Suggested Security Clauses for Suppliers

How to Use this document

<Change all items in yellow to align with your business needs/names.>

[Instruction: read these instructions then remove when document is complete.]

Disclaimer

This Content is not comprehensive and is for general information purposes only. This is not legal advice. It does not take into account your specific needs, objectives or circumstances, and it is not advice. While we use reasonable attempts to ensure the accuracy and completeness of the Content, we make no representation or warranty in relation to it, to the maximum extent permitted by law. For further information about the use of InfoSecAssure tools and templates please refer to the InfoSecAssure Website Terms of Use.

Table of Contents

[Right click and refresh table to update table of contents.]

[Suggested Definitions 3](#_Toc116337506)

[Suggested Security Clauses 4](#_Toc116337507)

[Cover email to Supplier 8](#_Toc116337508)

[[subscribe to InfoSecAssure to get access to our communications templates] 8](#_Toc116337509)

## Suggested Definitions

We would like to request a definitions section be added to the contract to ensure we understand terms used.

Here are the definitions we use in our suggested clauses:

**Industry Best Practice Security Standards** means those standards, protocols, requirements and specifications which meet sound industry practice requirements in relation to information technology, security, cybersecurity, privacy and record retention policies, including, as at the Effective Date, alignment with:

(a)             ISO 27001 (together with any associated ISO standards and guidelines such as ISO 27002), as modified, updated or replaced from time to time throughout the Term;

(b)             any other standards that become part of sound industry practice requirements during the Term (including any such standards as ISO 27017 and ISO 27018 relating to cloud); and

(c)             sound industry practice cybersecurity frameworks.

**Information Assets** means all information and information technology, including software, hardware, Cyber Critical Systems, <company name> Data and <company name> Materials, relating to or connected with the Agreement.

**Material Security Weakness** means a material Vulnerability or Information Security weakness in any Information Security Controls which is reasonably likely to result in an Information Security Incident, and which <supplier name> reasonably determines it cannot remediate in a timely manner.

<company name> **Data** means all data and information relating to <company name> and its operations, facilities, customers, clients, personnel, assets and programs in whatever form that information may exist and whether entered into, stored in, generated by or processed as part of the Services and any other data relating to the Service, including Personal Information and <company name>’s Confidential Information.

## Suggested Security Clauses

[Below is a suggested list of security clauses you may wish to consider in your contract negotiations with suppliers.]

[Use the security clauses that work the particular vendor and type of service they are offering. For example if a vendor is just providing a software license then you may only wish them to sign up for clauses that ensure they keep the security of the software current i.e provide you with security patches in a timely manner]

Please find below our suggested amendments in relation to security.

