Australian Government
Digital Transformation Agency

Protective Security Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

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)

Contact us

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

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

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 by the Commonwealth GovPass Authority

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **SHOULD** – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

Applicants undergo rigorous evaluations of all aspects of their identity service operations, including compliance with applicable Unclassified Australian Government protective security requirements as outlined in the current editions of the PSPF and ISM. In support of these compliance obligations, these Protective Security Requirements define the minimum protective security controls that agencies and organisations that apply for TDIF accreditation are required to implement for their identity services.

This document includes two parts:

- Part one: defines the protective security roles, responsibilities and documentation that Applicants are required to implement in order to secure their identity service, and
- Part two: lists the protective security documents and recommended content to be developed by Applicants to satisfy the documentation requirements of part one.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

Note:
Government agencies that comply with ISM and PSPF controls can, where appropriate, and in accordance with their business needs, threat environment

and risk appetite, seek waivers for Non Compliance against ISM or PSPF controls. In these scenarios Non Compliance is formally accepted by the agency's appropriate authority.

Government agencies that have been granted waivers for Non Compliance against ISM or PSPF controls that apply for accreditation under the Trust Framework **will not** have these waivers automatically recognised by the Trust Framework Accreditation Authority.

Applicants that have been granted waivers against ISM or PSPF controls are required to provide this information to the Trust Framework Accreditation Authority during the initial step of the Trust Framework Accreditation Process.

With due consideration of:

- These Protective Security Requirements.
- The waivers.
- The Applicant's business needs, threat environment and risk appetite.
- The cost of implementing and maintaining ISM and PSPF controls vs derived security benefit.
- Any alternative or supplementary controls implemented for the identity service.
- The maturity of the identity service.
- Perceived risks to the broader identity federation.

The Trust Framework Accreditation Authority may, at its sole discretion either accept or reject the waivers for the purpose of Trust Framework accreditation.

2 Part one: Protective security requirements

This document includes Protective Security Requirements and applicable Unclassified ISM controls the Applicant **MUST** implement for their identity service to the satisfaction of the Trust Framework Accreditation Authority[2].

These requirements cover the following protective security domains:

- Protective security governance, including:
  - Governance.
  - Internal system accreditation.
  - Compliance with legal requirements.
- Threat and risk management.
- Protective security roles and responsibilities.
- Protective security awareness training.
- Protective security documentation.
- Access security.
  - Internal system user access security.
- Communications and operations management, including:
  - Service continuity for identity services.
  - Network security and management.
  - Continuous monitoring and event logging.
  - Operating system and system file security.
  - Database security.
  - ICT asset handling and protection.
  - Mobile computing.
- Cryptography, including:
  - Using approved cryptographic algorithms, protocols and modules.
- Cyber security incident response management:
- Strategies to mitigate cyber security incidents.
- Physical and environmental security.
- Information classification and handling, including:

[2] For the purpose of this document, any ISM control applicable to an agency is to be read as being applicable to the Applicant. The scope of such controls are limited to the identity service being accredited and not to the wider ICT environment of the Applicants agency or organisation.

    - Exchange of information.
- Personnel security.
- Acquisition, development and maintenance, including:
    - ICT security product assurance.
    - Change management.
    - Protective security reviews.

2.1 Protective security governance

Objective: Applicants establish protective security governance processes and demonstrate their ongoing support for and commitment to protective security governance for their identity service.

2.1.1 Governance

The Applicant **MUST** establish a framework for governance and oversight of control of the protective security implementation for their identity service.

The use of third parties for security functions by the Applicant does not transfer security accountability or the protective security management responsibilities of the Applicant to the third party. The Applicant's Information Technology Security Officer or an equivalent position **MUST** monitor any outsourced security arrangements.

The Applicant **MUST** include conditions in relevant contracts that require a contracted third party to delete all of the Applicant's information (including all personal information) from its ICT systems at the completion or termination of the contract.

Applicable ISM controls: 1395, 0873, 1073.

2.1.2 Internal system accreditation

The Applicant **MUST** have a system owner who is responsible for the operation of their identity service.

Applicable ISM controls: 1072, 0791, 0027, 0797, 1141, 0902, 0805, 1140, 1142, 0808, 0064, 0070.

2.1.3 Compliance with legal requirements

The Applicant **MUST** implement procedures to monitor and maintain compliance to applicable statutory, regulatory and contractual security requirements for their identity service.

The Accredited Provider **MUST** undergoing an annual Trust Framework compliance assessment. Further details are available in the *Trust Framework: Annual Review.*

2.2 Threat and risk management

Objective: Applicants select and implement information security controls to mitigate credible, likely and realistic protective security threats and risks that may impact their identity service.

The Applicant **MUST** implement a risk management framework and risk management process consistent with the *Trust Framework: Risk Management Requirements* which covers Applicant-specific and shared risks.

The Applicant **MUST** establish a procedure to regularly assess risks arising from published technical vulnerabilities and bulletins or other notifications about known or emerging threats to information assets.

The Applicant **MUST** enact preventative measures to reduce and/or eliminate vulnerabilities and threats to their identity service.

If the Applicant contracts a third party to provide a protective security capability, the Applicant **MUST** consider the impact of any loss or compromise of personal information held by the third party, especially aggregated personal information, and include conditions in the contract to mitigate any assessed risks.

Applicable ISM controls: 1203, 1204, 1205, 1206, 1207, 1208.

2.3 Protective security roles and responsibilities

Objective: Applicants appoint and maintain key protective security roles within their organisation which cover the operation of their identity service.

The Applicant **MUST** at a minimum, maintain the following key protective security roles within their organisation:

- Information Technology Security Manager (ITSM), or an equivalent position responsible for the oversight of protective security practices for the identity service.
- Information Technology Security Officer (ITSO), Advisor (ITSA) or an equivalent position responsible for:
    - The day-to-day performance of protective security functions.
    - To administer and configure a broad range of physical and logical security systems.
    - To analyse and report on protective security issues.
    - Advise senior management on the security of the Applicant's identity service.
- System administrators, responsible for the day to day administration of the identity service.
- Internal system users, responsible for the day to day operation of the identity service.

Part two of this document includes recommended procedures to be included for these protective security roles.

The Applicant **MUST** ensure that all protective security responsibilities are clearly defined.

The Applicant **MUST** ensure the protective security roles have a detailed knowledge of protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.

