



Security Requirements for My Health Record Connecting Systems Conformance Profile

7 September 2023 Draft version v1.1

Draft for external review

Document ID: **DH-3802:2023**

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au



Acknowledgements

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer

The Australian Digital Health Agency (“the Agency”) makes the information and other material (“Information”) in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Copyright © 2023 Australian Digital Health Agency

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

OFFICIAL

Document information

Key information

Owner	Connected Care Branch, Digital Solutions Division
Contact for enquiries	Australian Digital Health Agency Help Centre
Phone	1300 901 001
Email	help@digitalhealth.gov.au

Document version history

Version	Date	Release comments	Agency reference
Draft 1.0	19/12/2022	First draft release for external review	DOC22/37985
Final Draft 1.1	07/09/2023	Final draft release for external review	DOC23/072234

Table of contents

1	Introduction	5
1.1	Purpose	5
1.2	Intended audience	5
1.3	Scope.....	5
2	Security framework	6
3	Conformance Requirements.....	7
3.1	Authentication hardening.....	8
3.2	Access to systems and their resources	14
3.3	Encryption	17
3.4	Application development.....	19
3.5	Web application development.....	22
3.6	Application hardening.....	24
3.7	Operating system hardening.....	27
3.8	System patching.....	28
3.9	Data backup and restoration	30
4	Compliance Requirements	32
4.1	Access to systems and their resources	32
4.2	Application development.....	32
4.3	System patching.....	35
4.4	Data backup and restoration	37
	Appendix A Implementation guidance	38
	Acronyms	40
	Glossary.....	42
	References.....	44

1 Introduction

The Agency is cognisant of the inherent cyber security risks posed by systems connected to and accessing the My Health Record system, as well as potentially vulnerable aspects of the national infrastructure and all services under its care. To address this risk, a set of security requirements for systems connecting to the My Health Record system have been identified. The controls that are most relevant to the development of software for healthcare organisations, have been selected from the Australian Cyber Security Centre's (ACSC) Information Security Manual (ISM) [ACSC2023a].

The focus of this conformance profile is on incorporating the security control functionalities within software systems that are connected to the My Health Record system either directly or indirectly. This conformance profile is intended to set a minimum standard or baseline level of cyber security that is expected of connecting systems, and that is consistently adopted. The requirements in this conformance profile are intended to strike an appropriate balance between strengthening the cyber security posture of all connecting systems and minimising potential impacts on software providers and overall system participation. In doing so, this conformance profile supports the overarching goals of improving security within healthcare software systems and fostering a secure and trusted healthcare ecosystem.

Implementers should refer to the My Health Record System Conformance Assessment Scheme (CAS) [AGENCY2023] for information about declaring conformance to this conformance profile.

1.1 Purpose

This document lists the security requirements that are applicable for healthcare software systems integrating with the My Health Record system.

The profile includes two main sections:

1. Conformance requirements that apply to the healthcare software system
2. Compliance requirements that apply to the software provider organisation.

1.2 Intended audience

The intended audience includes:

- Software developers
- Software provider organisations
- Healthcare organisations and providers

1.3 Scope

This document contains both conformance and compliance requirements that are to be applied to connecting systems that access the My Health Record system via the Business-to-Business (B2B) Gateway services.

2 Security framework

The security framework applicable to this conformance profile is the ISM. As described in the ISM, the ISM is a security manual *“to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats.”* [ACSC2023a].

The ISM is general and broad in nature and not all controls can be applied to all software. Of the controls that can be applied to software, the Agency has identified controls that provide direct benefits without imposing unreasonable imposts on the software product.

It is acknowledged that the ISM is updated periodically, and the alignment to ISM controls within this profile is based on a specific version indicated in the document references. Software providers are encouraged to adopt the latest and/or stronger controls in future ISM releases if they choose, provided this does not introduce conflicts with the requirements in this profile. For the avoidance of doubt, the relaxing of controls in a future ISM release is considered a conflict, in which case the requirements specified in this profile continue to prevail.

3 Conformance Requirements

This section lists the security conformance requirements for healthcare software systems. For a healthcare software system to be considered conformant, it must meet the mandatory requirements and all relevant conditional requirements. Conditional requirements are deemed mandatory if the specific conditions are met for the implementation.

While conformance to the recommended requirements is not mandated, it is advisable for healthcare software systems to implement recommended requirements where possible, as these requirements may become mandatory in future releases.

The conformance requirements apply to both healthcare software systems directly connected to the My Health Record system and other software systems indirectly connected to it. Indirect connections include systems that interface with the My Health Record system through one or more middleware.

Given the diverse integration methods of healthcare software with the My Health Record system, it is not expected that a single connecting system alone will fulfill all the requirements outlined in this conformance profile. It is likely that multiple software systems will collaboratively meet the requirements defined in this profile during implementation.

Requirements follow a standard form, utilising the following language:

SHALL: When appearing in a conformance requirement, the verb SHALL indicates a mandatory requirement. Its negative form SHALL NOT indicates a prohibition.

SHOULD: When appearing in a conformance requirement, the verb SHOULD indicates a recommendation. Its negative form SHOULD NOT indicates an option that should not be supported.

Note: the unique numbering of each requirement contained within this section of the profile is not intended to be sequential. Further, any gaps in numbering are intentional and inconsequential. Requirements have been grouped according to the categories of controls outlined in the ISM or a suitable equivalent.

3.1 Authentication hardening

This section includes the requirements for strengthening the system authentication processes used to grant system access. Examples of multi-factor authentication include passwords, one-time SMS codes, one-time password applications, universal 2nd Factor security keys, physical one-time password tokens, biometrics (such as fingerprint or face identification), and smartcards.

SEC-0081**Session and screen locking**

The healthcare software system SHALL automatically log off an account or require re-authentication after a period of inactivity.

