Rapid Prototyping, Development and Evaluation Program

2016 Relationship Agreement

Schedule 3

Part 2 – Defence Security Requirements Policy

Version 1.0

Approved By M. Hufield.

This Policy may be amended from time to time by the Commonwealth Board Member

Change History

VERSION	DATE	DESCRIPTION OF CHANGE
1.0		Initial document

Table of Contents

1. REFERENCES

A. RPDE 2016 Relationship Agreement and Standing Offer

B. Defence Security Manual (DSM)

C. Australian Protective Security Policy Framework (PSPF)

D. Information Security Manual (ISM)

2. INTRODUCTION

2.1. Purpose

This Policy contains provisions setting out the manner in which the Commonwealth and the Members of the Program have agreed to consistently apply security measures across RPDE.

2.2. Objectives

The objectives of the Defence Security Requirements Policy is to provide guidance to Members on:

(a) the application of the DSM in RPDE;

(b) the application of the ISM in RPDE; and

(c) compliance with the PSPF in RPDE

to ensure all RPDE personnel comply with relevant Departmental policies.

3. DEFINITIONS

TERM OR ABBREVIATION	MEANING
Contractor	means Contractors under a Services Contract
Member	means a member of the Program in accordance with the Relationship Agreement.
Personnel	of a Member includes that Members employees and contractors or consultants.
Policy	means any policy or policies relating to the operation of the RPDE Program endorsed by the Board from time to time.
Relationship Agreement	means the deed titled '2016 Relationship Agreement' (including and schedule or annexure to the deed) as amended from time to time.
Standing Offer	means the deed of standing offer as agreed and executed by the Commonwealth and each Member setting out the terms on which Services will be provided.

4. BACKGROUND

4.1. The DSM details the standards, processes and procedures that direct the application of protective security measures by Defence personnel and external service providers (Contractors) to ensure Defence's compliance with legislation and Australian Government Policy. It establishes best practice for the protection of people, information, capabilities, bases and facilities and, ultimately, Defence's ability to function in support of Government.

4.2. Defence must comply with the Australian Protective Security Policy Framework (PSPF) and the Australian Government Information Security Manual (ISM), and the DSM references these mandatory Commonwealth policies, principles, standards and procedures.

4.3. The PSPF has been developed to ensure there is consistent application of security measures across all areas of the Australian Government.

5. ACCESS

5.1. Where a Member requires access to any Commonwealth premises, the Member agrees to:

(a) comply with any security requirements notified to the Member by the Commonwealth from time to time or contained within the RDPE Policies; and

(b) ensure that any of its Personnel or sub-contractors are aware of the Commonwealth's security requirements and comply with those requirements.

6. MEMBER RESPONSIBILITIES

6.1. The Member will, and will arrange with any of its Personnel or sub-contractors involved in the provision of Services to:

(a) agree to and co-operate with any security checks or clearances as required by the Commonwealth;

(b) notify the Commonwealth of any changes to circumstances which may affect the Member's capacity to provide Services in accordance with the Commonwealth's security requirements; and

(c) provide any written undertakings in respect of security or access to the Commonwealth in the form required by the Commonwealth.

7. SECURITY OF INFORMATION

7.1. The security classification of work to be performed under a Services Contract will be up to and including TOP SECRET/ SECRET level. The Member will comply with the requirements of Defence industrial security policy and will ensure that all its sub-contractors, officers, employees and agents who have access to classified information in any form possess an appropriate security clearance.

7.2. The Member will ensure that where necessary to complete a Services Contract:

(a) it will maintain a facility and/or storage; and

(b) where a sub-contractor is required to have access to security classified information, the sub-contractor possesses a Defence Industry Security Program accredited facility,

7.3. Without limiting clause 20 of the Relationship Agreement a Member agrees not to release any security classified information furnished or generated under a Services Contract to a third party, including a representative of another country, without prior written approval of the originator through the Commonwealth.

7.4. All security classified information transmitted between the Members or a Member and a sub-contractor, in Australia, whether generated in Australia or overseas, will be subject to the provisions of the Defence industrial security policy.

8. TRANSMISSION OF INFORMATION

8.1. All security classified information transmitted between the Members or a Member and a sub-contractor overseas, whether generated in Australia or overseas, will be subject to the laws of the overseas country regarding the custody and protection of security classified information, and to any bilateral security instrument between Australia and the overseas country.

9. REPORTING LOST OR INCORRECTLY DISCLOSED INFORMATION

9.1. A Member will promptly report to the Defence Security Authority through the RPDE Security Manager any instance in which it is known or suspected that security classified information furnished or generated under this Agreement, its Standing Offer or any Services Contract has been lost or disclosed to unauthorised parties, including a representative of another country.

10. FACILITY SECURITY

10.1. Each Member agrees to ensure that, where a sub-contractor is required to have access to security classified information, the sub-contractor possesses a facility security clearance of the appropriate type and level of security classification, issued by the Defence Security Authority in the case of an Australian based sub-contractor or the relevant government industrial security authority in the case of an overseas based sub-contractor where Australia has a bilateral security agreement in place.

11. COMPLIANCE

11.1. Each Member must ensure the requirements of this Policy, are included in all sub-contracts where the sub-contractor requires access to security classified information in order to perform Services under a Services Contract.

11.2. The Commonwealth may take any action necessary against a Member to assure or enforce compliance with this Policy.

12. INFORMATION SECURITY

12.1. The appropriate Australian Government Security Classification is to be used when the document contains classified information. The following principles of good information security practice are applied to this dissemination limiting marker:

(a) information can only be released to organisations and individuals with a demonstrated need to know

(b) information is stored and processed away from public access

(c) the removal of information from agency premises is on the basis of identified need

(d) disposal of information is by secure means

(e) transmission and transfer of information is by appropriate means.

13. FURTHER INFORMATION AND GUIDANCE

13.1. The RPDE Security Manager is the first point of contact for all security related matters.