



**Australian Government**

---

**Department of Defence**

**ENTERPRISE PROCESS OWNER – PERSONNEL SYSTEMS**

**EPOP-101.1**

**PMKeyS  
INFORMATION SYSTEM  
SECURITY PRACTICES AND PROCEDURES  
(PMKeyS IS-SPP)  
Version 2**

### REVISION HISTORY

<b>Author</b>	<b>Organisation</b>	<b>Date</b>	<b>Version</b>	<b>Comment</b>
Jane Burroughs	DCIO-P	1 August 05	1.6	Changes from ISA review for OHSC.
Noureen Rainsford	PCSC	12 Sept 05	1.6.1	Amendments.
Jane Burroughs / Kim Harrison	DCIO-P	12 Jan 06	1.6.2	Clarification of user access requirements.
Noureen Rainsford/John Crispin	PCSC	31 Jan 06	1.6.3	Update document – Roles of ISSO & Security Manager
Kim Harrison	DCIO-P	15 Feb 06	1.6.4	Updated comments from PCSC.
Phil Walker	DPCSC	10 Mar 06	1.6.5	Updated comments
Kim Harrison	DCIO-P	23 Mar 06	2	Updated to include PCSC comments.

### AUTHORISATION

<b>Document Owner(s):</b>	<b>Version</b>	<b>Date</b>
Director – Domain Chief Information Officer – Personnel Systems (D-DCIOP) on behalf of DGPS	V1.6.1	Original signed 3/3/06
Director – Domain Chief Information Officer – Personnel Systems (D-DCIOP) on behalf of DGPS	V1.5	Original Signed 17/03/05
Director – Domain Chief Information Officer – Personnel Systems (D-DCIOP) on behalf of DGBPMI	V1.0	Original Signed 13/09/02

<b>Business Representative(s):</b>	<b>Version</b>	<b>Date</b>
Director - Occupational Health, Safety & Compensation Management Information (DOHSC MI) On behalf of DGOHSC	V1.5	Original Signed 17/03/05

\* Business Representative authorisations of controlled documents are required when specified by the Document Owner.

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

D-DCIO-P (CP1-7-169)  
Department of Defence  
CANBERRA ACT 2600

# TABLE OF CONTENTS

*Document Owner(s): ..... Error! Bookmark not defined.*  
*Business Representative(s): ..... Error! Bookmark not defined.*

<b>DEFINITION OF TERMS.....</b>	<b>2</b>
<b>PART 1 – GENERAL INFORMATION .....</b>	<b>3</b>
<i>Introduction.....</i>	<i>3</i>
<i>Audience.....</i>	<i>3</i>
<i>Goals.....</i>	<i>3</i>
<i>Objectives.....</i>	<i>3</i>
<i>Scope.....</i>	<i>3</i>
<b>PART 2 – PRACTICES AND PROCEDURES.....</b>	<b>4</b>
<i>General .....</i>	<i>4</i>
<i>Conditions of Access .....</i>	<i>4</i>
<i>Password Management .....</i>	<i>4</i>
<i>User Responsibilities.....</i>	<i>5</i>
<i>Privileged Users.....</i>	<i>5</i>
<i>Special Authoriser.....</i>	<i>6</i>
<i>System Sponsor .....</i>	<i>6</i>
<i>Breaches of Security.....</i>	<i>6</i>
<b>ANNEX A TO THE IS- SPP .....</b>	<b>8</b>
DUTIES OF THE PMKEYS INFORMATION SYSTEM SECURITY OFFICER (PMKEYS ISSO) .....	8
DUTIES OF THE PMKEYS SECURITY MANAGER .....	8

## DEFINITION OF TERMS

**RESTRICTED System High** – The Application has a system security rating of RESTRICTED System High when:

- a. The highest classification of information processed on PMKeyS is RESTRICTED;
- b. Access to an associated Workstation is restricted to users with a minimum security clearance of RESTRICTED; and
- c. Access to PMKeyS is restricted to users who have a need-to-know for that information to which formal access approval has been granted.

**Workstation** - The term Workstation refers not only to the computer unit but to any storage and production media used in conjunction with the unit. This includes media such as floppy disks, removable drives, separate printers and storage containers.

