

Schedule 4

Data Security

About this Schedule

This schedule is specifically incorporated by reference into the Master Services Agreement between the Customer and Supplier to the extent it relates to the security measures taken by the Supplier.

1. **Supplier Security Practices**

1.1 Supplier will develop, implement, operate and maintain security policies, systems, standards and procedures, which:

- (a) are consistent with Best Industry Practice, having regard to the nature of Supplier's Services and associated security risks;
- (b) are certified to or aligned with ISO/IEC 27001 and 27002;

(Supplier Security Practices).

1.2 Supplier will:

- (a) at all times comply with Supplier Security Practices;
- (b) ensure that Supplier's Personnel comply with Supplier Security Practices;
- (c) provide Supplier Personnel with appropriate training on Supplier Security Practices;
- (d) provide confirmation to Customer, as reasonably requested by Customer from time to time, regarding compliance with Supplier Security Practices by Supplier and Supplier's Personnel;

(e) regularly review and update if required Supplier Security Practices, and

(f) have a documented change control process for systems documentation associated with Supplier Security Practices.

2. **Risk Management**

2.1 Supplier will:

- (a) implement a defined risk management process or methodology that describes how Supplier intends to assess, respond, and monitor risk as well as implement risk management compliance consistently across the organisation;
- (b) formalise a defined risk assessment approach that includes requirements to conduct a risk assessment (such as impact analysis and risk treatment options) as well as any necessary reporting of the risk assessment results; and
- (c) ensure risk owners are assigned to identified risks.

3. Data sovereignty

Supplier will not use any Cloud Infrastructure outside of Australia to store or process any Customer Data without obtaining Customer's prior written approval, which may be given or withheld at Customer's reasonable discretion and subject to any conditions required by Customer.

4. Notifiable Security Incident

4.1 Supplier will:

- (a) have a nominated contact to provide information to Customer in the event of a Notifiable Security Incident and notify Customer of Notifiable Security Incidents through agreed upon channels;
- (b) where a Notifiable Security Incident has occurred, reasonably cooperate in any legal action necessary for Customer to protect its rights relating to Customer Data, Customer's Network and Facilities and Customer Personnel; and
- (c) if reasonably requested, provide Customer with a copy of its security incident management process.

4.2 Supplier will notify Customer as soon as it becomes aware, and promptly confirm in a written security report to Customer:

- (a) any breach of Supplier's activities in compliance with this Schedule or Supplier Security Practices;

- (b) any threatened or actual Security Incident involving Supplier or Supplier Personnel;
- (c) any security failure or vulnerabilities (including any Malware in any software) which could or do compromise the security of any Customer Data or Customer's Network and Facilities or Customer Personnel; and
- (d) if Supplier becomes aware or suspects that any person who does not have the appropriate level of security clearance has had, may have had, or could gain access to, any Customer Data or Customer's Network and Facilities,

(each a **Notifiable Security Incident**).

4.3 If there is a threatened or actual Notifiable Security Incident, then Supplier will promptly, and at no additional cost to Customer:

- (a) reasonably cooperate with Customer to investigate the Notifiable Security Incident, including with any new Security Audit undertaken by Customer in response to the Notifiable Security Incident;
- (b) comply with any reasonable direction given by Customer to mitigate, remove, or remediate the security risk, threat or vulnerability in relation to any Customer

- Data, network, systems or Customer Personnel, at no additional cost to Customer and to restore any affected equipment, systems and/or software (as applicable); and
- (c) provide written security reports, as requested by Customer, containing details of the Notifiable Security Incident, progress on any investigation and, where appropriate, remediation plans,

4.4 Without limiting Customer's rights under this Schedule or the Master Services Agreement and notwithstanding any other provision of this Schedule, if clause 4.3 applies, Customer may (acting reasonably), by notice in writing to Supplier, require Supplier to suspend, delay, interrupt or stop the performance, completion or delivery of all or any Services until such time as Supplier remedies the matters giving rise to the Notifiable Security Incident.