1. Information Security Controls generally
	1. At all times in the performance of and in connection with the Agreement, <supplier name> must, in respect of the Information Assets, establish, implement, maintain, enforce and continuously improve Information Security Controls which comprehensively ensure the Information Security of all those Information Assets.
	2. The Information Security Controls must:
		1. form part of a risk management program in relation to those Information Assets, including identifying Information Security Incidents and establishing and maintaining safeguards against them;
		2. in any event be no less rigorous than those controls required to meet Industry Best Practice Security Standards;
		3. be commensurate with:
			1. Vulnerabilities and Threats to the Information Assets;
			2. the Criticality and Sensitivity of the Information Assets;
			3. the stage at which the Information Assets are within the process from planning and design through to decommissioning and disposal of the Information Asset; and
			4. the potential consequences of an Information Security Incident;
		4. ensure that appropriate levels of security are applied to the Information Assets to protect against:
			1. security breaches;
			2. fraudulent access to any <company name> Data contained in the Information Assets;
		5. hacking;
			1. infecting with viruses;
			2. other direct or indirect attacks that may corrupt <company name> Data and/or the Information Assets; and
	3. ensure that Vulnerabilities in respect of the Information Assets do not result in Information Security Incidents that adversely impact <company name> or its clients and customers or prevent <supplier name> from delivering the Services or performing its obligations under the Agreement and are managed in a manner which is consistent with, and no less rigorous than, Industry Best Practice Security Standards.
2. Harmful Code
	1. The Information Security Controls referred to in clause X.X must:
		1. include such Information Security Controls as necessary or desirable to prevent intrusions, viruses, trojan horses, worms, time bombs and other similar harmful software (Harmful Code) which may affect Information Security; and
		2. in respect of any software deployed or provided in the delivery of the Services, ensure that such Information Security Controls incorporate relevant security testing to prevent the implementation of Harmful Code.
3. Access
	1. <supplier name> must implement Information Security Controls to ensure that:
		1. only Personnel with a legitimate need are able to access the Information Assets and only to the extent required to perform their role in relation to the Agreement;
		2. no persons other than those with Authorised Access are able to access the Information Assets;
		3. those Personnel with Authorised Access do not exceed the scope of their Authorised Access.
	2. <supplier name> must, upon written notice by <company name>, provide <company name>’s Personnel with a list of Personnel who have access to Information Assets and the level of access to the Information Assets.
4. **Personnel**
	1. <supplier name> must implement and comply with appropriate controls (including background checks) for all of its Personnel who have administration level access, who have any access to information Assets, or who have access to or control any critical part of, the Information Assets.
5. **Fourth Parties**
	1. <supplier name> may engage any entity that uses or will use the Information Assets of <supplier name> to perform any part of <supplier name>’s obligations under the Agreement (Fourth Party).
	2. <supplier name> must:
		1. inform <company name> of any Fourth Party;
		2. ensure that it has legally binding arrangements in place with any Fourth Party;
		3. ensure any Fourth Party has equivalent or more stringent Information Security Capability obligations than those set out in this Addendum imposed on <supplier name>; and
		4. procure that the Fourth Party complies with those obligations.
	3. <supplier name> will remain fully responsible for any acts and omissions of a Fourth Party in connection with the Agreement and indemnifies and must keep indemnified <company name> and their Personnel against all losses, expenses, costs (including legal costs on a full indemnity basis), claims or actions arising, either directly or indirectly, in connection with such acts and omissions.
6. **Data sovereignty**
	1. Other than as expressly provided in the Agreement, in the performance of and in connection with the Agreement, <supplier name> must not (and to be clear, must ensure that its Personnel or Fourth Parties do not), without the express prior written authorisation of <company name>, use, transfer or relocate any or all Information Assets relating to or connected with the Agreement (including <company name> Data), to a jurisdiction outside Australia.
7. **Response to Information Security Incidents and material weaknesses**
	1. <supplier name> must:
		1. promptly, and in any case within:
			1. 48 hours, notify <company name> in writing upon becoming aware of any Information Security Incident or imminent Threat of an Information Security Incident; and
			2. 5 Business Days, notify <company name> in writing upon becoming aware of a Material Security Weakness;
		2. take all reasonable steps to investigate the cause of the Information Security Incident or Material Security Weakness, mitigate the impact of, and remediate, such incident or rectify any Material Security Weakness in a timely manner having regard to the risk factors, and advise remediation steps, and a timetable for restoration of any compromised Information Assets or processes;
		3. provide <company name> with a post-incident report, regular updates in relation to the remediation activity (until such time as the Information Security Incident is resolved);
		4. co-operate with the OAIC or any Regulator in any investigation in relation to such Information Security Incident;
		5. promptly respond to any security related questions received from the OAIC or a Regulator and provide related materials upon request;