The period of inactivity SHALL be no longer than 15 minutes.

Priority:

Mandatory

Notes:

Healthcare organisations may define a period of inactivity after which the user's terminal may be considered unattended and vulnerable to misuse in their specific setting, but it must be no longer than 15 minutes.

Software-as-a-Service/hosted service providers that are unable to set a unique time period for each organisation may select a time period no longer than 15 minutes for all organisations and users.

Traces:

ISM Security Control 0428:

Systems are configured with a session or screen lock that:

- activates after a maximum of 15 minutes of user inactivity, or if manually activated by the user
- conceals all session content on the screen
- ensures that the screen does not enter a power saving state before the session or screen lock is activated
- requires the user to reauthenticate to unlock the system
- denies users the ability to disable the session or screen locking mechanism.

SEC-0086	Storage of credentials - user If the healthcare software system stores user credentials in any form, it SHALL ensure that the credentials are stored securely. To securely store credentials, passwords or passphrases: <ul style="list-style-type: none">• SHALL NOT be stored as plain text• SHALL be stored with salt added and encrypted using an ASD approved hashing algorithm. Priority: Conditional Notes: It is recommended the salt is unique and randomly generated for each user, with a minimum of 32 bytes. It is understood and acceptable that the algorithm used to generate the salt may result in generating the same salt for different users. Information about ASD approved cryptographic and hashing algorithms can be found in the Australian Cyber Security Centre's Guidelines for Cryptography [ACSC2023b]. Traces: ISM Security Control 1402: Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.
SEC-0271	General user access The healthcare software system SHALL have the capability to authenticate users using multi-factor authentication. Priority: Mandatory Notes: Multi-factor authentication helps to mitigate the risk of an attacker gaining access to the sensitive data accessible to general users due to widely used attacks on single factor username and password. It is important for the healthcare software system to provide the multi-factor authentication functionality, providing the healthcare organisation with the option to enable this feature based on the organisation's risk profile. Traces: ISM Security Control 1504: Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. ISM Security Control 1679: Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

SEC-0270	Privileged user access The healthcare software system SHALL authenticate all privileged users (e.g system administrators) using multi-factor authentication.
Priority:	Mandatory
Notes:	Privileged users are those who can alter or circumvent a system's security measures, access and modify system configurations, account privileges, and audit logs, and access important data repositories. This can also apply to users such as software developers, who may have only limited privileges, but can still bypass security measures. For this reason, they are more likely to be targeted by threat actors as they could provide full access to systems, so it is important that multi-factor authentication is used for these accounts.
Traces:	ISM Security Control 1173: Multi-factor authentication is used to authenticate privileged users of systems.

SEC-0083

Breached credential validation

The system SHALL validate the user's credentials with a known breached credentials service or against an external known breached credential list.

The healthcare software system SHALL perform the validation when:

- user credentials are created
- user credentials are updated
- user credential is used and has not been validated in the last 24 hours.

Priority:

Mandatory

Notes:

Validation of user credentials is required only once every 24 hours to avoid frequent execution of credential checks, that may adversely impact the breached credentials service performance and interrupt clinical workflow, especially if free services (e.g "Have I Been Pwned") are slow to respond during high traffic periods.

Software providers should note some breached credential lists are updated infrequently (e.g once or twice a year).

Refer Appendix A.1 for implementation guidance.

Traces:

ISM Security Control 1590:

Credentials are changed if:

- they are directly compromised
- they are suspected of being compromised
- they appear in an online data breach database
- they are discovered stored on networks in the clear
- they are discovered being transferred across networks in the clear
- membership of a shared account changes
- they have not been changed in the past 12 months.

SEC-0580	Notification when credential previously exposed in data breaches If the healthcare software system performs breached credential validation and the credential was found in a past breach, the system SHALL alert a responsible person and prompt the user to update the credential before the next login. The alert to the responsible person SHALL NOT disclose the credential that has been breached.
Priority:	Conditional
Notes:	This requirement intends to prevent interruption to clinical workflow and not force a user to update their password during the provision of healthcare. A responsible person may be a system administrator or direct supervisor. The alert might be an internal email or text message or some obvious indication to the responsible person inside the healthcare software system. An unobtrusive entry in an audit or transaction log or similar data store is not considered a sufficient alert.
Traces:	ISM Security Control 1590: Credentials are changed if: <ul style="list-style-type: none">• they are directly compromised• they are suspected of being compromised• they appear in an online data breach database• they are discovered stored on networks in the clear• they are discovered being transferred across networks in the clear• membership of a shared account changes• they have not been changed in the past 12 months.

SEC-0075	Access to breached credentials service <p>If the healthcare software system accesses a breached credentials service and the system receives no or delayed response, the system SHALL permit users to use their credentials and allow access to the system.</p> <p>Priority: Conditional</p> <p>Notes: The meaning of “delayed response” is determined by the software provider and will depend on the importance and criticality of the healthcare software system and its target environment.</p> <p>This requirement intends to prevent interruption to clinical workflow if free services that provide no Service Level Agreements (e.g “Have I Been Pwned”) are slow to respond during high traffic periods.</p> <p>Traces: ISM Security Control 590: Credentials are changed if:</p> <ul style="list-style-type: none">• they are directly compromised• they are suspected of being compromised• they appear in an online data breach database• they are discovered stored on networks in the clear• they are discovered being transferred across networks in the clear• membership of a shared account changes• they have not been changed in the past 12 months.
SEC-0088	Disable application-level authentication <p>If the healthcare software system is integrated with an enterprise Single-Sign-On (SSO) service, the healthcare software system SHOULD provide the capability to disable any application-level authentication.</p> <p>Priority: Recommended</p> <p>Notes: Single-Sign-On service is a centralised authentication service that allows users to access multiple applications and systems within an organisation using a single set of login credentials. This includes healthcare software systems that verify the user's credentials against the organisation's authentication directory, such as Active Directory or an enterprise identity management system.</p> <p>This requirement implies that application-level authentication, including multi-factor authentication, may be turned off when a Single-Sign-On service is used.</p> <p>Traces: No applicable trace to ISM Security Controls.</p>

