COMPLIANCE CODE FOR CLASS P2 PERMITS

Compliance Code Version History

Version	Date of Effect	Description
1	30/09/2017	Compliance Code first issue
2		
3		
4		
5		

Purpose

The purpose of this *Compliance Code* is to establish a standard set of requirements for Class P2 permits. It also sets out forms for the submission of applications, notifications and reports.

Scope

This *Compliance Code* applies to permits to possess *associated technology* issued under section 13 of *the Act*, identified under paragraph 3 of the permit as Class P2. The requirements of the *Compliance Code* applies to all *associated technology* in the possession of the Permit Holder.

1. **Objectives**

The Permit Holder shall implement an integrated set of measures to:

1.1. control the access, use and destruction of *associated technology*;

1.2. protect against unauthorised access to, handling or communication of *associated technology*;

1.3. protect against unauthorised removal (theft) of *associated technology*; and

1.4. locate and recover missing *associated technology*.

2. **Procedures**

The Permit Holder shall:

2.1. maintain documented procedures for implementing the objectives and conditions of the Permit and *Compliance Code*;

2.2. ensure that procedures describe, inter alia:

2.2.1. the roles, responsibilities and accountabilities of all personnel required to implement the procedures; and

2.2.2. a description of all security features and provide details of the class of approved containers as defined in the *PSPF*;

2.3. appropriately protect the procedures in accordance with the *PSPF*; and

2.4. review all its procedures for efficiency and effectiveness during the lifetime of this Permit.

3. Accounting and Control System for Associated Technology

The Permit Holder shall:

3.1. identify all locations where *associated technology* on the Permit Holder's *register of associated technology* are located;

3.2. maintain organisational policies and procedures enabling the Permit Holder to determine the precise location of any item on the Permit Holder's *register* in less than 2 hours;

3.3. ensure that the copying or photocopying of any *associated technology* or part thereof is performed only by a person so authorised by the Permit Holder noting that all copies are in itself *associated technology*;

3.4. keep and maintain an up-to-date *register* of *associated technology*, including names and addresses of all persons that handle *associated technology*, recording details of each separate:

3.4.1. receipt of *associated technology*;

3.4.2. transfer of *associated technology*;

3.4.3. copying or photocopying of *associated technology* or part thereof; and

3.4.4. destruction or other form of decrease in the inventory of *associated technology*;

3.5. conduct an audit of the *register* of *associated technology* (stocktake) not more than thirty (30) days prior to and no later than 30 June each year (or other dates as may be designated by *ASNO* in advance), of any *associated technology* or item on the *register*;

3.6. submit *the register of associated technology* as audited by the Permit Holder to the *Director General* for each twelve-monthly period ending 30 June by 15 July of the same year. The register shall include all receipts, transfers, copying, destructions and period-beginning and end-lists; and

3.7. detect any loss of control of *associated technology* on the register within seven days.

4. Protective Security Measures

The Permit Holder shall establish and maintain *protective security* measures to ensure *associated technology* is appropriately secured consistent with guidelines in the *PSPF.* Documents marked with the *DLM* "Sensitive: Associated Technology" and without a security classification, shall be stored and transferred in accordance with Appendix B.

In particular, the Permit Holder shall:

4.1. limit access to those persons having both an appropriate need-to-know within the area and continuous measures to prevent unauthorised access to, or removal of *associated technology*;

4.2. maintain access combination settings of security containers (including vaults and doors with combination locks or access control) in accordance with *PSPF* guidelines including:

4.2.1. limit knowledge of access codes (including combination settings, passwords and personal identification numbers used with swipe cards) to the minimum number required for operational reasons and maintain a list of individuals with knowledge of access codes; and

4.2.2. limit access to keys to the minimum number required for operational reasons (maintain a list of individuals with access to keys) and hold keys in secure storage when not in use commensurate with the level of access the key provides; and

4.3. whenever an approved location is about to be left unattended, check that all *associated technology* and security repositories have been appropriately secured.

5. Compensatory Measures

5.1. Whenever the approved *protective security* system is not providing the required level of protection, the Permit Holder shall promptly implement compensatory measures to provide adequate protection.

5.2. For significant security events, the Permit Holder shall inform *ASNO* of the implementation and removal of compensatory measures.

6. Personnel Security

The Permit Holder shall ensure that individuals granted authorised access to *associated technology*:

6.1. possess the security clearance appropriate to the classification of the information as specified in the *PSPF*;

6.2. have a need-to-know; and

6.3. are appropriately trained in the procedures to fulfil the conditions of this permit.

7. Security of Information and Communications Technology (ICT) System(s)

The Permit Holder shall:

7.1. maintain measures to ensure that *ICT systems* that hold *associated technology* provides adequate protection commensurate with measures specified in the *PSPF, ISM* or Appendix B as appropriate;

7.2. identify and assess the risk of a breach of the *ICT system* integrity through unauthorised access, component failure or loss of access to *associated technology*;

7.3. control and document transfers of *associated technology* onto and from *ICT systems*;

7.4. maintain ongoing physical security of hardware containing or having contained *associated technology* until appropriately disposed of; and

7.5. prohibit offsite access to *ICT systems* containing classified *associated technology*.

8. **Information Classification**

The Permit Holder shall:

8.1. not alter the classification provided by the originator;

8.2. classify copies of *classified information* with the same classification as the original information;

8.3. mark files, binders, folders or groups of physically connected documents as classified at least to the level of the highest *classified information* contained therein; and

8.4. not discard any electronic media that contains or contained *associated technology* through garbage disposal or recycling collection. Such media should be destroyed in accordance with the *PSPF* – Information security management guidelines.

9. **Transport and Electronic Transfer Requirements**

9.1. For transport of *associated technology* within Australia, the transport shall take place accordance with the standards and procedures set out in:

9.1.1. the *PSPF* for *classified information;* or

9.1.2. Appendix B for items marked with the *DLM* "Sensitive: Associated Technology" without a classification;

9.2. Transport may be conducted by the Permit Holder or by couriers approved to deliver classified material by the Commonwealth's Security Construction and Equipment Committee (SCEC) that also holds a permit to transport *associated technology* under section 16 of *the Act.*

9.3. Electronic transfers (e.g. emails) of *associated technology* without a classification (i.e. *DLM* only) may be done with written approval from the *Director General*.

10. **Record Keeping**

The Permit Holder shall retain records pertaining this Permit for at least five years following their last entry to demonstrate compliance. In particular the Permit Holder shall:

10.1. record holdings and transfers of *associated technology*; and

10.2. keep a security incident log.

11. **Reportable Events**

11.1. The following is a list of events reportable to the *Director General* under Form ASO201:

11.1.1. a discrepancy in accounting for the *associated technology* including on *the register* for *associated technology*;

11.1.2. an actual, attempted or suspected:

i. theft, loss or compromise of *associated technology*; or

ii. compromise of system of accounting and control of *associated technology;*

11.1.3. any significant security incident in the form of:

i. a misuse of security-related equipment that may result in a security and/or safety vulnerability;

ii. a credible security threat made against the Permit Holder;

iii. adverse conduct with respect to the operation of the *protective security* system;

iv. adverse failure of the *protective security* system;

v. unauthorised entry to secure area or secure container; or

vi. any confirmed cyber-attack that threatens *protective security* objectives.

11.2. The Permit Holder shall conduct investigations into reportable events and provide a report to the *Director General*, within 30 calendar days of the notification (unless otherwise directed by the *Director General*) of the incident, detailing the actions undertaken in the investigation, findings of the investigation, actions to correct any compromise and actions taken to prevent recurrence of such incidents.

12. **Reports, Notifications and Application for Approvals**

The Permit Holder or d*esignated individual(s)* shall:

12.1. report to, notify or apply to the *Director General* as appropriate for each activity or item listed in the left column of the table in paragraph 13. Each such report, notification or application shall be made using the correctly completed form specified in the right column or using other formats as approved by *ASNO*. The reports, notifications or applications shall be delivered to the *Director General* in accordance with the reporting requirements specified on the relevant form; and

12.2. use the current version of these forms which are available from the *ASNO* website at www.dfat.gov.au/asno or by contacting the *Director General*.

13. ASNO Forms

Forms are reviewed or amended from time to time. Current forms can be downloaded from the *ASNO* website at: www.dfat.gov.au/asno or by contacting the *Director General*.

13.1. Approval Forms:

APPLICATION FORMS TO CONDUCT CERTAIN ACTIONS:[1]	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING:[2]	FORM TO USE:
Application to Create a New Approved Location	7 day notice for nuclear material 20 day notice for associated material	ASO112
A New (or Variation) to a Current Transport Plan		ASO113
Application to Transfer an Associated Item - Import, Export or Domestic Transfer	14 day application approval	ASO115
Application for Authorisation to Access Associated Items		ASO122

13.2. Notification Forms:

NOTIFICATION IS REQUIRED FOR: [1]	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING:[2]	FORM TO USE:
Notification of an Incident	Report *incidents* by phone within 2 hrs. of detection. Submit form within 4 hrs.	ASO201
Notification of Designation of an Individual		ASO214
Notification of Change to Permit Holder's Particulars	Within 10 days of effect of change	ASO231

13.3. Report Forms:

REQUIRED REPORTS:[1]	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING:[2]	FORM TO USE:
Report on Incident Investigation	Within 30 days of initial report	ASO303

[1] Each report, notification or application should be made by the *Permit Holder's representative* or by a *designated individual* as notified under ASO214, responsible for compliance with that application requirement.
[2] Refer to related form for detailed timeframe requirements. All days refer to consecutive business days.

APPENDIX A

18. **Table: Documents Related to Managing Compliance with Conditions in this Permit.**

Document short name	Document full name or description	Date of entry into force or start of application
PSPF	The Protective Security Policy Framework (A suite of documents available at *www.protectivesecurity.gov.au*)	As updated from time to time
PSPF - ISM	The Australian Government Information Security Manual (ISM)	As updated from time to time
PSPF - Physec	Physical Security Management Guidelines - Physical security of ICT equipment, systems and facilities	As updated from time to time
PSPF - Combination settings	Physical security Management Guidelines - Security zones and risk mitigation control measures	As updated from time to time

APPENDIX B

The Permit Holder shall apply the following *protective security* measures for *DLM* with respect to authorised uses in Section 7:

1. Store all *associated technology* in a locked location[1] and within commercial grade security safe or vault[2]
    a. storing all *associated technology* separately from other container contents;
    b. maintaining key/combination control to persons with need-to-know[2];
    c. changing keys/combinations if a compromise of the access is suspected which includes changing key/combination after personnel (with access) termination.
2. Transport *associated technology* in a closed, sealed and opaque package that does not reveals its contents.
3. For *ICT* media, the Permit Holder shall:
    a. mark or label all media and files with appropriate markings as directed by the *ISM* with "Sensitive: Associated Technology";
    b. restrict access to the *associated technology* to persons with established "need-to-know" only;
    c. protect *ICT* information on shared drives by commercial encryption using a passphrase;
    d. provide protective security to all electronic information, copies stored on media including backups and offsite storage; and
    e. not discard any electronic media that contains or contained *associated technology* through garbage disposal or recycling collection and should be destroyed in accordance with the *PSPF* – Information security management guidelines[1].

[1] ISM – Principles – Media Security
[2] PSPF – Physical Security Management Guidelines – Security zones and risk mitigation control measures