Australian Government
Digital Transformation Agency

Protective Security Requirements

Trusted Digital Identity Framework
March 2019, version 1.4

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au).

Conventions

TDIF documents refenced by this document are denoted in italics. For example, *TDIF: Overview and Glossary* is a reference to the TDIF document titled Overview and Glossary.

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *TDIF: Overview and Glossary.*

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties accessing this document or have questions or comments regarding this document please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document Management

The TDIF Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.01	Sept 2017	SJP	Initial version.
0.02	Jan 2018	SJP	Incorporates feedback from stakeholders and public consultation and merged the *Core Protective Security Requirements* and *Information Security Documentation Guide* into the one document.
1.0	Feb 2018		Endorsed for release by the TDIF Accreditation Authority.
1.1	Oct 2018	SJP	Minor content updates.
1.2	Dec 2018	SJP	Updated to align with the 2018 edition of the PSPF and ISM.
1.3	Jan 2019	SJP	Incorporated feedback from stakeholders.
1.4	Mar 2019	SJP	Incorporated feedback from public consultation.

Contents

1 Introduction

Agencies and organisations that apply to be accredited under the TDIF undergo a series of rigorous evaluations across all aspects of their identity service operations. The *TDIF: Accreditation Process* requires Applicants to demonstrate their identity service is usable, privacy enhancing and is secure and resilient to cyber threats. The intent of these evaluations is to determine whether the Applicant's identity service meets the TDIF Guiding Principles[1] and whether it is suitable to join the identity federation.

This document defines the minimum protective security requirements that the Applicant's identity service is required to meet to the satisfaction of the TDIF Accreditation Authority. The requirements listed in this document do not replace, remove or diminish existing government agency or organisation obligations for cyber security or risk management. Rather, they supplement existing obligations and apply specifically to identity services that undergo the *TDIF: Accreditation Process*. Applicants that are state government agencies are advised to consult relevant protective security state regulators (where available) prior to undergoing TDIF accreditation.

In accordance with their business needs and threat environment, Applicants can seek exemptions for requirements listed in this document. Further information on exemptions is outlined in the *TDIF: Accreditation Process*.

A number of requirements listed in this document align with cyber security advice, guidance, policies and publications developed by the Australian Government. This includes the current edition of the Protective Security Policy Framework (PSPF) developed by the Attorney-General's Department, and the Information Security Manual (ISM), developed by the Australian Cyber Security Centre (ACSC).

Security requirements listed in this document which have been derived from the PSPF or ISM are denoted with specific references to controls listed in those documents (e.g. ISM control: 0123; PSPF control: INFOSEC-10). Controls denoted with 'PROTSEC-x' indicates a protective security requirement derived from other government policy or the TDIF. Regardless of the source, the Applicant is required to meet all requirements listed in this document.

[1] See *TDIF: Overview and Glossary* for further information on the TDIF guiding principles.

References to specific PSPF or ISM controls that are applicable to an agency are to be interpreted as being applicable to the Applicant. Applicable ISM controls with a priority of 'should' are to be interpreted in this document as **MUST**. The scope of such controls are limited to the identity service being accredited and not to the Applicant's wider operating environment.

The current edition of the ISM states[2] 'organisations that do not handle government information can implement security controls marked as 'OFFICIAL' for a baseline level of protection, or those marked as 'PROTECTED' for an increased level of protection'[3]. Consistent with this risk-based approach, the requirements listed in this document include relevant ISM controls marked as 'OFFICIAL' and 'PROTECTED' that the Applicant is required to meet.

If there is conflict between:

- Any requirement listed in this document and the current edition of the PSPF, then the PSPF takes precedence.
- Any requirement listed in this document and the current edition of the ISM, then the ISM takes precedence.

The intended audience for this document includes:

- Applicants and Accredited Providers.
- Security assessors and practitioners
- Australian Cyber Security Centre (ACSC)
- Australian Signals Directorate (ASD).
- Relying Parties.
- TDIF Accreditation Authority.

[2] page 7 in the section titled 'applicability of security controls'.

[3] These applicability markings are based on the protective markings described in the PSPF

2 Protective security requirements

2.1 Requirements for cyber security roles

Objective: The Applicant demonstrates their ongoing support for and commitment to protective security governance.

Chief Information Security Officer

Applicable ISM controls: 0714, 1478.

System ownership

Applicable ISM controls: 1071, 0027, 1526.

Responsibilities

Applicable ISM controls: 1525, 0027, 1526.

2.2 Requirements for authorising systems

Objective: The Applicant performs internal system certification and accreditation of its identity service as part of initial accreditation, annual compliance audits and re-accreditation).