**PMKeyS** – In this document the terms 'PMKeyS' include the HRM PMKeyS Business Application, PMKeyS Self Service (PSS) and Customer Relations Management (CRM) applications e.g. OHS&C module. 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 the IS-SPP directions apply to the entire PMKeyS suite.

# PART 1 – GENERAL INFORMATION

## Introduction

1. Computer security concerns the control of information. Security measures are implemented to ensure information that is stored, processed and transferred is adequately protected according to its sensitivity. The Information System - Security Practices and Procedures (IS-SPPs) are designed for a system security rating of RESTRICTED HIGH and apply to the entire PMKeyS suite.
2. PMKeyS is hosted on the Defence DRN. This IS-SPP does not replace the DRN IS-SPP. Refer to the DRN IS-SPP for a full description of the responsibilities of all users that access the DRN.

## Audience

3. This IS-SPP is to be read prior to all users being granted access to the PMKeyS Business Application and/or the CRM Application. It is a requirement that the IS-SPP is acknowledged as read by all users of PMKeyS every twelve months.

## Goals

4. The goals of this IS-SPP are to:
  - a. Establish a standard set of security policy practices and procedures to be used by all authorised users of PMKeyS.
  - b. Reduce the risk of information loss by accidental or intentional disclosure, destruction or denial of access.
  - c. Maintain the Confidentiality, Integrity and Availability (CIA) of PMKeyS, and
  - d. Ensure all authorised personnel take responsibility for the data they manage/use.

## Objectives

5. To realise these goals, the following objectives must be achieved:
  - a. Prevent unauthorised access, disclosure, modification, manipulation or deletion of PMKeyS data.
  - b. Authentication of PMKeyS users.
  - c. Establish security mechanisms that are flexible and responsive to changes in organisational structures and individual responsibilities.
  - d. Provide the 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 that the system sponsor and/or delegates and authorised users are aware of their respective responsibilities with regard to maintaining the security of information.

## Scope

6. EPOP-101.1 is a 'living' document and its contents will be constantly monitored to ensure it is up-to-date and relevant.
7. The practices and procedures contained in this document are to apply to all data created, processed and stored on PMKeyS.

## PART 2 – PRACTICES AND PROCEDURES

### General

8. PMKeyS has a security rating of RESTRICTED System High. All users must be cleared to RESTRICTED and have a 'need-to-know' for information to which formal access has been approved.

### Conditions of Access

9. Before gaining access to the PMKeyS Business Application and/or the CRM application, personnel must:
- Be granted a security clearance commensurate to the classification of RESTRICTED.
  - Have a 'need to know' the information for the purpose of performing assigned tasks.
  - Have been appropriately assessed for required PMKeyS access and are competent to transact in PMKeyS.
  - Be aware of their responsibilities in using PMKeyS; refer to Part 2 – User Responsibilities.
  - Read and understand this IS-SPP.
  - Sign an '[Application for Access to PMKeyS](#)' form.

10. **Supervisors** are to ensure that personnel requesting access to the PMKeyS Business Application and/or CRM have:

- Applied for the appropriate access and limited to that required to perform their assigned tasks.
- Undertaken the relevant assessment for the PMKeyS Business Application and/or CRM. Assessment is to be for the modules that are relevant to the access requested.
- Read and understood this IS-SPP.

11. Where access is requested to sensitive data such as but not limited to, Career Management, Discipline, Human Resource Budgeting, Drugs and Alcohol and Professional Development and Training, **Special Authorisation** is required before access can be granted.

### Password Management

12. Each user will be issued a user access account. PMKeyS identifies every individual user by a unique user name, which is protected by a password. Users are to change their password during their initial work session. The password protects the user's account from unauthorised use. Passwords are classified as RESTRICTED and are not to be revealed to any other person.

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

- Users are forced to change passwords every 28 days for PMKeyS Business Application and 45 days for PSS and CRM.
- Passwords must be a minimum of eight alpha/numeric characters long.
- Passwords should not to be simple words and must include at least one embedded numeric character.
- The same password cannot be used in any 16 password rotation.
- Users will be locked out after three successive failed logon attempts.

