

## Privacy Statement

The PMKeyS Portal is accessible from both the Defence Restricted Network and the Internet.

The PMKeyS Portal and the single sign-on applications accessible from the Portal (e.g. PMKeyS Self Service (PSS) and People Central sites) have been developed in accordance with the [Australian Privacy Principles](#) (APPs) as described in the [Privacy Act 1988](#) and the Office of the Australian Information Commissioner - [Guidance for agency websites: 'Access to Information'](#). For more information, see: [OAIC - The Privacy Act](#)

### 1. Collection of Personal information

- 1.1 Applications hosted on the PMKeyS Portal seek to comply with the APPs in the collection, storage, use and disclosure of personal information. Specifically, PSS allows employees to update certain personal information and emergency contacts such as address and telephone numbers; submit leave applications and Employment Preferences and Restriction (EPARs) [via AD148](#) (ADF members).
- 1.2 PSS progressively allows staff to undertake more personal transactions on-line. By necessity, and in support of workflow, this requires that certain information is made available to line managers and supervisors to the extent that is reasonably required to fulfil their management responsibilities. For example, they will have access to Emergency Contact details, so that in the event of an emergency, prompt action can be taken to notify primary contacts, should this be necessary.
- 1.3 In order to make an informed decision about whether to grant leave, immediate line managers are able to view leave balances. APP 6 binds all individuals, including managers, supervisors and administrative support staff in regards to the use and disclosure of any personal information contained in PMKeyS.

### 2. Use and disclosure of Personal information

- 2.1 APP 6 outlines the rules for use and disclosure of personal information held by an APP entity. All PMKeyS users are to ensure that personal information contained in PMKeyS, is handled in accordance with APP 6.
- 2.2 [Defence Privacy Policy](#) and [Enterprise Records Management \(ERM\)](#) outlines the governance, process, procedures and responsibilities when managing personal records in Defence. [ERM 3](#) defines access and disclosure of Defence records.
- 2.3 Unauthorised or inappropriate use or disclosure of personal information is considered a breach of the [APS Code of Conduct](#) in the case of APS employees, or the [Defence Force Discipline Act 1982](#) (DFDA) in the case of ADF members.

- Breaches may result in corrective action under the procedures set out on the People Connect Website: [Privacy Data Breaches](#) or the relevant provisions of the [Defence Force Discipline Act 1982](#).
- Concerns regarding breaches of privacy should be directed to [Defence Privacy Service](#).



# **Australian Government**

---

## **Defence**

**ENTERPRISE PROCESS OWNER – PEOPLE**

**EPO-P 101.1**

**PMKeyS  
Information System -  
Security Practices and Procedures (IS-SPP)**

**Version 4.5**

(intentionally left blank)

## REVISION HISTORY

Author	Organisation	Date	Version	Comment
s47E(d)		1 AUG 2005	1.6	Changes from ISA review for OHSC.
		12 SEP 2005	1.6.1	Amendments.
		12 JAN 2006	1.6.2	Clarification of user access requirements.
		31 JAN 2006	1.6.3	Update document – Roles of ISSO & Security Manager
		15 FEB 2006	1.6.4	Updated comments from PCSC.
		10 MAR 2006	1.6.5	Updated comments
		23 MAR 2006	2	Updated to include PCSC comments.
		28 NOV 2006	2.1	Update to reflect restructure.
		20 AUG 2008	2.2	Review and update
		NOV 2010	2.3	Review and update
		AUG 2014	3.0	Review and update to reflect new Privacy laws
		NOV 2017	3.1	Review and update
		DEC 2017	3.2	Review and update
		DEC 2017	3.3	Review and update
		SEP 2019	4.0	Minor updates, incremented for authorisation.
		NOV 2019	4.1	Review and update
		FEB 2020	4.2	Review and update
		MAY 2020	4.2	Review and update
		AUG 2020	4.3	Change password length from ten to 14 characters
		SEP 2022	4.4	Update password character requirements, access to PI data obligations
		DEC 2022	4.5	Review and update