4.5 If a notice is given under clause 4.4, where Customer caused or contributed to the Notifiable Security Incident, Customer will continue to pay Service Fees and other charges in respect of the relevant Services the subject of such notice for a period of up to 20 Business Days.

5. Vulnerability Management

5.1 Supplier will, for systems and other information resources holding or handling Personal Information:

- (a) scan these systems and other information resources (as relevant) with applicable industry-standard security vulnerability scanning software;
- (b) perform security reviews in accordance with Best Industry Practice; and
- (c) conduct generalised penetration testing and provide a summary to Customer on request; and

5.2 Penetration testing conducted under clause 5.1 will be performed annually and immediately after any significant infrastructure or application upgrade or modification.

5.3 Supplier will actively monitor industry resources for timely notification of all applicable security alerts pertaining to Supplier's systems and other information resources.

5.4 Supplier will:

- (a) ensure that no Malware is introduced by Supplier or Supplier Personnel into any environment, equipment, software or system of Customer; and
- (b) ensure that all software is tested properly to identify and remove or disable any Malware.

5.5 Supplier will:

- (a) have a formal process to manage anti-virus and Malware;

- (b) have up-to-date endpoint protection including data loss prevention and storage/email encryption applied; and
- (c) perform regular patch management and timely patch deployment.

5.6 Supplier will:

- (a) prepare and maintain a system monitoring plan, detailing the recommended security configuration for alerts and logging for the software, and the recommended approach to security monitoring of the software by the Customer security operations centre;
- (b) enable logging and monitoring of all sessions on systems handling Customer Data, including logging and monitoring of the end user or application origination IP address, destination IP address, ports/service protocols used and duration of access. Session logs will be retained for a minimum of 120 Business Days from session creation; and
- (c) ensure that monitoring tools are used to validate that the hardware, firmware and software used to log sessions are continuously operational.

5.7 Supplier will, in its delivery of the Services:

- (a) prohibit and prevent any person who does not have the appropriate level of security clearance or authorisation from Customer for gaining access to any Customer Data or Customer Networks and Facilities;
- (b) immediately notify Customer, and comply with all reasonable directions of Customer, if Supplier becomes aware or suspects that any person who does not have the appropriate level of security clearance has had, or may have had, access to any Customer Data or Customer Networks and Facilities;
- (c) not access (physically or remotely), connect any equipment to, or install any software on, Customer's Network and Facilities unless expressly permitted by Customer and, if required by Customer, under its (or its nominees') supervision; and
- (d) comply with any of Customer's applicable policies when working at Customer's premises, or using Customer's equipment or Customer Data, networks or systems.

6. Security audit

- 6.1 Supplier will, in response to a Notifiable Security Incident or otherwise once in each calendar

year, undertake a Security Audit in accordance with this clause 6.

- 6.2 A Security Audit will only extend to Supplier Personnel, systems or premises in circumstances where it is reasonably necessary having regard to the purpose for which the Security Audit is being undertaken.
- 6.3 If requested, Supplier will provide a report in respect of the most recent Security Audit, including the date(s) on which the audit was conducted and a summary of the key outcomes.

7. Customer Data management

- 7.1 Supplier will ensure that Supplier Personnel take all reasonable steps, including appropriate technical and operational measures, to protect Customer Data and any information technology system owned or used by Customer (including Customer's Networks and Facilities, equipment and other assets) from unauthorised use, access or interference.

8. Privacy

- 8.1 Supplier will:
- (a) ensure that, any Personal Information is collected, used, stored, disclosed, processed or otherwise handled by Supplier and Supplier Personnel in accordance with the *Privacy Act 1988* (C'th), and any other applicable Law;
 - (b) ensure that Supplier and Supplier Personnel provide collection statements in accordance with Australian

Privacy Principle 5 and any other applicable Law;

- (c) in the event of any actual or suspected data breach, (including misuse of, interference with, loss of, unauthorised access to, unauthorised modification of or unauthorised disclosure of Personal Information) or any other actual or suspected interference with privacy related to the Services:
 - (1) immediately notify Customer, and keep Customer updated as details are identified;
 - (2) cooperate with Customer in respect of the matter; and
 - (3) promptly take any necessary steps to contain and rectify the matter and its consequences;
- (d) in the event of any complaint or request for access relating to Customer Data:
 - (1) immediately notify Customer in writing, and promptly provide Customer with details;
 - (2) cooperate with Customer in respect of the matter; and
 - (3) promptly take any necessary steps to address the complaint or the request.