Applicable ISM controls: 0741, 0768.

2.4 Protective security awareness and training

Objective: A security culture is fostered through continual protective security awareness and training tailored to specific identity service roles and responsibilities.

The Applicant **MUST** provide protective security awareness training upon appointment and annually for personnel who operate or maintain the identity service. Training **MUST** cover topics such as responsibilities, consequences of noncompliance, and potential security risks and countermeasures.

The Applicant **SHOULD** ensure that security personnel are familiar with information security roles and services provided by Australian Government agencies.

Applicable ISM controls: 0252, 0253, 0255, 0922.

2.5 Protective security documentation

Objective: Applicants produce protective security documentation for their identity service.

The Applicant **MUST** at a minimum, implement the following protective security documentation for their identity service:

- Information Security Policy.
- Security Risk Management Plan.
- Vulnerability Management Plan.
- Incident Response Plan.
- Physical and Environmental Security Plan.
- System Security Plan.
- Standard Operating Procedures.
- Personnel Security Plan.
- Disaster Recovery and Business Continuity Plan.
- Emergency Response Management Procedures.
- Cryptographic Key Management Plan.

Applicable ISM controls: 0886, 0044, 0787, 0885, 0046, 0047, 0887, 0888, 1154, 0039, 0049, 0890, 0040, 0809, 1163, 0909, 0911, 0112, 0113, 0043, 0058, 0041, 0895, 0067, 0051, 0789, 0056, 0057, 0913, 0914, 0062, 1159, 0510, 0511.

Part two of this document includes recommended structure and content to be included for each protective security document.

2.6 Access security

Objective: Access to the Applicant's identity service, underlying business processes and the information they process, store or communicate is controlled through strong user identification and authentication practices.

2.6.1 Internal system user access security

The Applicant **MUST** establish and frequently review controls for access to the identity service, underlying business processes and information they process, store or communicate.

The Applicant **MUST** establish, maintain and frequently review procedures to control the allocation of access rights to the identity service, underlying business processes which encompass the user-access lifecycle (i.e. establishment to retirement of access privileges) and the requirement to strictly control and monitor the use of privileged accounts and positions of trust.

Applicable ISM controls: 0413, 0414, 0973, 0416, 0417, 0976, 1227, 0418, 1402, 0419, 0430, 1404, 0431, 0432, 0407, 0441, 0408, 0979, 0980, 0856.

2.7 Communications and operations management

2.7.1 Service continuity for identity services

Objective: Applicants establish a managed process to maintain business continuity for their identity service.

The Applicant **MUST** determine the functionality and quality of service acceptable to legitimate users of their identity service, how to maintain such functionality, and what functionality can be lived without if a service disruption were to occur.

The Applicant **MUST** ensure that protective security controls are embedded in their business continuity management process for their identity service.

Business continuity plans **MUST** be tested, maintained and re-assessed at least annually.

Availability monitoring with real-time alerting **MUST** be implemented to detect an attempted denial of service and measure its impact.

Applicable ISM controls: 1019, 1458, 1431, 1432, 1433, 1434, 1435, 1436, 1190, 1441.

2.7.2 Network security and management

Objective: The confidentiality, integrity and availability of networks relied on by the identity service are maintained.

The Applicant **MUST** implement appropriate security management of networks and supporting infrastructure relied on by the identity service. Controls **MUST** be applied to protect sensitive information transmissions that access or uses public networks.

Access controls **MUST** be applied and maintained for both internal and external network services, connection paths and network-attached resources.

Applicable ISM controls: 1296, 0813, 1074, 1182, 1427, 1311, 1312, 1380, 1381, 1382, 1383, 1442, 1385, 1386, 1387, 1388, 0513, 0515, 0516, 0518, 1178, 1301, 1303, 1223, 0514, 1181, 0385, 1460, 1461, 1462, 1463, 1006, 0071, 1304, 1305, 1307, 0521, 1186, 1428, 1429, 1430, 0568, 0569, 0570, 0571, 0572.

2.7.3 Continuous monitoring and event logging

Objective: Identity service security events are logged and audited.

The Applicant **MUST** actively monitor their identity service in order to detect and respond to anomalous events and **MUST** implement event-logging mechanisms to provide evidence in case of security incidents.

Applicable ISM controls: 0576, 0577, 1028, 1029, 1030, 1185, 0580, 1405, 1344, 0587, 0988, 0582, 0584, 0987, 0585, 0586, 0989, 0859, 0991, 0109, 1228.

2.7.4 Operating system and system file security

Objective: The confidentiality, integrity and availability of operating systems including system files which underpin the identity service are maintained.

The Applicant **MUST** ensure security capabilities at the operating system and system file level are enabled to restrict access to authorised users of the identity service, underlying business processes and information assets.

Applicable ISM controls: 0383, 1410, 0382, 1418, 1408, 0380.

2.7.5 Database security

Objective: The confidentiality, integrity and availability of database systems and their content which underpin the identity service are maintained.

The Applicant **MUST** ensure security capabilities within databases are enabled to restrict access to authorised users of the identity service, underlying business processes and information assets.

Applicable ISM controls: 1243, 1245, 1246, 1247, 1248, 1249, 1250, 1251, 1252, 1256, 1425, 0393, 1255, 1258, 1266, 1268, 1270, 1271, 1272, 1269, 1275, 1276, 1277, 1278, 1273, 1274.

2.7.6 ICT asset handling and protection

Objective: ICT assets which support the identity service are appropriately handled and protected.

The Applicant **MUST** account for and protect all ICT assets which support their identity service.

ICT assets that supports the identity service **MUST** be protected from physical and environmental security threats in order to prevent unauthorised access, loss or damage to information.

All ICT assets which support the identity service **MUST** be controlled and protected.

Applicable ISM controls: 0159, 0336, 0293, 0332, 0333, 1359, 0337, 0832, 0347, 0348, 0947, 1069, 0363, 0364, 0313, 0311, 0316.

2.7.7 Mobile computing

Objective: Information on mobile devices which support the identity service are protected from unauthorised disclosure, modification or loss.

The Applicant **MUST** ensure security capabilities are implemented to restrict access to portable storage devices and other portable information assets including mobility devices and systems which support the identity service.

Applicable ISM controls: 1047, 0693, 0869, 1085, 0863, 0864.

2.8 Cryptography

Objective: Applicants use cryptographic products, algorithms and protocols that have been evaluated by the Australian Signals Directorate to protect their identity service.