## AUTHORISATION

Document Authoriser	Version	Signature
Director s47E(d)	v4.5	s47E(d)

Proposals for amendment, or requests for copies of this Documentation Control Standard, are to be forwarded to:

Assistant Director s47E(d)  
s47E(d)  
Department of Defence  
CANBERRA ACT 2600

## TABLE OF CONTENTS

<b>Definition of Terms .....</b>	<b>v</b>
<b>Part One – General Information .....</b>	<b>1</b>
Introduction.....	1
Document Relationships .....	1
Audience .....	1
Goals .....	1
Objectives.....	1
Scope .....	2
<b>Part Two – Practices and Procedures.....</b>	<b>3</b>
General.....	3
Conditions of Access.....	3
Password Management .....	4
User Responsibilities.....	4
Privileged Users .....	5
Special Authorisers .....	5
System Security Sponsor .....	5
Access to PMKeyS Sourced Data through other Applications or Databases .....	6
Breaches of Security .....	6
<b>Annex A.....</b>	<b>8</b>
Duties of the PMKeyS Information Technology Security Officer (ITSO).....	8
Duties of the PMKeyS Information Technology Security Manager (ITSM).....	8

## DEFINITION OF TERMS

**PROTECTED** – the Application has a system security rating of PROTECTED where:

- a. The highest classification of information processed on Personnel Management Key Solution (PMKeyS) is PROTECTED;
- b. Access to an associated workstation is restricted to users with a minimum security clearance of Baseline as outlined in the [Protective Security Policy Framework \(PSPF\)](#); [and](#)
- c. Access to PMKeyS is restricted to users who have a genuine '[need-to-know](#)' requirement to view PROTECTED data and have been granted formal approval.

**Workstation** – the term 'Workstation' refers not only to a computer unit (including Defence Protective Laptop) but to any storage and production media used in conjunction with a unit. This includes remote logon via DREAMS, the Home portal and media such as; removable drives for example USB Flash drives, separate printers and other storage devices.

**PMKeyS** – the term 'PMKeyS' includes the PMKeyS portal, Business Application, and Self Service. The term extends to Customer Relations Management (CRM) applications, including ComTrack Self Service (CSS), which are accessed via the PMKeyS Portal. Where aspects of this document relate to the PMKeyS Business Application only, the relevant paragraphs will include the words 'PMKeyS Business Application'. In all other cases this IS-SPP applies to the entire PMKeyS suite.

**PMKeyS Data** – the term 'PMKeyS Data' refers to data accessed directly through the PMKeyS application and/or sourced from PMKeyS reports, extracts and interfaces. The term also refers to data that is available through other applications that are automatically or manually loaded with data sourced from PMKeyS.

**Human Resource Reporting Applications** – this document does not specifically cover the access management arrangements for Human Resource Reporting Applications, including Management and Analysis Reporting Solution (MARS), Human Resource Metric System (HRMeS) and a data integration platform named InfoSphere; the Goals and Objectives of this IS-SPP apply to the Human Resource Reporting Applications. For details on access management practices and procedures for the Human Resource Reporting Applications, refer to the [MARS Website](#).



## PART ONE – GENERAL INFORMATION

### Introduction

1. ICT Security in the context of PMKeyS concerns the control of data in PMKeyS. Security measures are implemented to ensure that data is stored, processed, transferred, and is adequately protected according to its sensitivity. The PMKeyS Security Operating Procedures, known as the PMKeyS Information System - Security Practices and Procedures (IS-SPP), are designed for a system security rating of PROTECTED and apply to the entire PMKeyS software suite.