3.2 Access to systems and their resources

SEC-0062	<p>Role-based access</p> <p>The healthcare software system SHALL support role-based access control for authorised users to access the My Health Record system.</p> <p>Priority: Mandatory</p> <p>Notes: Only users authorised by the healthcare organisation as having specific My Health Record system rights may have access to that particular My Health Record functionality. This includes viewing, authoring, and uploading My Health Record clinical documents.</p> <p>Role-based access enables the principle of least privilege to be adhered to, ensuring users are granted only the minimum level of permission required to do their job and perform their tasks. Limiting permissions in this way restricts the capability of a threat actor in the event of account compromise.</p> <p>Implementers may choose to implement other additional access controls, e.g attribute-based access control, in addition to the role-based access control.</p> <p>Traces: No applicable trace to ISM Security Controls.</p>
SEC-0060	<p>Access to the My Health Record</p> <p>The healthcare software system SHALL allow access to the My Health Record system without the need for the user account to have administrator functions on the operating system.</p> <p>Priority: Mandatory</p> <p>Notes: Administrator accounts are often targeted as their accounts can potentially give full access to a system. By not requiring the clinical software to run in administration mode, user accounts can be appropriately restricted without impacting the use of the clinical software.</p> <p>Traces: ISM Security Control 1508: Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties. ISM Security Control 0445: Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.</p>

SEC-0160	Access to backup files The healthcare software system SHALL only allow administrators assigned a dedicated backup administrator role to access, change and erase backup files and data.
Priority:	Mandatory
Traces:	ISM Security Control 1705: Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.
SEC-0070	Privileged account access Software functions associated with advanced or power-users SHALL be restricted to a role appropriate to those functions.
Priority:	Mandatory
Notes:	Privileged users are those who can alter or circumvent a system's security measures, access and modify system configurations, account privileges, and audit logs, and access important data repositories. This can also apply to users such as software developers, who may have only limited privileges, but can still bypass security measures.
Traces:	ISM Security Control 1508: Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties. ISM Security Control 0445: Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.

SEC-0087 Disable inactive user accounts

The healthcare software system SHOULD automatically disable a user account that has not been active for at least 45 days.

Priority: Recommended

Notes: Removing or suspending access to systems can prevent them from being accessed when there is no longer a legitimate use, such as when users change duties or leave an organisation.

Healthcare organisations may define a period of inactivity after which the user account may be considered inactive and vulnerable to misuse in their specific setting, but it should be no longer than 45 days.

Software-as-a-Service/hosted service providers that are unable to set a unique period for each organisation may select a period no longer than 45 days for all organisations and users.

Traces: ISM Security Control 1404:
Unprivileged access to systems and applications is automatically disabled after 45 days of inactivity
ISM Security Control 1648:
Privileged access to systems and applications is automatically disabled after 45 days of inactivity.

3.3 Encryption

SEC-0110 **Approved cryptographic algorithms and protocols for transmission of information**

The healthcare software system SHALL encrypt all information transmitted using only Australian Signals Directorate (ASD) approved cryptographic algorithms and ASD-approved cryptographic protocols, except for the data used to support technical operation of the system.

Priority: Mandatory

Notes: Support for protocols SSL 1.0/SSL 2.0/SSL 3.0/TLS 1.0/TLS 1.1 must be disabled as they have been deprecated due to exploitable weaknesses.

Information about ASD approved cryptographic and hashing algorithms can be found in the Australian Cyber Security Centre's [Guidelines for Cryptography](#) [ACSC2023b].

Traces: ISM Security Control 0471:
Only AACAs or high assurance cryptographic algorithms are used by cryptographic equipment and software.
ISM Security Control 0481:
Only AACPs or high assurance cryptographic protocols are used by cryptographic equipment and software.

SEC-0084 **Encryption of data at rest on partition**

The healthcare software system SHALL store all data on a partition encrypted with an Australian Signals Directorate (ASD) approved cryptographic algorithm.

Priority: Mandatory

Notes: The software system should routinely interrogate the environment it operates on to determine if the partition is encrypted. For example, this might happen once a day or at the start of each session.

Full disk encryption provides a greater level of protection than file-based encryption. While file-based encryption may encrypt individual files, there is the possibility that unencrypted copies of files may be left in temporary locations used by an operating system.

Information about ASD approved cryptographic and hashing algorithms can be found in the Australian Cyber Security Centre's [Guidelines for Cryptography](#) [ACSC2023b].

Traces: ISM Security Control 0459:
Full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition, is implemented when encrypting data at rest.

SEC-0125	Encryption of data at rest in database The healthcare software system SHALL store all data in a database (or files) that is encrypted with an Australian Signals Directorate (ASD) approved cryptographic algorithm.
Priority:	Mandatory
Notes:	<p>Database level encryption is offered by many commercial database platforms. Software developers should leverage that functionality to offer protection against data theft.</p> <p>Information about ASD approved cryptographic and hashing algorithms can be found in the Australian Cyber Security Centre's Guidelines for Cryptography [ACSC2023b].</p>
Traces:	No applicable trace to ISM Security Controls.

3.4 Application development

SEC-0090

Return values of system calls

The healthcare software system SHALL be able to handle all possible return values for all system calls.

The system SHALL capture the return value for every system call and for every possible return value, the system SHALL have a deliberate course of action.

Priority:

Mandatory

Notes:

System call describes as a way for the system to request the operating system to perform certain tasks, for example, access a file, allocate memory or interact with hardware devices.

This describes a deliberate choice by the software developer to consider each possible documented system response rather than just ignoring the return values.