Conducting internal accreditations and certifications

PROTSEC-1: the Applicant **MUST** undergo the following security evaluations[4] as part of the TDIF Accreditation Process:

- An independent IRAP assessment by an approved IRAP Assessor.
- An independent penetration test.

Applicable PSPF controls: INFOSEC-11.
Applicable ISM controls: 0064, 0809, 0904, 1531, 0805, 1140.

[4] See *Trust Framework: Protective Security Reviews* for further information

2.3 Requirements for cyber security incidents

Objective: Key technical measures and appropriate procedures are in place to mitigate, detect, respond to and manage cyber security incidents which may impact the Applicant's identity service.

Detecting cyber security incidents

Applicable ISM controls: 0120.

Managing cyber security incidents

Applicable ISM controls: 0122, 0125, 0133, 0917, 0137, 1213, 0138.

Reporting cyber security incidents

Applicable ISM controls: 0123, 0141, 0140.

2.4 Requirements for outsourcing

Objective: The Applicant's use of third parties for security functions does not transfer security accountability for the protective security management responsibilities of the Applicant to the third party.

Applicable PSPF controls: GOVSEC-06.
Applicable ISM controls: 0873, 0072, 1073, 1451, 1452.

2.5 Requirements for security documentation

Objective: The Applicant maintains appropriate protective security documentation for their identity service.

Development and management of documentation

Applicable ISM controls: 0047, 0888.

System-specific documentation

PROTSEC-2: The Applicant **MUST** consider the potential sources of risk listed in Annex A of the *TDIF: Risk Management Requirements* as part of their risk management process.

PROTSEC-3: The Applicant **MUST** maintain a disaster recovery and business continuity plan which adequately covers their identity service. The plan is required to cover business continuity governance, training requirements for recovery team members, recovery objectives and priorities, continuity strategies, testing requirements and restoration procedures.

PROTSEC-4: The Applicant **MUST** maintain a cryptographic key management plan which identifies the implementation, standards, procedures and methods used by the identity service for key management. The plan is required to cover cryptographic key lifecycle management, how records will be maintained and audited, the conditions under which compromised keys will be declared, maintenance of cryptographic components, evidence of cryptographic evaluations undertaken.

Applicable PSPF controls: GOVSEC-03.
Applicable ISM controls: 0041, 0042, 0043.

2.6 Requirements for physical security

Objective: Physical security measures are applied to facilities and network infrastructure to protect the Applicant's identity service.

Physical security measures are applied to facilities and network infrastructure to protect identity services.

Facilities and systems

Applicable PSPF controls: PHYSEC-15.
Applicable ISM controls: 1053, 1530, 0813, 1074, 0157, 1296, 0164.

ICT equipment and media

Applicable ISM controls: 0336, 0159, 0161.

2.7 Requirements for personnel security

Objective: Only appropriately screened and authorised personnel are allowed to access and operate the Applicant's identity service.

Cyber security awareness raising and training

Applicable ISM controls: 0252, 0432.

Access to systems and their resources

PROTSEC-5: Information that is generated, accessed, handled or exchanged by the Applicant's staff or identity service **MUST** occur in a legal, controlled and accountable manner.

Applicable PSPF controls: INFOSEC-10, PERSEC-12
Applicable ISM controls: 0434, 0435, 0405, 1503, 1507, 1508, 0445, 1509, 1175, 0430, 1404, 0407, 0441.

2.8 Requirements for evaluated products

Objective: The Applicant uses cryptographic products that have been evaluated through an ASD approved program.

Evaluated product acquisition

Applicable ISM controls: 0280, 0285.

Evaluated product usage

Applicable ISM controls: 0289.

2.9 Requirements for ICT equipment management

Objective: The Applicant's ICT equipment is appropriately handled and protected.

ICT equipment usage

Applicable ISM controls: 0293.

ICT equipment maintenance and repairs

Applicable ISM controls: 0310, 0944.

ICT equipment sanitisation and disposal

Applicable ISM controls: 0313, 0311, 1223.

2.10 Requirements for media management

Objective: Media used by the Applicant is appropriately handled and protected.

Media usage

Applicable ISM controls: 1359, 0323, 0325, 0332, 0337, 0341, 0342, 0343, 0345, 0831, 1059, 0347, 0338.

Media sanitisation

Applicable ISM controls: 0348, 0947, 1464.

Media destruction

Applicable ISM controls: 0363, 0350, 0370, 0371.

Media disposal

Applicable ISM controls: 0374, 0378.