2. PMKeyS is hosted on the Defence Protected Network (DPN) and is accessible directly via the DPN (including via Defence Protected laptops), through a DREAMS logon to the DPN, the Home portal, and through the deployable networks. §22

This IS-SPP does not replace the [Defence Security Principles Framework \(DSPF\)](#), that outlines the responsibilities of all users' access to the DPN. Document Relationships

3. This IS-SPP is referenced to the [Australian Government Information Security Manual \(ISM\)](#), the Protective Security Policy Framework (PSPF), the [Defence Security Principles Framework \(DSPF\)](#), and the [Australian Privacy Principles \(APPs\)](#) as stated in the *Privacy Act 1988*.

4. Detailed instructions on the management of access to PMKeyS are provided on the [PMKeyS – Access & Password webpage](#).

### Audience

5. This IS-SPP is to be read prior to all users being granted access to the PMKeyS Business Application and/or the CRM and/or CSS Applications. It is a requirement that the IS-SPP is read and acknowledged by all users of PMKeyS.

### Goals

6. The goals of this IS-SPP are to:

- a. Establish a standard set of security policy practices and procedures to be used by all users of PMKeyS;
- b. Reduce the risk of information loss by accidental or intentional disclosure, destruction or denial of access;
- c. Maintain the security, privacy, integrity and availability of PMKeyS and the data held in PMKeyS; and
- d. Ensure all personnel with access to PMKeyS take responsibility for the data they manage and/or use.

### Objectives

7. To meet these goals, the following objectives must be achieved:

- a. Prevention of unauthorised access, disclosure, modification, manipulation, or deletion of PMKeyS data;
- b. Authentication of PMKeyS users;
- c. Establishment of security mechanisms that are flexible and responsive to changes in organisational structures and individual responsibilities;

- d. Provision of means for identifying unauthorised access to PMKeyS and/or data and for taking appropriate corrective, preventative or disciplinary action;
- e. Limit the use of PMKeyS to the purposes for which such resources are intended;
- f. Ensure appropriate governance is in place for the security and privacy protection of PMKeyS data when accessed through applications and databases other than PMKeyS; and
- g. Ensure that the system sponsor and/or delegates and authorised users are aware of their respective responsibilities with regards to maintaining the security of the data.

### **Scope**

- 8. This is a 'living' document and its contents will be constantly monitored to ensure it is up-to-date and relevant.
- 9. The practices and procedures contained in this document are to apply to all data created, processed, and stored on PMKeyS.

## PART TWO – PRACTICES AND PROCEDURES

### General

10. PMKeyS has a security rating of PROTECTED. All users must be cleared to Baseline and have a 'Need-to-Know' requirement for data to which formal access has been approved. s47E(d)

### Conditions of Access

11. Before gaining access to the PMKeyS Business Application and/or the CRM application, personnel must:

- a. Read and understand this IS-SPP.
- b. Be aware of their responsibilities in using PMKeyS, as detailed in paragraphs 22 – 27 below.
- c. Be granted as a minimum, a security clearance equal to the classification of Baseline. Higher security clearances are required for some levels of PMKeyS access.
- d. Have a 'Need-to-Know' requirement to access the data for the purpose of performing assigned tasks.
- e. Have been appropriately trained for the required PMKeyS access, and are competent to browse and/or transact in PMKeyS. Have completed the Campus courses mandatory for PMKeyS access; *Australian Privacy Principles eAssessment* and *Defence One Introduction & Reporting*. To gain access to the Global Payroll application, the *Defence One Introduction to Global Payroll* Campus course must also be completed.
- f. Request PMKeyS Access via Self Service. This access request method is available to users where their Service or Group has mapped PMKeyS access roles to positions, and where the user has completed the prerequisite PMKeyS training courses. In cases where the PMKeyS roles to position have not been mapped, or access is requested for a CRM application, the user and supervisor are to complete *Webform AD688 Application for PMKeyS Access* form.
- g. Access to s47E(d) data can only be granted with the agreement of the relevant s47E(d) authorisers.

12. **Supervisors** are to ensure that personnel using the [Webform AD688](#):

- a. Applied for the appropriate access required to perform their assigned tasks;
- b. Met mandatory training requirements for the access requested; and
- c. Read and understood this IS-SPP.