All forms of input including those from system calls should be checked to avoid injection attacks or buffer overflow attacks. This may include, but not be limited to, return values of system calls resulting from:

- uploading attachments, which form part of a package sent to the My Health Record
- the use of peripheral device interactions (such as barcode readers).

This can be achieved by the correct management of every known return value and then trapping and handling all other values. The trapped values must be managed in a way that does not compromise the healthcare software system.

Traces:

ISM Security Control 0401:

Secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, and secure programming practices are used as part of application development.

SEC-0220

Penetration testing

If the healthcare software system is accessible via an external endpoint, the system SHALL be penetration tested periodically at an interval not exceeding 12 months since the last test.

Identified vulnerabilities SHALL be addressed and the system re-assessed so that no residual vulnerabilities remain with a rating score higher than 6.9, as determined by the Common Vulnerability Scoring System (CVSS) v3.1.

Priority:

Conditional

Notes:

This requirement applies to systems accessed over the public internet (i.e outside the organisation's network), for example, Software-as-a-Service (SaaS) systems hosted by a third party service provider with a public network, and internal systems that can be accessed from an external endpoint. Accessing an internal network via VPN is not considered an external endpoint.

Penetration testing can be performed by a security organisation or individual testers. The software provider organisation has the flexibility to determine the appropriate security organisation or individual tester that is suitable for their own software system.

Refer to Common Vulnerability Scoring System Specification Document [FIRST2019] for detailed information and documentation with respect to the Common Vulnerability Scoring System (CVSS) v3.1.

Traces:

ISM Security Control 0402:

Applications are comprehensively tested for security vulnerabilities, using both static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.

SEC-0221

Vulnerability testing

If the healthcare software system is not accessible via an external endpoint (i.e internal access only), the system SHALL be vulnerability tested periodically at an interval not exceeding 12 months since the last test.

Identified vulnerabilities SHALL be addressed and the system re-assessed so that no residual vulnerabilities remain with a rating score higher than 6.9, as determined by the Common Vulnerability Scoring System (CVSS) v3.1.

Priority:

Conditional

Notes:

This requirement applies to systems accessed via an internal endpoint only (i.e. internal organisation network), for example, software that is installed on a desktop or internally hosted applications (on premise) that are not accessible via an external endpoint.

Vulnerability assessment can be performed by a security organisation or individual testers. The software provider organisation has the flexibility to determine the appropriate security organisation or individual tester that is suitable for their own software system.

Refer to Common Vulnerability Scoring System Specification Document [FIRST2019] for detailed information and documentation with respect to the Common Vulnerability Scoring System (CVSS) v3.1.

Traces:

ISM Security Control 0402:

Applications are comprehensively tested for security vulnerabilities, using both static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.

3.5 Web application development

The requirements in this section apply to healthcare software systems that are web-based (e.g web pages etc).

SEC-0180 HTTP security policies

If the healthcare software system is a web-based system, the system SHALL implement:

- Content-Security-Policy
- HTTP Strict Transport Security (HSTS)
- X-Frame-Options response headers.

Priority: Conditional

Traces: ISM Security Control 1424:
Web applications implement Content-Security-Policy, HSTS and X-Frame-Options via security policy in response headers.

SEC-0190 HTTPS exclusively

If the healthcare software system is a web-based system with user input, the healthcare software system SHALL serve all web application content exclusively on HTTPS.

Priority: Conditional

Notes: Information about ASD approved cryptographic and hashing algorithms can be found in the Australian Cyber Security Centre's [Guidelines for Cryptography](#) [ACSC2023b].

Traces: ISM Security Control 1552:
All web application content is offered exclusively using HTTPS.

SEC-0170 Output encoding

If the healthcare software system is a web-based system with outputs, the healthcare software system SHALL perform output encoding on all outputs produced.

Priority: Conditional

Notes: Output encoding is the process of replacing HTML control characters (e.g <, >, ", &, etc) into their encoded representatives. This is the best mitigation against cross-site scripting attacks.

Traces: ISM Security Control 1241:
Output encoding is performed on all output produced by web applications.

SEC-0100	Input validation for web-based applications If the healthcare software system is a web-based system, the system SHALL check all inputs (e.g datatypes and lengths) to ensure incorrect and inappropriate inputs are captured and managed without compromising the healthcare software system.
Priority:	Conditional
Notes:	<p>This requirement intends to ensure date fields contain dates, integer fields contain integers etc to protect infrastructure from unnecessary traffic and potential malicious activity.</p> <p>Examples of input validation include:</p> <ul style="list-style-type: none">• ensuring a telephone field does not contain letters• ensuring data used in a Structured Query Language query is sanitised properly• ensuring Unicode input is handled appropriately.
Traces:	<p>Refer to V5.1 Input Validation Requirements in the OWASP Application Security Verification Standard [OWASP2019].</p> <p>ISM Security Control 1240: Validation or sanitisation is performed on all input handled by web applications.</p>
SEC-0385	OWASP Application Security Verification Standard Level 1 If the healthcare software system is a web-based system with user input, the system SHALL follow the Open Worldwide Application Security Project (OWASP) Application Security Verification Standard to Application Security Verification Level 1.
Priority:	Mandatory
Notes:	<p>Level 1 is aimed at applications with low protection needs and is formulated in a way that its requirements can be checked in a penetration test. Level 1 controls can also be checked either automatically by tools or manually without requiring access to source code.</p> <p>Level 1 is considered the minimum required for all applications by OWASP. Refer also to requirement SEC-0220.</p>
Traces:	<p>Refer to the OWASP Application Security Verification Standard [OWASP2019].</p> <p>ISM Security Control 0971: The OWASP Application Security Verification Standard is used in the development of web applications.</p>