14. The PMKeyS ISSO is to be notified if a user's password is compromised, or suspected of being compromised. The PMKeyS ISSO is to log the details and initiate action for the compromised password to be changed.

15. Automated procedures for deletion of access to PMKeyS are documented in PMKeyS System Management Circular. Refer to [PSMC 3/2005](#) 'PMKeyS Access Automated Procedures Summary.'

16. The PMKeyS Information System Security Officer (PMKeyS ISSO) is responsible for monitoring and auditing the issuing of Operator IDs and passwords to authorised users (for a full description of the duties of the ISSO see [Annex A](#)).

17. For the PMKeyS Business Application, users forgetting their password or have been locked out are to notify the PCSC Security Maintenance Team. Contact e-mail: [pmkeys.password@defence.gov.au](mailto:pmkeys.password@defence.gov.au). Refer to [PSMC 11/2005](#) 'PMKeyS Support Contact Details'.

### **Password Management for PSS**

18. Access to PMKeyS Self Service (PSS) is given to all personnel upon commencement. Users are given a password to use in conjunction with their Employee ID. Users forgetting their password or who have been locked out are to notify the Defence Service Centre on 1800 680 202 and request a password reset for PMKeyS Self Service. For more information refer to [DEFGRAM No 322/2005](#), 'PMKeyS Self Service – Forgotten Password Hints and Automation of Password Resets' and [DEFGRAM No 139/2006](#), 'PMKeyS Self Service – New Arrangements for Password Resets'.

### **User Responsibilities**

19. All users must:

- a. Abide by the policies, practices and procedures set out in this IS-SPP.
- b. Report at once any attempted or actual breach of security to the PMKeyS ISSO. Contact email: [PMKeySSecurityPolicy@defence.gov.au](mailto:PMKeySSecurityPolicy@defence.gov.au)

20. All users are responsible for:

- a. Maintaining the **confidentiality** and **integrity** of information stored on PMKeyS.
- b. Reading and understanding the PMKeyS IS-SPP:
  - (1) prior to granting of access to the PMKeyS Business Application and/or CRM.
  - (2) when notified that amendments have been made.
  - (3) every 12 months.

21. Supervisors are responsible for:

- a. Ensuring that the user has read, understood and complies with the PMKeyS IS-SPP.
- b. The PMKeyS IS-SPP is read every 12 months.

22. 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.

23. All users are to use their account only for specific work related tasks. Unauthorised changes to or creation of PMKeyS accounts are not to be made and will be investigated as a breach.

24. All users, prior to being given access to PMKeyS, shall be made aware of their responsibilities and shall sign a declaration that they accept the above responsibilities. This declaration shall include having filled out and signed a [Request for PMKeyS Access Form](#). This will signify that they have read and understood and accept the terms and conditions set out in this PMKeyS IS-SPP and will entitle them to the status of a PMKeyS user.

### **Privileged Users**

25. The administration of PMKeyS permits certain PMKeyS users to hold accounts that enable a greater level of functionality than is offered by a standard user account. This includes maintenance personnel, security personnel, system administrators, database administrators and users granted with Privileged access as defined in the PMKeyS Production Class documentation. Privileged users have the same responsibilities as a standard PMKeyS user as outlined under User Responsibilities.

26. Privileged user access will be reviewed periodically for compliance confirmation. This can be done by the PMKeyS ISSO as part of the audit process or as required by users or user's supervisor/manager.

27. Privileged users are required to maintain a correction log as documented in PMKeyS System Management Circular. Refer to [PSMC 02/2006](#) 'PMKeyS Correction Mode – Supervisors' Responsibilities'. PMKeyS ISSO and/or their delegates may conduct regular auditing to ensure compliance with Supervisors' responsibilities.

### Special Authoriser

28. Special Authorisers are to ensure that personnel requesting access to PMKeyS have:

- a. Requested the appropriate privileged access to adequately perform their assigned tasks.
- b. Undertaken required PMKeyS assessment, and are competent to transact in PMKeyS.
- c. Read and understood the IS-SPP.

29. 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 CIA of information.

