Australian Government
Services Australia

Cyber Security Policy

Integrated Third Party Security

This document is intended for use by third party software developers on a need-to-know basis.

This policy describes the requirements for third party software developers engaged in the development and implementation of software which are supported by Services Australia's development material; and Application Programming Interfaces (APIs) or Web Services.

Status:	Endorsed
Authority:	Chief Information Security Officer (CISO)
Issuer:	Cyber Security Branch
Dissemination limiting marking:	**OFFICIAL**
Version:	2.1
Latest revision date:	29/07/2020
Initial issue date:	18/11/2019

Table of Contents

1. Introduction

This policy describes the security requirements for third party software developers engaged in the development and implementation of software which are supported by Services Australia's (the agency) development material; and Application Programming Interfaces (APIs) or Web Services under the relevant contractual agreements.

2. Objectives

The objectives of this policy are to:

1. Enable software developers to develop and provide secure code for use with agency APIs and Web Services.
2. Reduce the risk to the agency posed by third parties supplying software that use APIs and Web Services provided by the agency.
3. Reduce the risk of compromise of customer data.
4. Support relevant agreements establishing contractual relationships between third party software developers and the agency.

3. Terminology

The following table defines the terms used to describe accountabilities and application of controls within cyber security policies.

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 it 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 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.

4. Software Developer Requirements

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

1. All software and application development, testing, operation and support is conducted within Australia, unless otherwise approved by the agency in advance and in writing.
2. All production data is held within Australian jurisdiction, including where the software is hosted within a cloud environment.
3. The data is encrypted at rest and in transit using an Australian Signals Directorate approved algorithm, including where the software is hosted within a cloud environment.
4. Cyber security incidents are reported to the agency promptly and no longer than 12 hours after becoming aware of the incident. Cyber Security Incidents include, but are not limited to:
    - Compromise of Provider Digital Access (PRODA) credentials
    - Data breaches
    - Software developer data breaches
    - 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 agency APIs or Web Services **should** ensure that:

1. Security code review is conducted as part of the software development life cycle. Code review results are not required by the agency, but confirmation that code review has occurred and findings remediated should be reported as part of the product certification process.
2. Penetration testing of the software is conducted after integration of each major API or Web Service release. Test results are not required by the agency, 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. This requirement will become mandatory from March 2022.
3. Strategies are implemented to achieve compliance with the Australian Cyber Security Centre’s Essential Eight to maturity level three, which includes:
    - Application control (i.e. Application whitelisting)
    - Patching applications
    - Configuring Microsoft Office macro settings to block untrusted macros
    - Application hardening
    - Restricting administrative privileges
    - Patching operating systems
    - Multifactor authentication
    - Daily backups

5. Cloud Services Requirements

Software developers developing, implementing or providing software that integrates with agency APIs or Web Services and where the software is hosted within a cloud-based system or environment **must** ensure that:

1. Any cloud-based system or environment which processes, stores or transmits any official information provided by the agency has a current Information Security Registered Assessors Program (IRAP) assessment funded by the cloud service provider. The agency will not be held responsible for funding or conducting the IRAP assessment.
2. The IRAP assessment is reviewed in the context of any major change of administrative or technical environment that may impact on the effectiveness of any information security controls on which the assessment relies.
3. The security controls and configuration recommended by the IRAP assessor on the cloud-based system or environment are implemented and operated in the manner and scope in which the recommendations were intended. For example, the vendor cannot use an IRAP assessed cloud service provider in a location that was not assessed as part of the IRAP assessment, or use additional products offered by the provider which were not included in the scope of the IRAP assessment.
4. The ongoing compliance of the cloud-based system or environment is reported as requested by the agency.
5. A copy of an IRAP report concerning any system or environment covered by this policy is provided to the agency.

The agency may revoke the approval of any system or environment that is determined by the agency to be non-compliant with this policy.

For any clarification of the above requirements, the vendor or the service provider must contact the Services Australia Cyber Security Advisor at ITSA@Servicesaustralia.gov.au.

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

1. Software hosted by the cloud computing provider resides on server infrastructure physically dedicated to Australian Government use and is segregated from other government or non-government data.
2. 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.

6. Glossary of Terms

Definition or Acronym	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.
ACSC	The Australian Cyber Security Centre
ASD	Australian Signals Directorate
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. network, servers, storage, applications, and services) which can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST SP800-145)
Data Breach	A data breach occurs when personal or sensitive information that an entity holds has been accessed or disclosed to unauthorised entities. A data breach may be caused by malicious action, human error or failure in information handling or security systems. (Office of the Australian Information Commissioner, 2019)
Development Material	The specifications, requirements, software, test plans, tools (e.g. chat bots) and other material issued by the agency to software developers. This includes all intellectual property, media, documents and other property contained in agency material or provided to the software developers from time to time; and any updates and new releases of agency material.
IRAP	Information Security Registered Assessors Program
NIST	National Institute of Standards and Technology
Personal Information	The *Privacy Act 1988* defines ‘personal information’ as information or opinion about an identified individual, or information that an individual can be reasonably identified by, whether or not it is true or has been recorded. Common examples include a person’s name, signature, home address, email address, telephone number, date of birth, medical records, bank account details and employment details. (Office of the Australian Information Commissioner, 2017)
Production Data	Production data means all data used in digital transactions with the agency for the purpose of accessing government payments and services.
Sensitive Information	The *Privacy Act 1988* defines ‘sensitive information’ as: (a) information or an opinion about an individual’s: (i) racial or ethnic origin; or

	(ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
Software	Application that integrates the agency’s APIs, processes and stores production data, and associated data repositories.
Software Developer	The legal entity responsible for the development of a product which is supported by the agency’s development material; and Application Programming Interfaces (APIs) or Web Services under the relevant contractual agreement.