2.8.1 Using approved cryptographic algorithms, protocols and modules

The Applicant **MUST** only use security products that implement AACAs. Applicants that use a security product that implements an AACP MUST ensure that only AACAs can be used. The AACAs and AACPs are listed in the current edition of the Australian Government Information Security Manual.

The Applicant **MUST** implement AACAs and AACPs for all information and data while it is in transit and at rest. '*At rest*' means information and data stored in databases, on removable media, and on production, backup and archive servers.

Where an Applicant is an Identity Exchange, they **MUST** store all cryptographic keys for their identity service in a hardware-based cryptographic module approved by ASD.

Where an Applicant is an Identity Service Provider or Credential Service Provider and the outcome of their security risk assessment is rated as:

- *Significant* or higher, they **MUST** store all cryptographic keys for their identity service in a hardware-based cryptographic module approved by ASD.
- Lower than *Significant* they **SHOULD** store all cryptographic keys for their identity service in a hardware-based cryptographic module approved by ASD.

Applicable ISM controls: 0503, 0504, 1003, 1002, 1161, 1446, 1232, 0994, 0471, 0472, 0473, 0474, 0475, 0476, 0477, 0479, 0480, 0481, 0482, 1447, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1448, 1453, 1449, 0484, 0485, 0486, 0487, 0488, 0489, 0997, 0490, 0494, 0495, 0496, 1233, 0497, 0498, 0998, 0999, 1000, 1001.

2.9 Cyber security incident response management

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

The Applicant **MUST** implement procedures encompassing different cyber security incident types (e.g. suspicious or seemingly targeted emails with attachments or links, any compromise or corruption of information, unauthorised access or intrusion into the identity service or a data spill) and communicate these procedures to employees, contractors and third parties as part of a comprehensive protective security awareness program.

The Applicant **MUST** investigate any actual or suspected cyber security incidents reported by a contracted third party which may impact on the services they are contracted to provide.

Cyber security incidents **MUST** be reported through formal procedures and appropriate management channels as quickly as possible. At a minimum cyber security incidents **MUST** be reported to the Trust Framework Accreditation Authority and ASD[3].

Applicable ISM controls: 0120, 0121, 0123, 0124, 0139, 0140, 0141, 0142, 0122, 0125, 0126, 0916, 0129, 0130, 0131, 0132, 0133, 0134, 0135, 0136, 0917, 1212, 0137, 0138, 0915, 1213.

2.9.1 Strategies to mitigate cyber security incidents

The Applicant **MUST** undertake an active role in protecting their identity service, underlying business processes and information assets from exposure to malicious software and scripts including but not limited to:

- Implementing controls to prevent and restrict the proliferation of malicious code, virus and trojan software.
- Educating personnel in the risks associated with the use or introduction of unauthorised software products.

Applicable ISM controls: 1353, 1354, 0843, 0845, 0846, 0955, 1391, 1392, 1413, 0042, 0297, 0298, 0300, 0303, 0304, 0790, 0940, 0941, 1143, 1144, 1365, 1366, 1467, 1411, 0055, 1409, 1412, 0405, 0445, 0616, 0617, 0985, 1175, 1260, 1261, 1262, 1263, 1264, 1407, 0974, 1039, 1173, 1357, 1384, 1401, 0402, 0055, 0118, 0119.

2.10 Physical and environment security

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

The Applicant **MUST** establish or use information hosting facilities (including hosted facilities) which are housed in secure areas commensurate with identified risks to the

[3] See https://www.asd.gov.au/infosec/reportincident.htm for further information on reporting a Cyber Security Incident to ASD.

identity service and protected by a defined security perimeter, with appropriate security barriers and entry controls.

Such facilities **MUST** include physical protection mechanisms which minimise vulnerability to unauthorised access, damage and interference to the identity service.

Applicable ISM controls: 0150

2.11 Information classification and handling

Objective: Information that is generated, accessed, handled or exchanged by the identity service with other systems occurs in a controlled and accountable manner.

Information that is generated, accessed, handled or exchanged by the identity service **MUST** be classified to suitably reflect its importance, degree of sensitivity, handling and protection requirements. The sensitivity, handling and protection requirements **MUST** be reviewed at least annually.

Once assigned a classification or sensitivity rating, the information **MUST** be appropriately handled to adhere to the protection controls for confidentiality, integrity and availability.

2.11.1 Exchange of information

Exchanges of information between the Applicant and other organisations **MUST** be compliant with all applicable legislation and occur in a controlled and accountable manner.

Applicable ISM controls: 0072, 1451, 1452, 1024, 0958, 0995, 1170, 0959, 0960, 1171, 1236, 0963, 0961, 1237, 0659, 0651, 0652, 1389, 1284, 1288, 1289, 1290, 1291, 1292, 0677, 1293, 0660, 0673, 1294, 1295.

2.12 Personnel security

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

2.12.1 Pre-employment controls

Security responsibilities **MUST** be addressed at the recruitment stage, included in contracts and monitored during an individual's employment.

Candidates **MUST** be adequately screened, commensurate to the sensitivity of the information being handled or accessed.

At a minimum candidates **SHOULD** hold, or have the ability to acquire, an Australian Government Baseline Security Clearance[4].

2.12.2 During employment

The Applicant **MUST** demonstrate a commitment to ongoing protective security awareness to ensure that all employees, including contractors, consultants and temporary staff who operate or manage the identity service are equipped to support their organisation's security policies and objectives.

2.12.3 Cessation or changes to employment

The Applicant **MUST** implement and maintain a procedure or set of procedures to effectively manage departing employees or the withdrawal of assigned responsibilities for employees, contractors and other third party users who no longer have a legitimate need to access the identity service.

2.13 Acquisition, development and maintenance

2.13.1 ICT security product assurance

Objective: ICT security products that protect the identity service, underlying business processes or information assets are formally evaluated.

[4] See http://www.defence.gov.au/AGSVA/resources/fact-sheet-baseline-clearance-assessment.pdf for further information.

The Applicant **MUST** determine, document and subsequently test the operational requirements of new ICT security products prior to their acceptance and use in live operating environments. Anticipated capacity requirements **MUST** be forecast, to reduce the likelihood of system overload.

The Applicant **SHOULD** only use ICT security products that have had their functionality formally evaluated through an ASD approved evaluation program. Examples of these programs include the Evaluated Products List and Common Criteria scheme.

