by the Governance Framework – Air Force Personnel File – Air Force Unit Personnel Record.



	User Group	Privileges						Links
UPR	*PMKeyS SURNAME, Given Names - Unit Personnel Record(UPR) - Air Force*							
		See	Open	Create	Edit	Delete	Security	
	Member	✓	✓	✗	✗	✗	✗	Member
UPR Subfolders	*Discipline and Adverse Admin Action*							
		See	Open	Create	Edit	Delete	Security	
	Active Users	✗	✗	✗	✗	✗	✗	No links
	XXSQN UPR Exec Group	✓	✓	✓	✓	✓	✗	
	XXSQN UPR Group	✓	✓	✗	✗	✗	✗	
	Health							
		See	Open	Create	Edit	Delete	Security	
	Active Users	✗	✗	✗	✗	✗	✗	No links
	XXSQN UPR Exec Group	✓	✓	✓	✓	✓	✗	
	XXSQN UPR Group	✓	✓	✓	✓	✓	✗	
	Member	✓	✓	✗	✗	✗	✗	
	Training							
		See	Open	Create	Edit	Delete	Security	
	XXSQN UPR Training Group	✓	✓	✓	✓	✓	✗	No links
	Member	✓	✓	✓	✓	✗	✗	

Repositories

ACKM manages the following repositories and all file parts assigned to them:

a. HQAC – Air Force UPR Management Group – members who are of a generalist nature must be assigned to this repository.
b. HQAC – Air Force UPR Protected Identity Secure Group – members who are of a protected nature must be assigned to this repository.
c. HQAC – Air Force UPR – Archive – members whom have terminated from Air Force at completion of 5 year post discharge service in an inactive reserve capacity.

Members who are unable or not required to meet their five year inactive reserve obligations post-discharge are to have their AFUPR closed and assigned to the HQAC – Air Force UPR – Archive repository. Circumstances which may warrant this are:

a. Medical discharge
b. Administrative discharge/termination
c. Compulsory retirement or
d. Death.

BUSINESS RULES

Document Filing Responsibilities

The requirement to file documents onto a member's AF UPR is solely the responsibility of the administrative area to which the member belongs and not the UPR Management Team.

Unit administered documentation relating to a members AF career can be filed on an AF UPR. All documentation must be finalised before being filed. Loose documentation is not permitted within the UPR Structure, all documents should be filed on a corresponding folder within the subfolders provided.

Physical document shells must remain on the members AF UPR until the original physical document has been located. A thorough search must be conducted and documented by the units. If the corresponding document cannot be located, the shell will remain on the file and the file will remain Mixed Mode, even after digitisation IAW the instructions stipulated on the DRMP webpage.

To further maintain the privilege security, the ownership of objects contained within AF UPRs must be categorised as Defence.

Temporary UPR folders and loose documents are not to be created or held within the AF UPR OBJ Structure. Temporary folders and documents may be stored in the unit's Work Group area until the unit gains access to the members virtual AF UPR.

Temporary Access

If temporary access to a UPR is required the request must come from the Unit with the Chain of Command endorsement. Access requests will be reviewed on a case-by-case basis and granted if deemed necessary.

Please note that the temporary access won't be granted to complete the filing of loose documentation pertaining to members either posted out or discharged. Units are to liaise with the gaining Unit to organise the transfer of documentation via Drop Box or emailing PDFs. Alternatively, Units can email loose documentation to Your Customer Service Centre group mailbox for them to action the filing requests.

Key stakeholders have been provided access to all AF UPRs via the AFPF repository to ensure record management assistance is actioned when required.

**Access to UPRs within your Unit is managed by the WCG – see 'User groups' paragraph above

BUSINESS RULES

Conduct Records

Further information pertaining to the legal storage requirements of Conduct Records will be disseminated in due course.

CHAPTER 3

ACCESS AND SECURITY

s22

[redacted]

3.3 Defence personnel and external service providers must ensure that access to official information is limited to those who need-to-know the information for their official duties (except for unclassified information authorised for public release). This is called the need-to-know principle. Personnel found to be accessing information where they cannot justify their need-to-know, will be subject to disciplinary action. Integrity of the information is to be maintained by regular audits of the information for currency, relevance, security and filing compliance.

s22

[redacted]

INFORMATION SECURITY

3.6 Defence will protect official information in accordance with the expectations of the originator of the information. Where Defence is the originator of information, it will classify that information, according to the impact of access by, or disclosure to, unauthorised individuals, groups or organisations. Suitable controls are applied to official information to ensure that it is protected from unauthorised access or disclosure.

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

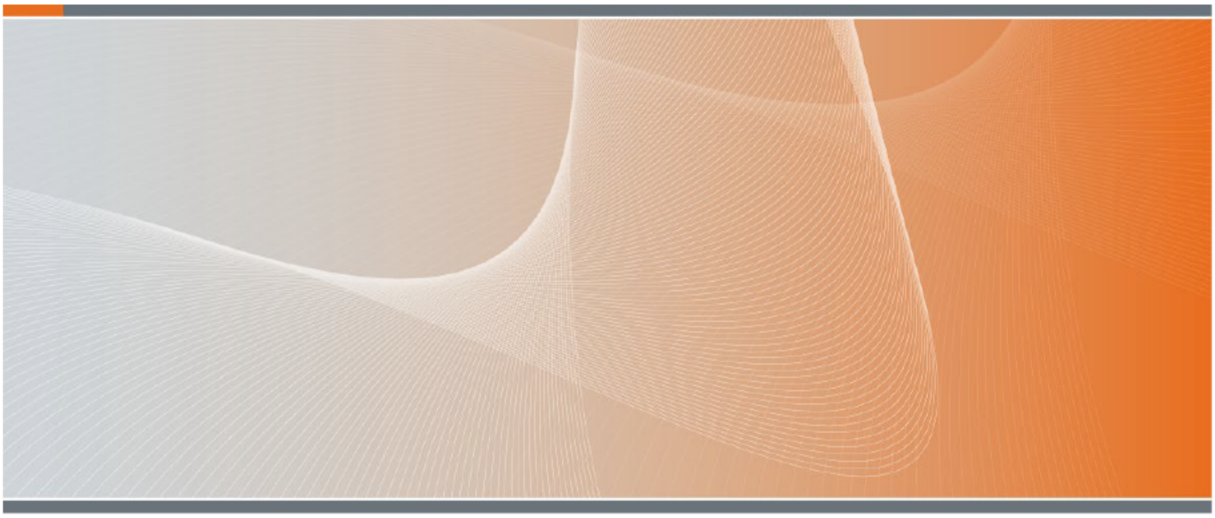
s22

[redacted]

Australian Government

Defence

DEFENCE RECORDS MANAGEMENT POLICY



s22

John Reid PSM
First Assistant Secretary
Enterprise Transformation and Governance

Department of Defence
CANBERRA ACT 2600

04 August 2023

AMENDMENT CERTIFICATE

Amendment number	Amendment	Effective date
AL1	s22 [redacted] **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 23

DEFENCE RECORDS MANAGEMENT POLICY

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

PRINCIPLE FOUR - ACCESS AND CONTROL OF DEFENCE RECORDS

1.53 Access to Defence records will be managed in a way that ensures 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 (OIAC) 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 identifies what each system user is able to do and mechanisms 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 resourced 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 specialised records management training.

1.69 **Workgroup Coordinators (WGC)** are 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 documents and artefacts that require records management; and

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

1.70 **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 holding for execution of sentences.

1.71 **All Defence Managers and Supervisors** are responsible for:

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

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

1.72 **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 1A

DEFINITIONS

s22

[redacted]