SEC-0390	<p>OWASP Application Security Verification Standard Level 2</p> <p>If the healthcare software system is a web-based system with user input, the system SHOULD follow the Open Worldwide Application Security Project (OWASP) Application Security Verification Standard to Application Security Verification Level 2.</p>
Priority:	Recommended
Notes:	<p>Level 2 ensures that security controls are in place, effective, and used within the application. Level 2 is typically appropriate for applications that handle significant business-to-business transactions, including those that process healthcare information, implement business-critical or sensitive functions, or process other sensitive assets, or industries where integrity is a critical facet to protect their business [OWASP2019].</p>
Traces:	<p>Refer to the OWASP Application Security Verification Standard [OWASP2019].</p> <p>ISM Security Control 0971: The OWASP Application Security Verification Standard is used in the development of web applications.</p>

3.6 Application hardening

SEC-0030	<p>Office templates with OLE packages</p> <p>The healthcare software system SHALL NOT use or be dependent on in any way Microsoft Office Templates with Object Linking and Embedding (OLE) packages.</p>
Priority:	Mandatory
Notes:	<p>Microsoft Office OLE Packages should be managed carefully by organisations as an adversary can also create macros to perform a variety of malicious activities.</p> <p>By avoiding the use of OLE Packages healthcare provider organisations may place restrictions on the use of Microsoft Office OLE Packages without having an impact on functionality of the clinical software.</p>
Traces:	<p>ISM Security Control 1542: Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.</p>

SEC-0260	Trusted macro execution The healthcare software system SHALL only permit Microsoft Office Macros that are from trusted locations (refer notes) or restrict all Office Macros. Priority: Mandatory Notes: Refer to the ACSC Microsoft Office Macro Security [ACSC2021a]. Traces: ISM Security Control 1487: Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.
SEC-0040	Office macro signing If the healthcare software system includes any Microsoft Office macros, the macros SHALL be digitally signed using a code signing certificate from a commercial third party Certificate Authority. Priority: Conditional Notes: Microsoft Office Macros should be managed carefully by organisations as an adversary can also create macros to perform a variety of malicious activities. By signing Microsoft Office macros, healthcare provider organisations may place restrictions on the use of Microsoft Office macros while still permitting execution of macros from a third party software provider organisation. Traces: ISM Security Control 1674: Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

SEC-0085	<p>Digital certificate validation</p> <p>If the digital certificate asserts the identity of an external party, or is issued by a trusted third party, the healthcare software system SHALL validate digital certificates.</p> <p>Priority: Conditional</p> <p>Notes: Certificate validation should be done by:</p> <ul style="list-style-type: none"> ensuring the certificate has not been revoked. This may be done by using a Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP) or other method verifying that the certificate is from a valid Certificate Authority. <p>Certificate pinning should be considered. Which is where, for specific web addresses a certificate is 'pinned' so that only certificates from a specific Certificate Authority are accepted.</p> <p>Where the network operation to access the CRL or OCSP fails, the certificate validation should not fail as a result.</p> <p>This requirement does not apply to certificates that are issued locally for internal use only. Internal certificates are likely to have other ways to deal with a compromised private key, e.g. reissue new certificates and private keys internally across all impacted systems.</p> <p>Refer to Appendix A.2 for implementation guidance.</p> <p>Traces: No applicable trace to ISM Security Controls.</p>
SEC-0570	<p>Digital certificate's expiry check</p> <p>The healthcare software system SHALL check the expiry date on digital certificates when the healthcare software system uses the certificate to:</p> <ul style="list-style-type: none"> authenticate an external individual decrypt a message received from an external endpoint <p>Priority: Mandatory</p> <p>Notes: Systems connecting to My Health Record are required to use NASH PKI certificates which are X.509.</p> <p>Refer to the NASH Certificates Developer Guide: https://developer.digitalhealth.gov.au/resources/nash-sha-2-certificates-developer-guide</p> <p>Traces: No applicable trace to ISM Security Controls.</p>

3.7 Operating system hardening

SEC-0310 Microsoft application block rules

If the healthcare software system can be operated on Microsoft Windows, the health software system SHALL not break Microsoft's recommended application block rules.

Priority: Conditional

Notes: For information about Microsoft recommended block rules refer to <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules>.

Traces: ISM Security Control 1544:
Microsoft's 'recommended block rules' are implemented.

SEC-0290 Restriction of executables

The healthcare software system SHOULD NOT allow the unauthorised execution of scripts, installers, executables from within the healthcare software system.

Priority: Recommended

Notes: Functions that allow uncontrolled access to the hard drive and operating system should be disallowed e.g providing a Disk Operating System (DOS) prompt within a healthcare software system.

Traces: ISM Security Control 1657:
Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

3.8 System patching

SEC-0010	Prohibit use of Java Applets or Flash The healthcare software system SHALL NOT use the following technologies: <ul style="list-style-type: none">• Java Applets• Flash.
Priority:	Mandatory
Notes:	This requirement applies specifically to ' <i>Java Applets</i> ' and is not relevant to Java technologies such as J2EE or J2SE. Oracle deprecated Java Applets in Java SE 9 and was removed in Java SE 11.
Traces:	Flash was discontinued in all major web browsers at the end of 2020, meaning that no security patches are available. Refer to https://theblog.adobe.com/adobe-flash-update/ . ISM Security Control 1486: Web browsers do not process Java from the internet. ISM Security Control 1704: Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.
SEC-0020	Prohibit use of Microsoft Office templates with embedded Flash, Silverlight or Shockwave controls The healthcare software system SHALL NOT use or be dependent on Microsoft Office templates in any way that include Flash, Silverlight or Shockwave content.
Priority:	Mandatory
Notes:	Microsoft has stopped support for embedded Flash, Silverlight and Shockwave content. For more details refer to Microsoft's Announcement .
Traces:	ISM Security Control 1704: Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