Applicable ISM controls: 0971, 0279, 0280, 0282, 0463, 0464, 0285, 0937, 0284, 0938, 0400, 1419, 1420, 1421, 1422, 1238, 0401, 1423, 1239, 1240, 1241, 1424, 0289, 0291.

2.13.2 Change management

Objective: Applicants implement protective security as an integral part of their identity service change management policy and process.

The Applicant **MUST** implement a program of compliance monitoring, periodic performance review and change management for their identity service.

The Applicant **MUST** implement a formal change management process for their identity service which is documented in their protective security documentation.

Applicable ISM controls: 1211, 0912, 0115, 0117.

2.13.3 Protective security reviews

Objective: The security functions of the Applicant's identity service are independently reviewed and maintained.

As part of the Trust Framework Accreditation Process, the Applicant **MUST** undergo the following security evaluations[5]:

- An independent IRAP assessment by an approved IRAP Assessor.

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

- An independent penetration test.

To maintain accreditation the Accredited Provider **MUST** undergo an annual compliance audit[6]. See the *Trust Framework: Protective Security Reviews* for situations when additional security reviews may be required beyond getting accredited and completing annual compliance audits.

[6] See *Trust Framework: Annual Review* for further information

3 Part two: Protective security documentation

The following table lists the suite of protective security documentation that the Applicant **MUST** develop in order to obtain accreditation under the Trust Framework. Further information about mandatory and recommended content for each document can be found under the appropriate heading below.

Table 1: protective security documentation

Document	Purpose of the document
Information Security Policy	The Information Security Policy is a statement of high level information security policies and is therefore an essential part of information security documentation.
Security Risk Management Plan	The Security Risk Management Plan is a best practice approach to identifying and reducing protective security risks.
Vulnerability Management Plan	Undertaking vulnerability management activities such as regular vulnerability assessments allow the Applicant to identify security weaknesses caused by misconfigurations, bugs or flaws.
Incident Response Plan	The Incident Response Plan describes what to do in the event of a cyber-security incident and how to respond appropriately to the situation.
Physical & Environmental Security Plan	A Physical and Environmental Security Plan defines the measures to counter identified risks to an Applicant's assets operating within fixed, mobile and deployed ICT computing environments (including environments hosted by third-parties)
System Security Plan	The System Security Plan is derived from the SRMP and describes the implementation and operation of controls for the Applicant's identity service.
Standard Operating Procedures	Standard Operating Procedures provide a step-by-step guide to undertaking security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by users without strong knowledge of a system.
Personnel Security Plan	The Personnel Security Plan describes how the Applicant's people, information and assets will be managed and protected.
Disaster Recovery & Business Continuity Plan	The Disaster Recovery and Business Continuity Plan helps minimise the disruption to the availability of information and systems after a cyber-security incident or disaster by documenting the response procedures.

Document	Purpose of the document
Emergency Response Management Procedures	Emergency Response Management describe the requirements for securing information and systems as part of the procedures for evacuating a facility in the event of an emergency.
Cryptographic Key Management Plan	The Cryptographic Key Management Plan identifies the implementation, standards, procedures and methods for cryptographic key management.

3.1 Documentation maintenance

The threat environment and Applicant's operating environments are dynamic. If the Applicant fails to keep their protective security documentation current to reflect the changing environment, their security measures and processes may cease to be effective. In that situation, resources could be devoted to areas that have reduced effectiveness, or are no longer relevant. The Applicant **MUST** review protective security documentation:

- At least annually.
- In response to significant changes in the environment, business or system.
- As a result of any cyber security incident.

As part of good documentation maintenance the Applicant **MUST** record the date and version history on each protective security document and be authorised by an appropriate representative of the Applicant's organisation.

3.2 Information Security Policy

The Information Security Policy describes the Applicant's commitment to information security, its approach to information security management and defines information security management responsibilities. It addresses the intended security objectives relating to personnel, access control, business continuity and protection of services, assets and business processes. These objectives are linked to the Applicant's Security Risk Management Plan.

At a minimum the following components **MUST** be included in the Information Security Policy.

Table 2: information security policy content

Topic	Components to be included
Risk management	Risk management roles and responsibilities.
Security awareness	Protective security roles and responsibilities. Information security awareness and training. Accreditation processes.
Access security	User access management. Network access control. Application and information access. Operating system access control.
Communications and operations management	Network security and connections to other systems. Monitoring and logging. Configuration control. Media control. Asset handling and protection. Vulnerability management. Protection against malware. Managing security incidents. Emergency management. Disaster recovery. Business continuity. Cryptographic controls.
Physical and environmental security	Building controls. Secure areas. Physical security for systems and assets.
Information management	Information classification and handling. Information exchange. Information backup, archive and retrieval.
Personnel security	Pre-employment checks. During and post-employment security. Changes to employment.
Acquisition, development and maintenance	Secure development process. Change management.

The following **SHOULD** be considered when developing the Information Security Policy:

- Statement of management intent.
- Information security policy objectives.
- How the information security policy objectives will be achieved.
- The legal framework under which the information security policy will operate.
- Stakeholders and their information security needs.
- The resources required to support the implementation of the information security policy.
- The performance measures to be established to ensure the information security policy is implemented and operates effectively.

3.3 Security Risk Management Plan

Security risks cannot be managed if they are unknown. Even if they are known, failing to deal with them is a failure of security risk management. For this reason, a Security Risk Management Plan consists of two components, a security risk assessment and a corresponding risk treatment strategy. The plan identifies security risks and appropriate mitigation measures for Applicant's identity service.

The Security Risk Management Plan **SHOULD** only be developed after the Applicant has read the *Trust Framework: Risk Management Requirements*. This will assist the Applicant to consider the following:

- The internal, external and security context for risk management.
- Risk tolerance and the rationale for adopting a particular risk appetite or threshold.
- Assets that require protection.
- The process by which the Applicant evaluates and continually monitors vulnerabilities, threats and risks.
- Appropriate risk treatments.
- Stakeholder communication and consultation regarding risk.

Note:
Applicants **SHOULD** apply business impact levels when determining the consequences of compromise or loss of entity information or assets, or harm to their people.

The *Australian Government protective security governance guidelines—Business impact levels*[7] provide a consistent approach to assessing the business impacts arising from the compromise of confidentiality, integrity or availability of resources or harm to individuals or organisations.

