Cyber Security Policy

Integrated Third Party Security Policy

This document is suitable for release to
Software Developers on a need-to-know basis

Status:	Release
Authority:	Chief Information Security Officer (CISO)
Issuer:	Cyber Security Branch
Dissemination limiting marking:	**OFFICIAL**
Version:	1.0
Initial issue:	18 November 2019
Latest revision:	18 November 2019

Table of Contents

1. Scope

This policy applies to any software developer developing, implementing or providing software for use by medical practitioners, health funds, pharmacies, hospitals, aged care facilities and other services that use Application Programming Interfaces (APIs) or Web Services provided by the Department of Human Services (the department).

2. Objective

The objectives of this policy are to:

1. Enable software developers to develop and provide secure code for use with departmental APIs and Web Services;
2. Reduce the risk to the department posed by third parties supplying software that use APIs and Web Services provided by the department;
3. Reduce the risk of compromise of departmental customers' data; and
4. Support interface agreements entered into with the department.

3. Background

Over recent years, the Australian Government has increased its security stance in response to the change in the threat environment facing Australian Government agencies. The large number of software developers providing software services to the medical and other industries that support departmental activities increases risk to the department. To reduce this risk, the department provides APIs and Web Services to software developers to facilitate online claiming and data transfer. This policy outlines the minimum security requirements for software developers to utilise these APIs and Web Services.

4. Terminology

The following table defines the terms used to describe this policy.

Term	Description
MUST	This word, or the terms 'REQUIRED' or 'SHALL', means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase 'SHALL NOT', means that is an absolute prohibition of the specification.
SHOULD	This word, or the adjective 'RECOMMENDED', means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase 'NOT RECOMMENDED' means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full

Term	Description
	implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective 'OPTIONAL', means that an item is truly optional.

5. Software Developer Requirements

Software developers developing, implementing or providing software that integrates with departmental APIs or Web Services **must** ensure:

1. All software and application development, testing, operation and support is conducted within Australia, unless otherwise approved by the department in advance and in writing.
2. All production data is held within Australian jurisdiction.
3. Data at rest is encrypted using an Australian Cyber Security Centre (ACSC) approved algorithm [1];
4. Cyber Security Incidents brought to the attention of the software developer are reported to the department[1] promptly, no longer than 12 hours after becoming aware of the incident. Cyber Security Incidents include but are not limited to:
    a. Compromise of Provider Digital Access (PRODA) credentials;
    b. Patient data breaches;
    c. Software developer data breaches; and
    d. Any breach of environments that affect the integrity of the software product, including third party environments.

In addition, software developers developing, implementing or providing software that integrates with departmental APIs or Web Services **should**:

5. Ensure security code review is conducted as part of the software development life cycle. Code review results are not required by the department, but confirmation that code review has occurred and findings remediated should be reported as part of the product certification process[2].
6. Ensure penetration testing of the software is conducted after integration of each major API or Web Service release. Test results are not required by the department, but confirmation that penetration testing has occurred and an appropriate remediation plan is in place should be reported as part of the product certification process[2].
7. Develop strategies to achieve compliance with the Australian Cyber Security Centre's Essential Eight [2] to maturity level three, which includes:
    a. Application whitelisting
    b. Patching applications
    c. Configuring Microsoft Office macro settings to block untrusted macros

[1] Contact DHS.CYBER.SECURITY@humanservices.gov.au
[2] This requirement will become mandatory from March 2022

d. Application hardening
e. Restricting administrative privileges
f. Patching operating systems
g. Multi factor authentication
h. Daily backups.

6. Cloud Provider Requirements

In addition to section 4, software developers developing, implementing or providing software that integrates with departmental APIs or Web Services and where the software is hosted within a cloud environment tenanted by multiple parties **must** ensure:

1. Cloud computing providers are listed on the ACSC's Certified Cloud Services List.
2. All production data is held within Australian jurisdiction.

In addition to the above, software developers developing, implementing or providing software that integrates with departmental APIs or Web Services and where the software is hosted within a cloud environment tenanted by multiple parties **should** ensure:

3. Software hosted by the cloud computing provider resides on server infrastructure physically dedicated to Australian Government use; and
4. Permanent privileged access to cloud infrastructure is limited to individuals who are Australian citizens and hold Australian Government Negative Vetting Level 1 security clearances or above.

7. Glossary of Terms

Term	Description
Application Programming Interfaces (APIs)	A set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.
Cloud Computing	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. – NIST SP800-145
Production Data	Production data means all data used in digital transactions with the department for the purpose of accessing government payments and services.
Software	Application that integrates the department's APIs, processes and stores production data, and associated data repositories.
Software Developer	The legal entity responsible for the development of a product which interfaces with Department of Human Services' ICT Systems

8. References

[1] Australian Cyber Security Centre (ACSC) Cryptographic evaluations (ACSC website).

[2] Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model (ACSC website).