SEC-0280	Automated deployment mechanism If the healthcare software system is externally hosted, the system SHOULD have an automated mechanism to verify that all applicable security patches and updates are installed and in operation. If there are any issues with the installation or updates, the system SHALL raise an alert to a responsible person. Priority: Recommended Notes: Externally hosted software refers to a system in which its server is hosted outside the boundaries and control of the healthcare organisation. Examples of such systems include Software-as-a-Service (SaaS), hosted cloud services, and hosted web applications provided by third party service providers. A responsible person may be a system administrator or direct supervisor. The alert might be an internal email or text message or some obvious indication to the responsible person inside the healthcare software system. An unobtrusive entry in an audit or transaction log or similar data store is not considered a sufficient alert. Traces: ISM Security Control 0298: A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.
SEC-0300	Patch and update on desktop software If the healthcare software system is installed on a desktop (on premise), the system SHOULD provide an automated mechanism to ensure that systems are patched and updated and applied to client systems. Priority: Recommended Notes: System that is installed on a desktop include software installed from a CD, executables and binaries, and software downloaded from web and installed on premise. Traces: ISM Security Control 0298: A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.

SEC-0301	<p>Patch and update on software internally hosted</p> <p>If the healthcare software system is internally hosted, the system SHOULD provide an automated mechanism to ensure that systems are patched, updated and applied to client systems.</p>
Priority:	Recommended
Notes:	Internally hosted system refers to a system in which its server is hosted within the boundaries and control of the healthcare organisation. Examples of such systems include on premise client/server architectures, and internally hosted application and data that is accessed via a web browser.
Traces:	<p>ISM Security Control 0298:</p> <p>A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.</p>

3.9 Data backup and restoration

SEC-0130	<p>Minimum storage time</p> <p>The healthcare software system SHALL NOT automatically delete or overwrite a backup file for at least 3 months from the time the backup file was created.</p>
Priority:	Mandatory
Notes:	This requirement intends to prevent backup files from automatically removing or deleting from the system. Implementers may choose to configure the time period for longer than 3 months.
Traces:	<p>ISM Security Control 1548:</p> <p>Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.</p>
SEC-0151	<p>Backup and restore functionality</p> <p>The healthcare software system SHALL provide backup and restore functionality. The backup frequency SHALL be at least daily.</p>
Priority:	Mandatory
Notes:	Some healthcare provider organisations will have enterprise-wide backup solution and may wish to disable application-level backup.
Traces:	<p>ISM Security Control 1548:</p> <p>Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.</p>

SEC-0370	Backup scope The healthcare software system SHALL backup the following data: <ul style="list-style-type: none">• all important information• configuration settings. <p>Priority: Mandatory</p> <p>Notes: Important information refers to the critical information that is essential for the functioning and operation of the software in an organisation. The specific types of important data are varied, but generally include (but not limited to): customer and healthcare provider data, clinical documents, system configurations and settings.</p> <p>Traces: ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.</p>
SEC-0140	On-screen backup instructions on desktop software If the healthcare software system is installed on a desktop (on premise), the system SHALL provide on-screen instructions on how to perform backup and restore functionality. <p>Priority: Conditional</p> <p>Notes: Systems that are installed on a desktop or on premise include software installed from a CD, executables and binaries, and software downloaded from web and installed.</p> <p>Traces: ISM Security Control 1548: Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.</p>
SEC-0141	On-screen backup instructions for internally hosted system If the healthcare software system is internally hosted, the system SHALL provide on-screen instructions on how to perform backup and restore functionality. <p>Priority: Conditional</p> <p>Notes: Internally hosted system refers to a system in which its server is hosted within the boundaries and control of the healthcare organisation. Examples of such systems include on premise client/server architectures, and internally hosted application and data that is accessed via a web browser.</p> <p>Traces: ISM Security Control 1548: Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.</p>

4 Compliance Requirements

This section lists the security compliance requirements for software provider organisations. For a software provider organisation to be considered compliant, it must meet the mandatory requirements and all relevant conditional requirements. Conditional requirements are deemed mandatory if the specific conditions are met for the implementation.

While compliance with recommended requirements is not mandated, it is advisable for software provider organisations to comply with recommended requirements where possible, as these requirements may become mandatory in future releases.

Note: the unique numbering of each requirement contained within this section of the profile is not intended to be sequential. Further, any gaps in numbering are intentional and inconsequential. Requirements have been grouped according to the categories of controls outlined in the ISM or a suitable equivalent.

4.1 Access to systems and their resources

SEC-0500	Privileged access policy The software provider organisation SHALL develop and implement a policy of ensuring privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.
Priority:	Mandatory
Notes:	This requirement is easiest implemented by having administrator accounts automatically expire after 12 calendar months.
Traces:	ISM Security Control 1507: Requests for privileged access to systems and applications are validated when first requested.

4.2 Application development

SEC-0430	Access to source code The software provider organisation SHALL ensure that proprietary source code cannot be accessed by unauthorised persons.
Priority:	Mandatory
Traces:	ISM Security Control 1422: Unauthorised access to the authoritative source for software is prevented.

SEC-0400	Platform-specific programming practices The software provider organisation SHALL ensure platform-specific secure programming practices are used when developing software.
Priority:	Mandatory
Notes:	Refer to platform-specific guidance such as: <ul style="list-style-type: none">• Common Weakness Enumeration (CWE) top 25: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html• Microsoft .NET secure coding guidelines: https://docs.microsoft.com/en-us/dotnet/standard/security/secure-coding-guidelines• OWASP Application Security Verification Standard [OWASP2019].
Traces:	ISM Security Control 0401: Secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, and secure programming practices are used as part of application development.
SEC-0440	Threat modelling and secure design The software provider organisation SHALL implement threat modelling and other secure design techniques to ensure that threats to software and mitigations to those threats are identified and accounted for.
Priority:	Mandatory
Notes:	Refer to the Open Worldwide Application Security Project (OWASP) Threat Modelling guide: https://owasp.org/www-community/Application_Threat_Modeling .
Traces:	ISM Security Control 1238: Threat modelling is used in support of application development. ISM Security Control 0401: Secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, and secure programming practices are used as part of application development.