The following components **SHOULD** be included in the Security Risk Management Plan.

Table 3: security risk management plan content

Components to be included	
Goals and objectives of the risk management process.	Scope of the risk assessment, including risk tolerance and specific inclusions and exclusions.
Risk treatment options and plans.	Staff responsibilities within the risk management process.
A system description.	The relationship between the system and the objectives of the wider organisation.
Risk management approaches used.	Data flows and data descriptions.
How data aggregation issues are managed.	

Note:
An important component of an Applicant's risk management approach relates to information handling and applying protective markings to ICT assets. Appropriate markings of information applies not only to the collection of personal and other information as part of the identity proofing process, but also

[7] See *References* for further information on business impact levels

to information such as passwords and passphrases. In relation to the information collected as part of the identity proofing process, the Applicant **SHOULD** also consider the issues of data aggregation and its impact on handling requirements. *The Australian Government Information security management guidelines – Management of aggregated information*[8] provides guidance on good management practices to address the information security risks associated with the aggregation of large volumes of information. The guidelines assist in identifying the value of aggregated information and provide guidance on the appropriate protections for aggregated information.

3.4 Vulnerability Management Plan

Undertaking vulnerability management activities such as regular vulnerability assessments, analysis and mitigation are important as threat environments change over time. Vulnerability assessments allow the Applicant to identify security weaknesses caused by misconfigurations, bugs or flaws.

The Vulnerability Management Plan **SHOULD** only be developed after the Applicant has read the *Trust Framework: Risk Management Requirements*. This will assist the Applicant to consider the vulnerabilities likely to impact their identity service.

Note:
The Applicant should continually evaluate vulnerabilities that may impact its identity service. If the Applicant does not assess, analyse and minimise its vulnerabilities it may be a potential target for an attacker to gain access to personal, sensitive, classified or valuable information.

The Australian Signals Directorate publication '*Know and minimise your vulnerabilities before they are used against you*[9] provides guidance for Information Technology Security Advisors in protecting their systems and information.

[8] See *References* for further information on the management of aggregated information
[9] See *References* for further information on minimising vulnerabilities

The Applicant **SHOULD** implement a vulnerability management plan that includes one or more of the following approaches:

- Conducting vulnerability assessments and undertaking routine vulnerability scans on systems throughout their lifecycle to identify vulnerabilities.
- Analysing identified vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls.
- Using a risk-based approach to prioritise the implementation of identified mitigations or treatments.
- Monitoring new information on new or updated vulnerabilities in operating systems, software and devices as well as other elements which may adversely impact on the security of a system.

3.4.1 Conducting vulnerability assessments

Conducting vulnerability assessments prior to systems being used, and after significant changes, can allow the Applicant to establish a baseline for further information security monitoring activities. Conducting vulnerability assessments annually can help ensure that the latest threat environment is being addressed and that systems are configured in accordance with the associated information security documentation.

The Applicant **SHOULD** have vulnerability assessments conducted by suitably skilled personnel independent to the target of the assessment or by an independent third party. Where possible it is recommended that system managers do not conduct vulnerability assessments themselves. This ensure that there is no conflict of interest, perceived or otherwise, and that the assessment is undertaken in an objective manner.

Depending on the scope and subject of the vulnerability assessment, the Applicant **SHOULD** gather information on areas such as:

- Priorities, risk appetite and business requirements.
- System functions and security requirements.
- Risk assessments, including threat data, likelihood and consequence estimates and existing controls in place.

- Effectiveness of existing controls.
- Other possible controls.
- Vendor and other security best practice.

Vulnerability assessments **MAY** consist of:

- Conducting documentation-based security reviews of systems' designs before they are implemented.
- Detailed manual testing to provide a detailed, in-depth assessment of a system once implemented.
- Supplementing manual testing with automated tools to perform routine, repeatable security testing.
- These tools **SHOULD** be from a reputable and trusted source.

The Applicant **MUST** conduct vulnerability assessments on systems:

- Before the system is deployed, this includes conducting assessments during the system design and development stages.
- After a significant change to the system that significantly impacts on the agreed and implemented system architecture and Information Security Policy.
- After significant changes to the threats or risk faced by a system, for example, a software vendor announces a critical vulnerability in a product used by the Applicant.
- As a result of a specific cyber security incident.
- At least annually, as part of a regular scheduled assessment, or as specified by an ITSM or the system owner.

3.4.2 Analysing and mitigating vulnerabilities

Vulnerabilities can be introduced as a result of poor security practices, implementations or accidental activities. Therefore, even if no new vulnerabilities in deployed products have been disclosed there is still value to be gained from conducting regular vulnerability analysis.

Mitigation efforts are best prioritised using a risk-based approach in order to address the most significant vulnerabilities first.

The Applicant **SHOULD**:

- Analyse any vulnerabilities to determine their potential impact on systems and determine appropriate mitigations or other treatments.
- Mitigate or otherwise treat identified vulnerabilities as soon as possible.

Where two or more vulnerabilities are of similar importance, the mitigations with lower cost (in time, staff and capital) **SHOULD** be implemented first.

3.5 Incident Response Plan

An Incident Response Plan outlines actions to take in response to a cyber security incident. In most situations, the aim of the response will be to preserve any evidence relating to the cyber security incident, and to prevent the incident from escalating. (Returning to normal operations is an objective of the Disaster Recovery and Business Continuity Plan).

Note:
The Australian Signals Directorate has developed prioritised mitigation strategies to help technical information security professionals mitigate cyber security incidents. This guidance addresses targeted cyber intrusions, ransomware and external adversaries with destructive intent, malicious insiders, business email compromise and industrial control systems.

This guidance is informed by ASD's experience responding to cyber security incidents, performing vulnerability assessments and penetration testing Australian government organisations. Further information is available in the following ASD publications:

- Strategies to Mitigate Cyber Security Incidents[10].
- Strategies to Mitigate Cyber Security Incidents - Mitigation Details.

Applicants **MUST** consider these publications when developing their Incident Response Plan.

[10] See *References* for further information on mitigating cyber security incidents

The Applicant **MUST** develop and maintain an Incident Response Plan and supporting procedures. At a minimum, the following components **MUST** be included in the Incident Response Plan.