### System Sponsor

30. The System Sponsor delegate (DPCSC), and/or delegate/s are responsible for the following:

- a. Review the PMKeyS IS-SPP ensuring that it continues to comply with the goals and objectives as stated in Part 1 General Information, Goals and Objectives.
- b. Ensure the implementation and sustained compliance of the PMKeyS IS-SPP.
- c. Resolve information system security issues in consultation with the PMKeyS ISSO.
- d. Ensure an ISSO is nominated for the PMKeyS application.
- e. Ensure that the ISSO and Security Manager carry out their duties IAW Annex A.
- f. Ensure that this IS-SPP is available for viewing by all users on PMKeyS by ensuring a current version is located on the PMKeyS Intranet site.

### Breaches of Security

31. All breaches of security are to be reported and investigated in accordance with the standards contained in Defence Security Manual (DSM). Any attempted or actual breach of PMKeyS security is to be reported to the PMKeyS ISSO. Contact email: [PMKeySSecurityPolicy@defence.gov.au](mailto:PMKeySSecurityPolicy@defence.gov.au)

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

- a. Attempts to access information and/or resources without the required authorisation, clearance and/or briefing.
- b. Attempts to access information and/or resources, and can not justify his/her need for access.
- c. Attempts to circumvent the access mechanisms that have been applied to protect information and/or resources.
- d. Attempts to deny functionality of the system to any other person without prior authorisation.
- e. Attempts to corrupt information that may be of value to Defence.
- f. Does not take reasonable steps to confirm that the information that he/she originates will be protected.
- g. Extracts information from the system and passes it to a person who does not have an established need-to-know or is not authorised to access that information.
- h. Attempts to modify information and/or resources without authority.
- i. Processes information that is classified above the level allowed.

33. The Personal Information contained within PMKeyS is subject to [Information Privacy Principle \(IPP\) 10](#) (concerning limits on use of personal information) and [Information Privacy Principle 11](#) (concerning limits on disclosure of information) contained in the *Privacy Act 1988*. (For further information refer to the *Defence Workplace Relations Manual*, Chapter 14, Part 1 'The Privacy Act and Defence' and Chapter 14, Part 2 'Managing Personal Records').

34. Intended unauthorised or inappropriate use or disclosure of personal information contained within PMKeyS is an infringement of IPP 10 and IPP 11. It is also a breach of the Australian Public Service Code of Conduct in

Section 13 of the Public Service Act 1999 and the *Defence Force Discipline Act 1982* (DFDA). Such breaches may result in corrective action taken under the relevant provisions of the DFDA, or the procedures set out in *Defence Workplace Relations Manual*, Chapter 10, Part 2 'Breaches of the Australian Public Service Code of Conduct'. Actions include:

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

## ANNEX A TO THE IS- SPP

### DUTIES OF THE PMKeyS INFORMATION SYSTEM SECURITY OFFICER

1. **The Information System Security Officer** is the PMKeyS Security Policy Manager within PMKeyS Customer Support Centre (PCSC). The PMKeyS ISSO is responsible to the System Sponsor and/or delegate for the following:

- a. Perform administration in support of PMKeyS security and the application of Defence security policy and standards.
- b. Develop and implement PMKeyS security policy in consultation with PMKeyS clients.
- c. Ensuring procedures are in place to grant the appropriate PMKeyS access to personnel based upon the business authorised roles to be performed by the users requesting access.
- d. Maintain and periodically audit a list of all 'Privileged Users'.
- e. Review and contribute to the relevant PMKeyS security training.
- f. Provide an escalation path to enable personnel to bring to notice all suspicious incidents.
- g. Maintain a register of reported fraudulent and security breach incidents and forward to relevant identified authority as required.
- h. Act as the liaison between system personnel and assist in identifying and correcting security deficiencies.

**Note:** A deputy PMKeyS ISSO, the PCSC Assistant PMKeyS Security Policy Manager, has been appointed and is able to perform all of the PMKeyS ISSO duties mentioned above in the absence of the PMKeyS ISSO.

### DUTIES OF THE PMKeyS SECURITY MANAGER

1. **The PMKeyS Security Manager** is the PCSC Assistant Director of Operations and is responsible for the following aspects of the system management in relation to security:

- a. Management of PMKeyS security policy.
- b. Standards compliance is maintained in accordance with the Defence Security Manual,

2. The PMKeyS Security Manager is **not** to be the PMKeyS ISSO.