9. Background screening of Supplier Personnel

9.1 Supplier will ensure that all Supplier Personnel used to perform the Services are fit and proper to perform their proposed role.

9.2 In determining whether a person is fit and proper to perform his or her proposed role, Supplier will ensure that for each of the Supplier Personnel:

(a) they are fit and proper having regard to the nature, location, and inherent requirements of that role;

(b) Supplier will conduct at least the following background checks:

(1) obtain proof of identity;

(2) where necessary, obtain proof of a right to work;

(3) where relevant to the role ensure that all:

(A) relevant licences and certifications have been obtained;

(B) relevant professional memberships are current; and

(C) necessary qualifications have been

obtained and are current;

(c) undertake any other checks that are reasonable in the circumstances to ensure that the person is fit and proper to perform their proposed role;

(d) in respect of Privileged Personnel:

(1) a nationally coordinated criminal history check; and

(2) if they have been an Australian resident for less than 12 months, an international police check from each country in which that Privileged Personnel has resided in the prior 12 months.

9.3 Supplier will ensure that in carrying out any aspect of the Services, any Supplier Personnel deemed to be fit and proper will not present a risk to:

(a) the health and safety of any person; or

(b) the property of Customer or any person.

9.4 If Supplier becomes aware at any time that any of Supplier Personnel may not be fit and proper, Supplier will not permit relevant Supplier Personnel to perform or to continue to perform any aspect of the Services.

9.5 If any of the additional security checks reveal that the relevant Supplier Personnel is not able to or

should not perform the specified role, Supplier will not allow the relevant Supplier Personnel to perform that role.

10. Definitions

10.1 Unless the context otherwise requires, all terms used in this Schedule that are defined in the Master Services Agreement bear the meaning ascribed in the Master Services Agreement.

10.2 In this Schedule, unless the context otherwise requires:

(a) **Best Industry Practice** means a standard of service, in terms of security standard and procedures which, when considered collectively, is equal to or better than that being provided at the relevant time by any other supplier of like or similar services anywhere in Australia, or if there are no such suppliers in Australia, in any location outside of Australia in which Supplier operates;

(b) **Customer Networks and Facilities** means telecommunications networks and facilities and systems owned, operated or used by Customer;

(c) **Malware** includes:

(1) any back door, time bomb, drop dead device, or any other code designed to

disable or reduce the functionality of software;

(2) any virus, Trojan horse, worm, malicious code or other software routine designed to permit unauthorised access to, disable, damage, or reduce the functionality of, the software;

(3) any means which enables or potentially enables covert remote access to the software; and

(4) any functionality or feature that has not been disclosed to, and agreed prior to the date of supply with, the Customer, including any additional or undisclosed functionality or feature that might create a security vulnerability;

(d) **Notifiable Security Incident** has the meaning given in clause 4.2

(e) **Privileged Personnel** means Supplier Personnel that have access to any information technology system (including hardware and software) owned or used by the Customer, including the Customer's Networks and Facilities equipment, and

- other information technology assets,
- (f) **Security Audit** means an investigation, assessment, review or audit conducted pursuant to clause 6, in relation to:
- (1) Supplier's compliance with this Schedule;
- (2) any threatened or actual Notifiable Security Incident; or
- (3) any other matter concerning Supplier's activities as they relate to this Schedule, as determined by Supplier.
- (g) **Supplier Security Practices** has the meaning given in clause 1 of this Schedule.

Version history

This is version 1.0 of this Schedule.

Version	Approved	Effective	Notes
1.0	29/05/2025	30/05/2025	First version published