Table 4: incident response plan content

Components to be included	
Broad guidelines on what constitutes a cyber security incident.	The expected response (and time frame) to each cyber security incident type.
The minimum level of cyber security incident response and investigation training for system users and system administrators.	The authority responsible for initiating investigations of a cyber security incident.
The steps required to ensure the integrity of evidence supporting a cyber security incident.	The steps necessary to ensure that critical systems remain operational.
Security incident responsibilities and procedures for each system in relevant SSP, SOPs and IRP.	How to formally report cyber security incidents.
Clear definitions of the types of cyber security incidents that are likely to be encountered.	The authority responsible for responding to cyber security incidents.
The criteria by which the responsible authority would initiate or request formal, police or Australian Security Intelligence Organisation (ASIO) investigations of a cyber-security incident.	Other authorities or parties (e.g. clients and agencies) impacted by the incident which need to be informed in the event of an investigation being required.
The details of the system contingency measures or a reference to these details if they are located in a separate document.	Procedures for dealing with data spills.
Logging requirements, including what information is logged, log retention periods and who has access to logs.	

The Incident Response Plan **SHOULD** only be developed after the Applicant has read the *Trust Framework: Privacy Requirements*. This will assist the Applicant to understand their data breach response management obligations.

3.5.1 Cyber Security Incident Register

All cyber security incidents **MUST** be recorded in a register. At a minimum the following information **SHOULD** include:

- The date the cyber security incident was discovered.
- The date the cyber security incident occurred.
- A description of the cyber security incident, including people and locations involved.
- The actions taken in response to the incident.
- The person to whom the cyber security incident was reported.

The Applicant **MUST** report all cyber security incidents to ASD using the Cyber Security Incident Reporting (CSIR) scheme[11].

3.6 Physical and Environmental Security Plan

A Physical and Environmental Security Plan defines the measures to counter identified risks to an Applicant's assets operating within fixed, mobile and deployed ICT computing environments (including environments hosted by third-parties).

The Applicant **MUST** develop and maintain a Physical and Environmental Security Plan, which covers their identity service. At a minimum, this plan **SHOULD** include the following components.

Table 5: physical and environmental security plan content

Components to be included	
Measures that are scalable to meet increases in threat levels.	The location and nature of the operating environment.
Whether the Applicant has sole or shared ownership or tenancy of the operating environment.	Whether the public or other non-agency personnel have a right of entry to the operating environment.
The potential sensitivity or possible security classification of information to be stored, handled, processed or otherwise used in each part of the operating environment.	ICT assets, including, but not limited to, data, software, hardware and portable equipment such as laptops, tablets, smart phones and personal electronic devices.
ICT-related equipment (for example, file servers, workstations, terminals, main distribution frames and cabling) and utilities.	Any other resources that will be within the operating environment.

[11] See https://www.asd.gov.au/infosec/reportincident.htm for further information on reporting a cyber security incident to ASD.

Components to be included	
Specifications as to the security ratings of the various areas and zones within the operating environment.	Any requirements for No Lone Zones.
Protective measures required for: the entire operating environment; and designated areas within the operating environment, such as a room intended hold information of a higher classification than the rest of the operating environment.	What differing measures will be required for: storage, handling and processing of classified or sensitive information; and classified or sensitive discussions and meetings.

3.7 System Security Plan

The System Security Plan describes the implementation and operation of ICT system controls. The Applicant **MUST** develop and maintain a System Security Plan which covers their identity service. At a minimum, this plan **MUST** include the following components.

Table 6: system security plan content

Components to be included		
Management of visitors (e.g. escorting).	Security roles and responsibilities.	Management of staff.
Staff training requirements.	Management of contractors.	Response details in the event of an incident.
Personnel access controls.	System monitoring, logging and maintenance regimes.	Staff authorisation, clearance and briefing requirements.
Application and operating system patching strategies.	Staff requirements to hold positions of trust.	Intrusion detection and prevention strategies.
Physical access controls.	Role and access privileges of guards.	Standard Operating Procedures for system-specific roles.
Cryptographic key management.	Intruder alarm systems.	Network and logical access controls.
ASD's Essential Eight[12].	Denial of service controls.	Quality of Service targets.

[12] See *References* for further information on the ASD's Essential Eight

3.8 Standard Operating Procedures

The Applicant **MUST** ensure that Standard Operating Procedures are developed for all personnel that interact with their identity service, including the following types of roles:

- Information Technology Security Managers (ITSM).
- Information Technology Security Officers (ITSO)[13].
- System Administrators.
- Internal system users.

The Applicant **SHOULD** include a SOP, which requires all personnel with access to the identity service to notify an ITSM of any cyber security incident. The Applicant **SHOULD** require ITSMs, ITSOs, System Administrators and system users to sign a statement confirming they have read and agree to abide by their respective SOPs.

3.8.1 Information Technology Security Managers

The ITSM SOPs cover the management and leadership activities related to system operations. The Applicant **SHOULD** document the following procedures in the ITSM's SOPs:

Table 7: ITSM SOPs content

Topic	Procedures to be included
Cyber Security Incidents	Reporting and managing cyber security incidents.

3.8.2 Information Technology Security Officers

The ITSO SOPs cover the operationally focused activities related to system operations. The Applicant **SHOULD** document the following procedures in the ITSO's SOPs.

[13] For the purpose of this document, an ITSO may also be referred to as an Information Technology Security Advisor (ITSA) or an equivalent position within the agency or organisation.

Table 8: ITSO SOPs content

Topic	Procedures to be included
Access control	Authorising access rights to applications and data.
Asset musters	Labelling, registering and mustering assets, including media.
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users and retention schedule for logs.
Configuration control	Approving and releasing changes to the system software and configurations.
Cyber security incidents	Detecting potential cyber security incidents. Establishing the cause of any cyber security incident, whether accidental or deliberate. Conducting investigations. Actions to be taken to recover and minimise the exposure from a cyber-security incident.
Data transfers	Managing the review of media containing information that is to be transferred off-site (including sites used for backup operations, archival and storage). Managing the review of incoming media for viruses or unapproved software.
Managing ICT equipment	Managing the sanitation, destruction and disposal of unserviceable ICT equipment and media.
Conducting system audits	Reviewing system user accounts, system parameters and access controls to ensure that the system is secure. Checking the integrity of system software. Testing access controls. Inspecting ICT equipment and cabling.
System maintenance	Maintaining the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches, updates and antivirus signatures, and applying appropriate hardening techniques.
User account management	Authorising new system users, removing or disabling unused accounts, replacing default passwords, account sharing and account lockouts.
Identity fraud control	Contribute to the development of fraud awareness training programs. Contribute to the development of fraud control plans.