13. **Special Authorisation** is required before access can be granted to sensitive data including, but not limited to; Career Management, Discipline, Human Resource Budgeting, Drugs and Alcohol and Professional Development & Training. Additional detail is provided at paragraphs 32 – 33 below.

### Password Management

14. Access to the PMKeyS portal is given to all ADF and APS personnel upon commencement. Access to the PMKeyS portal is only given to contractors where access to the PMKeyS Business Application has been authorised.

15. PMKeyS identifies individual users by their unique Operator ID and password. s47E(d)

16. Users must change their password during their initial login. The password protects the user's account from unauthorised use. Passwords are classified as 'Official: Sensitive' and must not be revealed to any other person.

17. The following policies are to be enforced by PMKeyS on all user passwords:

s47E(d)

18. The s47E(d) is to be notified if a user's password is compromised, or suspected of being compromised. The s47E(d) is to log the details and initiate action for the compromised password to be changed.

19. Automated procedures for deletion of access to PMKeyS are documented on the PMKeyS website. s47E(d)

s47E(d)

21. Users are required to set up their PMKeyS Portal password reset hint on initial login. Users who have forgotten their password (and have not set up a reset hint) or have a locked account are to contact the Defence Service Network (DSN) for assistance. Refer to the [Password Management](#) webpage.

### User Responsibilities

22. All users must:

- a. Abide by the policies, practices and procedures set out in this document; and
- b. Report at once any attempted or actual breach of security to the s47E(d) via email s47E(d) and/or s47E(d)
- c. Report any shared or suspected s47E(d) data spills by completing an [XP188 form](#)

23. It is the responsibility of all users to:

- a. Maintain **confidentiality** and **integrity** of information stored on PMKeyS; and
- b. Read and understand the PMKeyS IS-SPP prior to granting access to the PMKeyS , CRM and/or CSS Business Applications, or when notified that amendments have been made.

24. Supervisors are responsible for ensuring that a user has read, understood and complies with the PMKeyS IS-SPP.

25. No user is to attempt to bypass or defeat the security systems, or attempt to obtain use of passwords or privileges issued to another person.

26. All users must use their own account for specific work-related tasks only. Unauthorised changes to, or creation of, PMKeyS accounts is not permitted. Any suspected changes will be investigated as a breach.

27. Prior to granting access to PMKeyS, all users are to be made aware of their responsibilities and complete a declaration as acceptance of responsibilities. By signing an AD688 Application for PMKeyS Access form, or by accepting the *Privacy & Security Acknowledgement* when applying for PMKeyS access via Self Service, the user acknowledges they have read, understood, and accept the terms and conditions set out in this PMKeyS IS-SPP.

### Privileged Users

28. The administration of PMKeyS permits certain users to hold accounts that enable a greater level of functionality than is offered by a standard user account. s47E(d)

Those with privileged access have the same responsibilities under the IS-SPP as a standard user.

s47E(d)

30. Privileged user access are reviewed quarterly for compliance confirmation by the s47E(d) and/or their delegates. An access review can be conducted at any time by the user themselves, or the user's supervisor/manager.

31. Privileged users are required to maintain a correction log as documented in the Requirements webpage. The s47E(d) and/or their delegates/Business areas may conduct regular audits of correction logs to ensure compliance.

32. Special Authorisers are in place to ensure that personnel requesting access to PMKeyS have:

- a. Requested the appropriate privileged access to adequately perform their assigned tasks;
- b. Undertaken the required PMKeyS training and are competent to transact in PMKeyS;
- c. Read and understood the PMKeyS IS-SPP; and
- d. Understand the Australian Privacy Principles and how they apply to PMKeyS.

33. Special Authorisers are to ensure they are aware of their respective responsibilities and the responsibilities of the users they are authorising with regard to maintaining the security and privacy of information.