SEC-0420	<p>Security vulnerability notification</p> <p>The software provider organisation SHALL notify the Australian Digital Health Agency and all customers using the software, within 14 calendar days of security vulnerabilities discovered after the software is in production/use.</p> <p>Priority: Mandatory</p> <p>Traces: ISM Security Control 0298: A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.</p>
SEC-0520	<p>Separate production environment from testing and development environments</p> <p>The software provider organisation SHALL operate the production environment separate from testing and development environments.</p> <p>Priority: Mandatory</p> <p>Traces: ISM Security Control 0400: Development, testing and production environments are segregated.</p>
SEC-0540	<p>Modifying software in development or testing environment</p> <p>If the healthcare software system is externally hosted, the software provider organisation SHALL only make changes to the software's source code and master data in the development and/or testing environments prior to deploying to the production environment.</p> <p>Priority: Conditional</p> <p>Traces: ISM Security Control 1419: Development and modification of software only takes place in development environments.</p>
SEC-0530	<p>Separate testing environment from development environments</p> <p>The software provider organisation SHOULD operate development and testing environments as segregated environments.</p> <p>Priority: Recommended</p> <p>Traces: ISM Security Control 0400: Development, testing and production environments are segregated.</p>

SEC-0560	Independent library testing The software provider organisation SHOULD ensure that all independent libraries used within their software are tested for security vulnerabilities prior to any release.
Priority:	Recommended
Traces:	ISM Security Control 0402: Applications are comprehensively tested for security vulnerabilities, using both static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.

4.3 System patching

SEC-0250	Patch and updating approach The software provider organisation SHALL implement a centralised and managed approach and process that maintains the integrity of patches or updates to ensure that all required system components and patches are in place and current.
Priority:	Mandatory
Notes:	The centralised and managed approach is used to patch or update applications, operating systems, drivers and firmware, and ensures that they have applied successfully.
Traces:	ISM Security Control 0298: A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.
SEC-0410	End of support notifications The software provider organisation SHALL notify all known customers of a software product and the Agency when the system or version is no longer supported or receiving security updates.
Priority:	Mandatory
Traces:	ISM Security Control 0304: Applications that are no longer supported by vendors are removed.

SEC-0460	<p>Patch and update drivers and firmware</p> <p>If the healthcare software system is externally hosted, the software provider organisation SHALL develop and enact a policy where security vulnerabilities in applications, drivers and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of release or within 48 hours if there is a known exploit.</p> <p>Priority: Conditional</p> <p>Traces: ISM Security Control 1697: Patches, updates or vendor mitigations for security vulnerabilities in drivers and firmware are applied within two weeks of release, or within 48 hours if an exploit exists.</p>
SEC-0470	<p>Patch and update operating system and firmware</p> <p>If the healthcare software system is externally hosted, the software provider organisation SHALL develop and enact a policy for security vulnerabilities to be patched, updated or mitigated within two weeks of release, or within 48 hours if there is a known exploit.</p> <p>Priority: Conditional</p> <p>Traces: ISM Security Control 1694: Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.</p>
SEC-0480	<p>Supported operating systems and ICT equipment</p> <p>If the healthcare software system is externally hosted, the software provider organisation SHALL replace or update operating systems for servers and ICT equipment when the operating systems are no longer supported (i.e patches or updates for security vulnerabilities are no longer available).</p> <p>Priority: Conditional</p> <p>Traces: ISM Security Control 1501: Operating systems that are no longer supported by vendors are replaced.</p>

4.4 Data backup and restoration

SEC-0510	Source code backup The software provider organisation SHALL backup their source code regularly. Priority: Mandatory Notes: The source code backup should be retained with a frequency and retention timeframe in accordance with business continuity requirements within the organisation. Traces: ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.
SEC-0131	Backup retention If the healthcare software system is externally hosted, the software developer organisation SHALL ensure that backup files are retained for a period enabling the software to restore to a point within the last 3 months. Priority: Conditional Traces: ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.
SEC-0380	Full back up testing If the software provider organisation offers backup services, the backup SHALL be tested through a full restoration at least once when initially implemented, and then each time fundamental information technology infrastructure changes occur. Priority: Conditional Traces: ISM Security Control 1515: Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises.

Appendix A Implementation guidance

A.1 Breached credential service

Services exist that allow for the checking of user credentials and whether they have been exposed within a security breach. These services differ from simple credential checking as they do not just use an algorithm, they use a database of known breached credential information.

These services are highly effective at reducing compromises to systems that only use single factor for authentication such as username/id and password. However, they should be used in conjunction with other controls such as Multi-factor Authentication mechanisms, since breached credential lists are only updated when the credential breaches are discovered by the breached credential service operators.

Several industries perform this check on their customer accounts at registration and credential change as a good control against password spray and other security attacks.

Some useful guidance links include:

- 2019-130: Password spray attacks – detection and mitigation strategies [ACSC2019]
- Creating Strong Passphrases [ACSC2021b]

One way to check your credentials is by using the service *'Have I been Pwned'*.

This service is referred to by ACSC and has an API for cloud use or a method for offline use that requires manual syncing to the resource.

A risk-based approach should be used to determine how often an organisation should update their breached credential list if they choose the offline method.

API: <https://haveibeenpwned.com/API/v3>.

Password Lists: <https://haveibeenpwned.com/Passwords>.

A.2 Digital Certificate Validation

Implementation advice for the validation of digital certificates and use of Certificate Authorities (CAs):

- It is recommended that software developers are using CAs and certificates which implements Certificate Transparency (CT), except when NASH certificates are used.
- The National Authentication Service for Health (NASH) is a PKI that was established for healthcare in Australia and is highly recommended as a PKI solution, (refer <https://www.servicesaustralia.gov.au/national-authentication-service-for-health>).