3.8.3 System Administrators

Whilst the system administrator SOPs primarily focus on the administrative activities related to system operations, they also support the ITSO SOPs. The Applicant **SHOULD** document the following procedures in the System Administrator's SOPs.

Table 9: System Administrator SOPs content

Topic	Procedures to be included
Access control	Implementing access rights to applications and data.
Configuration control	Implementing changes to the system software and configurations.
System backup and recovery	Backing up data, including audit logs. Securing backup tapes. Recovering from system failures.
User account management	Adding and removing system users. Setting user privileges. Cleaning up directories and files when a user departs or changes roles.

3.8.4 Internal system users

The user SOPs focus on day-to-day activities that users need to be aware of, and comply with, when using systems. The Applicant **SHOULD** document the following procedures in the System User's SOPs.

Table 10: internal system user SOPs content

Topic	Procedures to be included
Cyber security incidents	What to do in the case of a suspected or actual cyber security incident.
End of day	How to secure systems at the end of the day.
Media control	Procedures for handling and using media.
Passphrases	Protecting passphrases, authentication tokens and activation data.
Temporary absence	How to secure systems when temporarily absent.

3.9 Personnel Security Plan

Personnel Security is the management of staff to assist in the protection of the Applicant's people, information and assets. In a security aware culture personnel security includes three major components:

- Identification of suitable staff to access Applicant's information, resources and assets.
- Education and training of staff about their security roles and responsibilities.
- Monitoring and evaluation of staff continued suitability.

The Applicant **MUST** develop and maintain a Personnel Security Plan, which covers the personnel who interact with their identity service. At a minimum, this plan SHOULD include the following components.

Table 11: personnel security plan content

Components to be included	
Pre-employment checks: Identity verification. Eligibility checks (e.g. citizenship or visa working conditions). Qualification checks. Previous employment checks (e.g. referee checks). Criminal record check.	Monitoring and evaluation of: Access controls. Physical and logical access privileges. Physical access and IT systems monitoring. Maintenance and repair of IT systems by uncleared technicians.
Employee screening and where necessary, security clearance requirements for positions.	Security awareness, training and education requirements.

3.10 Disaster Recovery and Business Continuity Plan

Disaster Recovery and Business Continuity Plans help minimise the disruption to the availability of information and systems after an event or disaster. Disaster Recovery and Business Continuity Plans work to maintain security in the face of unexpected events or changes. Together, these plans help to:

- Reduce the time between a disaster occurring and critical functions of systems being restored.

- Minimise the disruption to the availability of information and systems after a cyber security incident or disaster by documenting the response procedures.
- Ensure critical system functions continue to operate when the system is in a degraded state.

Note:
Business continuity management is the development, implementation and maintenance of policies, frameworks and programs to assist an organisation manage a business disruption, as well as build organisational resilience. The capability assists in preventing, preparing for, responding to, managing and recovering from the impacts of a disruptive event.

Business continuity management forms part of an Applicant's overall approach to effective risk management, and **SHOULD** be closely aligned to their incident response management, emergency response management and IT disaster recovery capabilities.

The Australian National Audit Office publication *Business Continuity Management*[14] assists Applicants to plan for continued delivery of critical business processes in the event of business disruption.

The Applicant **MUST** develop and maintain a Disaster Recovery and Business Continuity Plan, which covers their identity service. At a minimum, this plan **MUST** include the following components.

[14] See *References* for further information on business continuity management

Table 12: disaster recovery and business continuity plan content

Topic	Components to be included
Governance	Clearly defined and approved management processes to manage business continuity. Roles, tasks and responsibilities of internal and external providers including inter-dependencies: Sponsorship (organisational and financial support). Ownership (accountability and responsibility). Custodianship (tactical responsibility for BCM tasks). Links to the Applicant's SRMP and risk management processes. BCM testing arrangements. Managing changes to the Business Continuity Plan.
Training	Awareness and training requirements for: Response and recovery team members. General staff (including contractors).
Risk Assessment	Risk assessment has been undertaken to identify assets, threats, vulnerabilities and controls for BCM. Direct links between the SRMP and business continuity management processes and activities, including relevant disruption scenarios.
Business Impact Analysis	Recovery objectives and priorities have been established. Critical resources, facilities, equipment, assets and information have been identified and catalogued. Interdependencies of process have been identified. Continuity strategies implemented.
Disaster Recovery Planning	Business continuity plan is documented and endorsed. Business continuity plan is up-to-date. Response, recovery and restoration procedures are documented, approved and communicated to staff.
Testing and Monitoring	Business continuity testing requirements. Testing requirements for critical business processes. Process to update and revise plans following testing and exercising. Ongoing BCM monitoring requirements.

The following **SHOULD** be considered when developing the Disaster Recovery and Business Continuity Plan:

- Governance arrangement for disaster recovery and business continuity.
- Disaster recovery and business continuity awareness training needs.
- Possible disruption scenarios.

- Business impact analysis and the identification of critical assets.
- Business continuity testing.

3.10.1 Testing and validating the Disaster Recovery Plan

Regular testing and validation of the Disaster Recovery Plan is crucial to effective disaster recovery and business continuity planning with the results of these tests being recorded and incorporated into the review and updates of the Disaster Recovery Plan.

Testing and validation of the Disaster Recovery Plan **MUST** be carried out annually and **SHOULD** be implemented in the following steps:

- Identify areas to be tested and evaluated.
- Prepare the plans.
- Undertake testing and validation.
- Review and assess the results.
- Update plans accordingly.

3.10.2 Denial of service continuity plan

As part of business continuity management, the Applicant **MUST** develop a denial of service continuity plan, which includes:

- How to identify signs of a denial of service.
- How to identify the source of a denial of service, either internal or external.
- How capabilities can be maintained during a denial of service e.g. personal mobile phones That have been identified for use in case of an emergency.
- What actions can be taken to clear a denial of service e.g. banning certain devices/IPs at the call controller and firewalls, implementing quality of service, changing authentication, changing dial-in authentication.

The Applicant **SHOULD** determine the functionality and quality of services acceptable to legitimate users of online services, how to maintain such functionality, and what functionality can be lived without during a denial of service.

The Applicant **SHOULD** implement Internet Best Current Practice 38 (BCP38) on networks.