### System Security Sponsor

34. The System Security Sponsor s47E(d) and/or their delegates are responsible for:

- a. Conducting a review of the PMKeyS IS-SPP to ensure it continues to comply with the goals and objectives detailed in Part One (General Information) of this document;
- b. Ensuring the implementation of, and sustained compliance by running monthly and quarterly reports, and engaging with customer to justify their requirement for accessing PMKeyS and meeting their obligations for security, the PMKeyS IS-SPP;
- c. Resolving information system security issues in consultation with the s47E(d)



- d. Ensuring an s47E(d) is nominated for the PMKeyS application;
- e. Ensuring that the s47E(d) carry out their duties in accordance with Annex A of this document; and
- f. Ensuring that the current version of the IS-SPP is available for viewing by all users on PMKeyS via the Portal login page, and on the PMKeyS website.

#### Access to PMKeyS Sourced Data through other Applications or Databases

35. PMKeyS data can be provided routinely or adhoc to other Defence and non-Defence applications and databases via interface or extract. To ensure appropriate security and privacy protection of the PMKeyS sourced data the following needs to occur before data will be provided:

- a. any application or database that will store PMKeyS data must undertake analyse from s47E(d) team and be accredited as reliable and trustworthy.
- b. the owners of the other applications and databases are to put in place Data Management Agreements (DMA) and procedures that adhere to Part One of this IS-SPP.

36. The s47E(d) is to ensure that a DMA is completed before PMKeyS data is provided to other Defence and non-Defence applications and databases. The s47E(d) is to ensure that the DMA is distributed and endorsed by other data owners such as the Director s47E(d) and the other system owner(s) as the recipients of the data.

37. For applications and databases outside Defence, s47E(d) is to ensure that a DMA is completed before PMKeyS data is provided to these non-Defence applications and databases.

38. For Defence applications and databases being provided with PMKeyS data through a PMKeyS batch process, s47E(d) is responsible for ensuring appropriate security management is applied. This is required before s47E(d) signs off the s47E(d)

39. For Defence applications and databases being provided with PMKeyS data through a s47E(d) provided extract, s47E(d) is responsible for ensuring appropriate security management is applied.

#### Breaches of Security

40. All breaches of security are to be reported and investigated in accordance with the standards contained in ISM and DSPF. Any attempted or actual breach of PMKeyS security is to be reported to the s47E(d) via email s47E(d)

41. Any user who has access to a Defence/Defence Industry domain or inter-domain connection will be in breach of security if they:

- a. Attempt to access information and/or resources without the required authorisation, clearance, and/or briefing;
- b. Attempt to access information and/or resources, and cannot justify their need for access;
- c. Attempt to circumvent the access mechanisms that have been applied to protect information and/or resources;
- d. Attempt to deny functionality of the system to any other person without prior authorisation;
- e. Attempt to corrupt information that may be of value to Defence;
- f. Do not take reasonable steps to confirm that the information that they originate will be protected;
- g. Extract information from the system and pass it to a person who does not have an established 'Need-to-Know' requirement, or is not authorised to access that information;

- h. Attempt to modify information and/or resources without authority; and
- i. Process information that is classified above the level allowed.