2.11 Requirements for system hardening

Objective: The Applicant's identity service is sufficiently hardened.

Operating system hardening

Applicable PSPF controls: INFOSEC-10.
Applicable ISM controls: 1407, 1408, 0383, 0380, 1491, 1410, 1469, 0382, 0843, 1490, 0846, 0955, 1471, 1392, 0957, 1414, 1492, 1341, 1034, 1416, 1417, 1418.

Application hardening

Applicable ISM controls: 1484, 1486, 1470.

System access

Applicable ISM controls: 0414, 0415, 0417, 0421, 0423, 1426, 1173, 1504, 1505, 1401, 1055, 1403, 0431, 0976, 1227, 0418, 1402, 0428, 0408.

2.12 Requirements for system management

Objective: The Applicant's identity service remains resilient in the face of targeted cyber intrusions.

System administration

Applicable ISM controls: 1380, 1382, 1381, 1383, 1384, 1385, 1386, 1387, 1388.

System patching

Applicable PSPF controls: INFOSEC-10.
Applicable ISM controls: 1143, 1144, 0940, 1472, 1494, 1495, 1496, 0303, 1497, 1499, 1500, 0304, 1501.

Change management

Applicable ISM controls: 1211, 0115.

Data backups

Applicable ISM controls: 1510, 1511, 1512, 1513, 1514, 1515, 1516.

2.13 Requirements for system monitoring

Objective: The Applicant can ensure the accountability of all user actions on their identity service and improve their changes of detecting malicious behaviour.

Event logging and auditing

Applicable PSPF controls: INFOSEC-11.

Applicable ISM controls: 0580, 1405, 0988, 0584, 0582, 1536, 1537, 0585, 0586, 0859, 0991, 0109, 1228.

Vulnerability management

Applicable ISM controls: 1163, 0911.

2.14 Requirements for software development

Objective: The confidentiality, integrity and availability of information processed by the Applicant's identity service are protected.

Application development

Applicable PSPF controls: INFOSEC-11.

Applicable ISM controls: 0400, 1419, 1420, 1422, 1238, 0401, 0402.

Web application development

Applicable ISM controls: 1239, 1240, 1241, 1424, 0971.

2.15 Requirements for database system management

Objective: The confidentiality, integrity and availability of the Applicant's database systems are sufficiently protected.

Database servers

Applicable ISM controls: 1425, 1269, 1277, 1270, 1271, 1272, 1273.

Database management system software

Applicable ISM controls: 1246, 1247, 1249, 1250, 1260, 1262, 1263.

Databases

Applicable ISM controls: 1243, 1256, 1252, 0393, 1255, 1268, 1258, 1274, 1275, 1278.

2.16 Requirements for email management

Objective: The confidentiality, integrity and availability of the Applicant's email systems are sufficiently protected.

Email infrastructure

Applicable ISM controls: 0572.

2.17 Requirements for network management

Objective: The confidentiality, integrity and availability of the Applicant's networks are sufficiently protected.

Network design and configuration

Applicable ISM controls: 0516, 0518, 1178, 1181, 0520, 1427, 1304, 0534, 1460, 1461, 1006, 1311, 0576, 1185.

Service continuity for online services

Applicable ISM controls: 1458, 1431, 1432, 1433, 1434, 1435, 1436.

2.18 Requirements for using cryptography

Objective: The Applicant only uses ASD approved cryptographic algorithms and protocols.

Cryptographic fundamentals

Applicable ISM controls: 1161, 0459, 0455, 0462, 1162.

ASD Approved Cryptographic Algorithms

Applicable ISM controls: 0471, 0472, 0473, 1446, 0474, 0475, 0476, 0477, 0479, 0480.

ASD Approved Cryptographic Protocols

Applicable ISM controls: 0481.

Transport Layer Security

Applicable ISM controls: 1371, 1373, 1374, 1375.

Secure Shell

Applicable ISM controls: 1506, 0484, 0485, 1449, 0487, 0489.

Internet Protocol Security

Applicable ISM controls: 0494, 0496, 1233, 0998.

Cryptographic system management

Applicable ISM controls: 0142, 1091, 0505.

2.19 Requirements for connecting networks and security domains

Objective: Where an Applicant connects to another government agency or organisation, they implement a firewall to protect them self from intrusions that originate outside of their environment.

Firewalls

Applicable ISM controls: 1527, 1193.

2.20 Requirements for data transfers and content filtering

Objective: Content filters used by the Applicant are appropriately configured, handled and protected.

Content filtering

Applicable ISM controls: 0651, 0652.