3.11 Emergency Response Management Procedures

Emergency response management is the activity that takes place immediately after an incident has occurred. It can also be referred to as the tactical management of a situation. The primary concern of the emergency response is the safety of people. During an incident, emergency response procedures may include the evacuation of a building, liaison with emergency services, initial assessment of damage that has occurred and implications for the Applicant.

Emergency Response Management Procedures describe the requirements for securing information and systems as part of the procedures for evacuating a facility in the event of an emergency.

During the evacuation of a facility, it is important that personnel secure information and systems as they would at the end of operational hours. This includes, but is not limited to, securing media and logging off workstations. This is important as a malicious actor could use such an opportunity to gain access to applications or databases that a user had already authenticated to, or use another user's credentials, for a malicious purpose.

Evacuation procedures **SHOULD** include the need for internal system users to secure information and systems before evacuation unless the chief warden, to avoid serious injury or loss of life, authorises personnel to evacuate immediately without securing information and systems.

3.12 Cryptographic Key Management Plan

The Cryptographic Key Management Plan identifies the implementation, standards, procedures and methods for key management. It provides a good starting point for the protection of cryptographic systems, keys and digital certificates. The level of detail included in the Cryptographic Key Management Plan **MUST** be commensurate

with the criticality, sensitivity and classification of the information to be protected and **MUST** include the following components at a minimum.

Table 13: cryptographic key management plan content

Topic	Component to be included
Objectives	Objectives of the cryptographic system and CKMP, including the Applicant's aims.
Accounting	How accounting will be undertaken for the cryptographic system. What records will be maintained. How records will be audited.
Cyber security incidents	A description of the conditions under which compromise of keys will be declared. References to procedures to be followed when reporting and dealing with compromised keys.
Cryptographic key management	How are keys generated. How are keys delivered to intended users. How are keys received, installed and activated. Key distribution, including locate, remote and central. How are keys transferred, stored, backed up and archived. How are keys recovered after a disaster as part of business continuity management. How are keys revoked, suspended, deactivated and destroyed. How are keys changed or updated. Logging and auditing of key management related activities.
Maintenance	Maintenance of the cryptographic system software and hardware. Destroying cryptographic equipment and media.
References	Vendor documentation. Relevant policies.
Sensitivity or classification	Sensitivity or classification of the cryptographic system hardware, software and documentation.
System description	Sensitivity or classification of the information protected. The use of keys. The ICT computing environment. Administrative responsibilities. Key lengths and algorithms used. Key lifetimes and crypto periods.

Topic	Component to be included
System topology	Diagrams and descriptions of the cryptographic system topology including data flows.
Cryptographic evaluations	Government approved evaluations performed on cryptographic systems (e.g Common Criteria, EPL, Protection Profiles, ACE, etc).

Keys or digital certificates used for digitally signing or encrypting messages that are suspected of being compromised (that is, lost, stolen, copied, or uncontrolled), are incapable of offering any assurance in the integrity of the subsequent messages digitally signed or encrypted by that key. Likewise, no assurance can be placed in the confidentiality of a message encrypted using the public key, since third parties could intercept the message and decrypt it using the private key.

Applicants that use Public Key Infrastructure are required to:

- Immediately revoke digital certificates that have been compromised.
- Immediately suspend digital certificates suspected of being compromised.

3.12.1 ASD Approved Cryptographic Algorithms and Protocols

Whilst there is no guarantee or proof of security of an algorithm against presently unknown intrusion methods, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible intrusion. There have been some cases where theoretically impressive vulnerabilities have been found, however these results are not of practical application.

The Applicant **MUST** use encryption products that implement Australian Signals Directorate Approved Cryptographic Algorithms (AACAs) and Australian Signals Directorate Approved Cryptographic Protocols (AACPs) as defined in the current edition of the ISM.

If a product implements unapproved protocols as well as AACPs, it is possible that relatively weak protocols could be configured without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

When configuring products that implement an AACP, the Applicant **MUST** ensure that only the AACP can be used by either disabling the unapproved protocols (which is preferred) or advising users not to use the unapproved protocols via a policy. The Applicant using a product that implements an AACP is required to ensure only AACAs can be used.

4 References

The following information sources have been used in developing this document.

1. Attorney General's Department, 2015, 'Australian Government Information security management guidelines – Management of aggregated information', Australian Government, Canberra. https://www.protectivesecurity.gov.au/informationsecurity/Documents/PSPF-InformationSecurityManagementGuidelines-ManagementOfAggregatedInformation.pdf
2. Attorney-General's Department, 2015, 'Protective security governance guidelines – Business impact levels', Australian Government, Canberra. https://www.protectivesecurity.gov.au/governance/security-risk-management/Documents/Business-impact-levels.pdf
3. Attorney General's Department, 2017, 'Protective Security Policy Framework (PSPF)', Australian Government, Canberra. https://www.protectivesecurity.gov.au/Pages/default.aspx
4. Australian National Audit Office, 2014, 'Business Continuity Management (report 6 of 2014-15)', Australian Government, Canberra. https://www.anao.gov.au/work/performance-audit/business-continuity-management
5. Australian Signals Directorate, 2017, '2017 Australian Government Information Security Manual: Controls (ISM)', Australian Government, Canberra. https://www.asd.gov.au/infosec/ism/
6. Australian Signals Directorate, 2017, 'Essential Eight Explained', Australian Government, Canberra. https://asd.gov.au/publications/protect/essential-eight-explained.htm
7. Australian Signals Directorate, 2012, 'Know and minimise your vulnerabilities before they are used against you', Australian Government, Canberra. https://www.asd.gov.au/publications/protect/Know_Minimise_Vulnerabilities.pdf
8. Bradner, S. 1997, 'Key words for use in RFCs to Indicate Requirements Level' (Requests for Comment 2119)', Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119
9. Ferguson, P. & Senie, D. 2000, 'Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing' (Best Current Practice 38)', Internet Engineering Task Force, Switzerland. https://tools.ietf.org/pdf/bcp38.pdf
10. Hoffman, P. 2002, 'SMTP Service Extension for Secure SMTP over Transport Layer Security' (Request for Comments 2487), Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2487
11. National Institute of Standards and Technology, 2013, 'Digital Signature Standard' (DSS) - NIST FIPS 186-4), US Department of Commerce, Maryland, United States of America. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
12. Privacy Act, 1988 (Cwth)