Useful links:

- RFC5280: Technical detail for certificate validation (<https://www.ietf.org/rfc/rfc5280.txt>)
- National Institute of Standards and Technology (NIST) provided resources for testing PKI implementations, including certificate validation and path checking (<https://csrc.nist.gov/projects/pki-testing>)

Acronyms

Acronym	Description
ACSC	Australian Cyber Security Centre
API	Application Programming Interface
ASD	Australian Signals Directorate
B2B	Business-to-business
CA	Certificate Authorities
CAS	Conformance Assessment Scheme
CRL	Certificate Revocation List
CT	Certificate Transparency
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DOS	Disk Operating System
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer (SSL)
ICT	Information and Communications Technology
ISM	(Australian Government) Information Security Manual
J2EE	Java 2 Platform Enterprise Edition
J2SE	Java 2 Standard Edition
MFA	Multi-factor authentication
NASH	National Authentication Service for Health
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OLE	Object Linking and Embedding
OWASP	The Open Worldwide Application Security Project
PKI	Public Key Infrastructure
SaaS	Software as a Service
SFA	Single-factor authentication
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Acronym	Description
VPN	Virtual Private Network
XSS	Cross-site Scripting
UC	Use cases developed to provide a structure to the sections within this document.
URL	Uniform Resource Locator

Glossary

Term	Meaning
Breached credentials service	A known breached credentials service is a service which provides either an application programming interface (API) to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.
Cryptographic Algorithm	An algorithm used to perform cryptographic functions such as encryption, integrity, authentication, digital signatures or key establishment.
CVSS	An open framework for communicating the characteristics and severity of software vulnerabilities.
External endpoints	Access to systems over the public internet (i.e outside the organisation's network), for example, Software-as-a-Service (SaaS) systems hosted by a third party service provider with a public network, and internal systems that can be accessed from an external endpoint. Accessing an internal network via VPN is not considered an external endpoint.
Externally hosted system	A system in which its server is hosted outside the boundaries and control of the healthcare organisation. Examples of such systems include Software-as-a-Service (SaaS), hosted cloud services, and hosted web applications provided by third party service providers.
Healthcare software system	Software and the environment that provides healthcare information to either healthcare providers, healthcare consumers or both.
Hosted Service Provider	Business that delivers IT functions such as infrastructure, applications, security, monitoring, storage, web development, website hosting and email, over the Internet or other wide area networks.
Internally hosted system	A system in which its server is hosted within the boundaries and control of the healthcare organisation. Examples of such systems include on premise client/server architectures, and internally hosted application and data that is accessed via a web browser.
OWASP	Open Worldwide Application Security Project which provides comprehensive resources for software developers that should be followed when developing web applications.
Passphrase	<p>A sequence of words used for authentication. [ACSC2021b]</p> <p>Passphrases are made up of four or more random words making them longer than a traditional password. This makes them harder to guess but easy to remember. Changing your passwords to a passphrase is a great way to improve your cyber security. For example, "red house sky train". [ACSC2021e]</p>
Penetration test	A method of evaluating the security of an ICT system by seeking to identify and exploit vulnerabilities to gain access to systems and data. Also called a 'pen test', it is a test using real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical systems or information.
Responsible person	A responsible person may be a system administrator or direct supervisor. The alert might be an internal email or text message or some obvious indication to the responsible person inside the healthcare software system. An unobtrusive entry in an audit or transaction log or similar data store is not considered a sufficient alert.

Term	Meaning
Privileged user	A user who can alter or circumvent a system's security measures, access and modify system configurations, account privileges, and audit logs, and access important data repositories. This can also apply to users such as software developers, who may have only limited privileges, but can still bypass security measures.
Privileged account	Refer to 'Privileged user'
Salt	A unique, randomly generated string that is added to each password as part of the hashing process. As the salt is unique for every user, an attacker has to crack hashes one at a time using the respective salt rather than calculating a hash once and comparing it against every stored hash. This makes cracking large numbers of hashes significantly harder, as the time required grows in direct proportion to the number of hashes.
SHALL	When appearing in a conformance requirement, this verb SHALL indicates a mandatory requirement. Its negative form SHALL NOT indicates a prohibition.
SHOULD	When appearing in a conformance requirement, this verb SHOULD indicates a recommendation. Its negative form SHOULD NOT indicates an option that should not be supported.
Software as a Service	Software that is either supplied as a cloud-based service or deployed over the Internet to run locally. Licenses and support for SaaS systems are commonly provided on a subscription basis, but other models are also used.
Vulnerability assessment	A documentation-based review of a system's design, an in-depth hands-on assessment, or automated scanning with software tools. In each case, the goal is to identify as many security vulnerabilities as possible.

References

- ACSC2019 *2019-130: Password spray attacks – detection and mitigation strategies*, Australian Cyber Security Centre, August 2019
- ACSC2021a *Microsoft Office Macro Security*, Australian Cyber Security Centre, October 2021
- ACSC2021b *Creating Strong Passphrases*, Australian Cyber Security Centre, October 2021
- ACSC2023a *Information Security Manual*, Australian Cyber Security Centre, March 2023
- ACSC2023b *Guidelines for Cryptography*, Australian Cyber Security Centre, June 2023
- AGENCY2023 *My Health Record System Conformance Assessment Scheme*, Australian Digital Health Agency, 2023
- FIRST2019 *Common Vulnerability Scoring System Specification Document*, Forum of Incident Response & Security Teams, August 2019. Available at: <https://www.first.org/cvss/v3.1/specification-document>
- OWASP2019 *Application Security Verification Standard 4.0* (Section V5.1 Input Validation Requirements), Open Worldwide Application Security Project, March 2019. Available at: <https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf>