# COMPLIANCE CODE FOR CLASS P1 PERMITS

**Compliance Code Version History**

| Version | Date of Effect | Description |
|---|---|---|
| 1 | 18/09/2017 | 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 P1 Permits/ Authorities. 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* and corresponding Authorities to communication information under section 18 of *the Act*, identified under paragraph 3 of the Permit/Authority as Class P1. The requirements of the *Compliance Code* applies to all *associated technology* in the possession of the Permit Holder and to information communicated by the Authority holder.

**Note that the export or communication of *associated technology* overseas from Australia may also require a permit from Defence Export Control**

1. **Determination of Associated Technology**

If the Permit Holder considers that a specification in respect of a Patent application may contain information of a kind referred to in the definition of *associated technology*, the Permit Holder should submit the information to the *Director General* for a determination.

1.1. The Permit Holder may use the list of trigger words listed in Appendix B as a guide to whether an application may contain such information.

1.2. In the interim, while the determination is in progress, the Permit Holder shall:

1.2.1. keep the information strictly in confidence between the Permit Holder, the client and Intellectual Property Australia as relevant; and

1.2.2. store the information in a locked container.

1.3. The remainder of this *Compliance Code* applies if and when a determination as been made that the Permit Holder holds *associated technology*, or when the Authority Holder needs to communicate information of a kind referred to in the definition of *associated technology*.

REFERENCE ONLY

1.4. Should the *Director General* determine that *associated technology* in possession of the Permit Holder is *classified information*, the Permit Holder shall promptly:

1.4.1. return the *associated technology* to the client, *ASNO* or other designated entity nominated by the *Director General*; or

1.4.2. seek an amendment to this Permit and Authority which provides for the security of classified *associated technology*.

## 2. Objectives

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

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

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

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

2.4. locate and recover missing *associated technology*.

## 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. allocate an unclassified item name to each associated item for reference in records, applications, notifications and reports;

3.3. mark all *associated technology*, clearly with its item name, top and bottom of each page[1], with *DLM* "Sensitive: Associated Technology" if not already so marked;

3.4. similarly mark files, binders, folders or groups of physically connected documents with the *DLM* "Sensitive: Associated Technology";

3.5. 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;

3.6. ensure that the copying (including of electronic files and media) 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;*

3.7. ensure that destruction of *associated technology* ensures complete destruction of the information that they contain, such that recognition, reconstruction or recovery of the *associated technology* is precluded;

3.8. keep and maintain an up-to-date *register* of *associated technology* which records the details of the following:

3.8.1. list of all *associated technology* held at the end of the previous reporting period;

[1] PSPF – Information security management guidelines – Protective marking and handling sensitive and security classified information

REFERENCE ONLY

3.8.2. receipt of *associated technology*, including:

i. date of receipt;

ii. name and address of the supplier;

iii. item description and identification; and

iv. overseas obligation(s), if any, under which the *associated technology* was supplied, i.e. obligation(s) arising as a result of the associated item having been supplied to Australia subject to a *prescribed international agreement*;

3.8.3. transfer of *associated technology*, including:

i. date of transfer;

ii. name and address of the transferee/recipient;

iii. item description and identification; and

iv. overseas obligation(s), if any, under which the *associated item* was supplied, and methods of transfer, including the carrier's name and address if applicable;

3.8.4. copying (including electronic files and media) or photocopying of *associated item* or part thereof, including:

i. date of copying or photocopying;

ii. name and position of the person performing the copying or photocopying;

iii. description and identification of item or part thereof copied or photocopied; and

iv. number of copies or photocopies made, and identification given to each copy or photocopy; and

3.8.5. destruction or other form of decrease in the inventory of *associated technology,* including date and details of decrease in the inventory;

3.9. 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*;

3.10. 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 period-end lists;

3.11. detect any *loss of control* of *associated technology* listed on *the register* within seven days; and

3.12. maintain a separate ledger which records details of each separate external communication of *classified information*, including:

3.12.1. date of communication;

REFERENCE ONLY

3.12.2. description and identification of the information, and form in which it is communicated;

3.12.3. method of communication;

3.12.4. name(s), address and business or profession of the person(s) to whom the information is communicated; and

3.12.5. reason for communication.

## 4. Personnel Security

The Permit Holder shall:

4.1. limit access to *associated technology* to those persons:

4.1.1. having an established need-to-know;

4.1.2. have undergone trustworthiness checking[1];

4.1.3. authorised through form ASO122; and

4.1.4. are appropriately trained in the procedures to fulfil the conditions of this Permit;

4.2. recover *associated technology* from individuals who no longer require access to such information or whose access authorisation has been revoked; and

4.3. under the authority to communicate information, inform the receiver of the information, prior to the information being communicated, of all the obligations attached to the information.