		6. promptly remediate the Information Security Incident (except to the extent such Information Security Incident is caused by <company name>’s failure to perform its obligations under this Agreement) or rectify any Vulnerabilities in its Information Assets or Material Security Weakness, and implement any recommendations relevant to its security obligations under the Agreement; and
		7. use all reasonable endeavours to prevent a recurrence of such Information Security Incident except to the extent such Information Security Incident is caused by <company name>’s failure to perform a task which falls within the scope of <company name>’s responsibilities under the Agreement.
8. **Testing program and implementation**
	1. <supplier name> must, in respect of the Information Assets, implement, maintain and execute a program for testing:
		1. Information Security Controls referred to in clause xxx;
		2. <supplier name> Information Security Incident response plans.
9. **Reporting and remediation**
	1. <supplier name> must provide to <company name> a copy of a report of all test results of annual penetration testing (limited to those results which relate to <company name> and the Information Assets).
10. **Certifications and security audits conducted or maintained by** <supplier name>
	1. Upon written request, <supplier name> must promptly provide <company name> with copies of the following, to contain (at a minimum) full and complete details of certifications insofar as they relate to, or could potentially relate to, <company name>, the Services or the Information Assets:
		1. all certifications obtained in connection with any of the Industry Best Practice Security Standards (including any associated “statements of applicability”);
		2. all reports relating to external audits performed in relation to Information Assets required in connection with any of the Industry Best Practice Security Standards; and
	2. In relation to clause 7(b) ii) above, where <supplier name> is precluded from providing <company name> with copies of any of the foregoing (due to security or confidentiality concerns), <supplier name> must provide access to copies of the same in a <supplier name> ‘read room’ environment where <company name> can review the material but not take copies or notes.
11. **Independent security investigations**
	1. Where reasonably requested by <company name>, <supplier name> must, in respect of the Information Assets, co-operate with any investigation relating to Information Security which is carried out on behalf of <company name> or by any law enforcement or Regulator.
12. **Assurance**
	1. <supplier name> must, on at least 20 Business Days’ notice, permit and provide persons nominated by <company name> (excluding a competitor of <supplier name>) supervised access during normal business hours, or as otherwise agreed, to:
		1. the Information Assets and Information Security Control environment;
		2. <supplier name> Information Security Policy Framework, including responding to <company name>’s security questionnaire, any third party assurance attestation letters describing results of penetration testing on <supplier name>’s internal data network, third-party assurance reports or assessment or certificates of registration verifying the effectiveness of <supplier name>’s cybersecurity controls as it relates to services provided to <company name>; and
		3. procedures to the extent such third-party reports or assessments or certificates of registration are available with respect to the Information Assets,
	2. for the purpose of conducting an assurance in relation to compliance with this Addendum, including reviewing the design and operating effectiveness of Information Security Controls (Information Security Control Assurance).
	3. <company name> may not request more than one Information Security Control Assurance per calendar year, except where:
		1. <company name>, acting reasonably is concerned about <supplier name>’s compliance with this Addendum;
		2. <company name>, has reasonably taken into account the impact of a potential Information Security Incident and the ability to place reliance on other control testing undertaken; or
		3. there have been changes to Vulnerabilities and Threats or material changes to the Information Assets.
	4. <company name> will bear its own costs associated with conducting an Information Security Control Assurance.
	5. <supplier name> must provide appropriately skilled persons and a nominated contact list to <company name> to enable it to conduct an Information Security Control Assurance.
	6. <supplier name> must, on request by <company name>, provide <company name> with all reasonable assistance to support an audit of <company name>’s IT Controls e.g. ISO 27001 Audit or SOC 2 Audit
	7. Without limiting anything else in this Addendum, in the event that <company name> reasonably seeks further information relating to <supplier name>’s cybersecurity or other information security controls and procedures, <supplier name> will make relevant subject-matter experts available in person, or by telephone, to answer <company name>’s questions and otherwise provide information and material, in relation to the Information Assets and Information Security within a reasonable period.

## Cover email to Supplier

### [subscribe to InfoSecAssure to get access to our communications templates]

[Adjust this cover email to send to your supplier when requesting changes to your agreement]

[Subject:] Requested amendment to standard contract between <supplier name> and <company name>.

[Body:]

<company name> would like to request amendments to our services contract <name of contract> to ensure we have the right governance in place to support our ongoing and productive relationship.

Reason for our request

* X
* X
* X
* X
* X

We are happy to talk you through our suggested changes.

We will consider making changes if required however we believe xxx

In needed we can also xxxx

We think you will find when you read our suggested changes they are reasonable and allow you to determine your own security program and governance approach xxxxxx