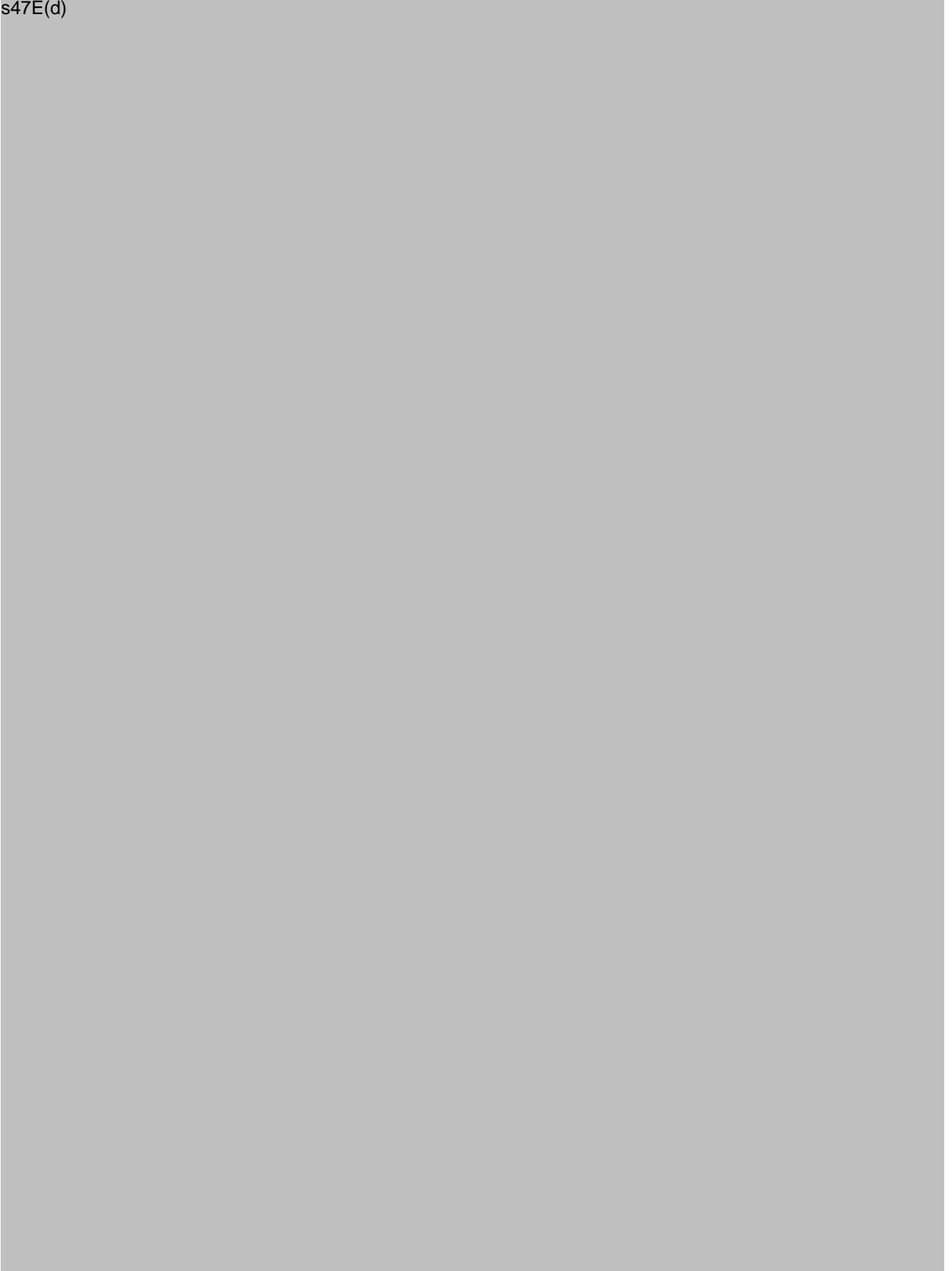
42. The personal information contained within PMKeyS is subject to the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988*. The APPs provide legal direction on the collection, storage, use and disclosure of sensitive and personal data. Please refer to the [Defence Privacy](#) website for further information.

43. Intended, unauthorised, or inappropriate use or disclosure of personal information contained within PMKeyS is an infringement of the *Privacy Act 1988*. It is also a breach of the *Public Service Act 1999* Part 3, Section 13 (the APS Code of Conduct), and the *Defence Force Discipline Act 1982*. Such breaches may result in corrective action taken under the relevant provisions of the *Defence Force Discipline Act 1982*, or the [APS Code of Conduct Procedures](#). Actions may include:

- a. A reprimand;
- b. Removal from part or all of the PMKeyS application;
- c. Reduction in salary by way of a monetary fine;
- d. Reduction in classification;
- e. Termination of service with the Department of Defence; and
- f. Civil charges.

## ANNEX A

s47E(d)





s47E(d)