## 5. Protective Security Measures

The Permit Holder shall establish and maintain the following *protective security* measures to ensure *associated technology* is appropriately secured in use, storage or transport:

5.1. store all *associated technology* in a locked location[2] and within commercial grade security safe or vault[2]:

5.1.1. storing all *associated technology* separately from other contents in the safe or vault;

5.1.2. maintaining key/combination control to persons established by paragraph 4.1; and

5.1.3. changing keys/combinations if a compromise of the access is suspected which includes changing key/combination after personnel (with access) termination;

5.2. ensure that all *associated technology*, including drafts, are not left unattended or unsecured at any time;

5.3. whenever an Approved Location is to be left unattended (e.g. end of day), check that all *associated technology* and security repositories have been appropriately secured; and

[1] PSPF – Personnel Security Guidelines – Agency personnel security responsibilities.
[2] PSPF – Physical Security Management Guidelines – Security zones and risk mitigation control measures.

REFERENCE ONLY

5.4. transport *associated items*:

5.4.1. only by persons established by paragraph 4.1 or using a carrier holding an appropriate Permit to transport *associated items* under Section 16 of *the Act*; and

5.4.2. in a closed and sealed opaque package.

6. **Security of Information and Communications Technology (ICT) Media**

For *associated technology* stored or transmitted electronically, the Permit Holder shall:

6.1. mark or label all media and files with appropriate markings as directed by the ISM[1] with "Sensitive: Associated Technology";

6.2. mark email subject and body with "Sensitive: Associated Technology"

6.3. restrict access to the *associated technology* on *ICT* media to persons with established by paragraph 4.1;

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

6.5. protect *ICT* information on shared drives by commercial encryption using a passphrase;

6.6. provide *protective security* to all electronic information, copies stored on media including backups and offsite storage, consistent with that specified in paragraph 5; and

6.7. 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.

7. **Communication, Transfer or Transport of Associated Technology outside of Australia**

The Permit Holder shall not communicate, transfer or transport *associated technology* outside Australia unless:

7.1. where the *associated technology* is of Australian origin or has been supplied to Australia subject to a *prescribed international agreement*, the *Director General* has given written permission for the communication or transfer (refer ASO125);

7.2. the proposed recipient of the *associated technology* is a foreign Patent Attorney or a foreign Patent Office from time to time approved by the *Director General*, or is a foreign client provided that the *associated technology* to be communicated or transferred is the property of that client;

7.3. the communication or transfer is for the purpose of securing a patent grant in Australia or elsewhere in accordance with the instructions of the relevant client or for the purpose of advising a client on patent-related matters; and

7.4. the communication or transfer is conducted by secure means approved by the *Director General.*

[1] Australian Government Information Security Manual – Principles – Media Security

REFERENCE ONLY

8. **Record Keeping**

The Permit Holder shall retain records for at least five years following their last entry to demonstrate compliance with the conditions of this Permit and Authority.

9. **Reportable Events**

9.1. The following is a list of events involving *loss of control* reportable to the *Director General* under Form ASO201:

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

9.1.2. an actual, attempted or suspected:

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

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

iii. unauthorised communication of *associated technology*;

9.1.3. 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; and

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

9.2. 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.

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

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

10.1. 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 11. 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

10.2. 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*.

REFERENCE ONLY

## 11. 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*.

### 11.1. 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 | 20 day notice for associated technology | 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 |
| Application to Approve a person to Receive Information | 5 day application approval | ASO125 |

### 11.2. 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 |

### 11.3. 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 |

REFERENCE ONLY

[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 - ISM | Principles – Media Security | As updated from time to time |
| PSPF – Information marking | Information security management guidelines – Protective marking and handling sensitive and security classified information | 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 |

REFERENCE ONLY

## APPENDIX B

19. **List of Trigger Words**

This list of trigger words can be used as a guide to ascertain the potential for information in a document to be *associated technology* noting that the presence of one or more words does not necessarily indicate it will be *associated technology* and the absence any trigger words does not guarantee that the information is not *associated technology*.

| | | | |
|---|---|---|---|
| Trigger words relating to **enrichment of nuclear material** | | | |
| *Redacted section* | | | |
| Trigger words relating to **reprocessing of irradiated nuclear material** | | | |
| *Redacted section* | | | |
| Trigger words relating to **production of heavy water** | | | |
| *Redacted section* | | | |

REFERENCE ONLY