Uniting

Annexure A of Terms and Conditions of Purchase Order – Special Conditions

1. DEFINITIONS.

In this Annexure A, unless the context requires otherwise (or unless defined below), words defined in the *PO Terms and Conditions* have the same meaning, and the following words have the following meanings:

'***Confidential Information***' means, in relation to a *Disclosing Party*:

(a) the terms of the *Agreement* and their subject matter, including *Information* submitted or disclosed by or on behalf of that party during negotiations, discussions and meetings relating to the *Agreement*;

(b) all *Information* regarding the current or future business interests, methodology or affairs of the *Disclosing Party*;

(c) all *Information* which the *Receiving Party* knows, or ought reasonably to be expected to know, is confidential to the *Disclosing Party*;

(d) *Information* that at the time of disclosure by the *Disclosing Party* is reasonably identified to the *Receiving Party* as being confidential; and

(e) all other *Information* belonging or relating to the *Disclosing Party*, other than *Information* that:

(i) is disclosed to the *Receiving Party* by a *Third Party* (not being the *Disclosing Party* or a related entity, employee or officer of the *Disclosing Party*) entitled to do so, whether before or after the date of the *Agreement*;

(ii) was already lawfully in the *Receiving Party*'s possession when it was given to the *Receiving Party* and was not otherwise acquired from the *Disclosing Party* directly or indirectly; or

(iii) is generally available to the public at the date of the *Agreement* or subsequently becomes so available, in each case other than by reason of a breach of the *Agreement* or any breach of confidence.

'***Data Breach***' has the meaning given in clause 4.2.

'***Defect***' includes any:

(a) material fault, failure, degradation, deficiency, error or non-conformance of the *Services* or any *Deliverables* with the *Specifications*, *Service Levels*, or provisions of the *Agreement*;

(b) functionality or performance of any *Services* or *Deliverables* materially below or not in accordance with, the *Specifications*, *Service Levels*, or provisions of the *Agreement*; and

(c) defect or other problem with any of the *Services* or *Deliverables* giving rise to a right or remedy of *Uniting* under the *Competition and Consumer Act 2010* (Cth) (including the Australian Consumer Law) or any similar law of any jurisdiction.

'***Disaster***' means an incident (including a *Force Majeure Event*) that significantly disrupts, or is likely to significantly disrupt:

(a) *Uniting's* ability to receive; or

(b) the *Supplier's* ability to supply,

any of the *Deliverable*s and/or *Services* (including interruption, destruction or other loss of operational capacity), which incident cannot be managed by the *Supplier* within the context of normal operating procedures.

'***Disclosing Party***' means the party to whom *Confidential Information* belongs or relates.

'***Eligible Data Breach***' has the meaning given in the *Privacy Act*.

'***Force Majeure Event***' means any act, event or cause (other than lack of funds) which is beyond the reasonable control of the party concerned including any:

(a) act of God, peril of the sea, accident of navigation, war, sabotage, riot, insurrection, civil commotion, national emergency (whether in fact or law), martial law, fire, lightning, flood, cyclone, earthquake, landslide, storm or other adverse weather conditions, explosion, power shortage, strike or other labour difficulty (whether or not involving employees of the party concerned), epidemic, pandemic, quarantine, radiation, shortage, strike or radio-active contamination; and

(b) action or inaction of any government agency or other competent authority (including any court of competent jurisdiction), including lockdown, expropriation, restraint, prohibition, intervention, requisition, requirement, direction or embargo by legislation, regulation, decree or other legally enforceable order.

'***Information***' means any information, whether oral, graphic, electronic, written or in any other form, including:

(a) forms, memoranda, letters, specifications, processes, procedures, statements, formulae, technology, inventions, trade secrets, research and development information, know how, designs, plans, photographs, microfiche, business records, notes, accounting procedures or financial information, sales and marketing information, names and details of customers, suppliers and agents, employee details, reports, drawings and data; and

(b) copies and extracts made of or from that information and data, whether translated from the original form, recompiled, partially copied, modified, updated or otherwise altered.

'***Personal Information***' has the meaning given in the *Privacy Act*.

'***PO Terms and Conditions***' means *Uniting's* 'Terms and Conditions of Purchase Order' of which this Annexure A forms part.

'***Privacy Act***' means the *Privacy Act 1988* (Cth).

'***Privacy Laws***' means all applicable privacy laws, including the *Spam Act 2003* (Cth), the *Privacy Act*, the *Privacy (Private Sector) Regulations 2001*, and State or Territory privacy laws as they exist and are amended from time to time.

'***Receiving Party***' means, in relation to *Confidential Information* belonging or relating to a *Disclosing Party*, the party to whom that *Confidential Information* is disclosed or who possesses or otherwise acquires that *Confidential Information*.

'***Recipient***' has the meaning given in clause 5.

'***Relevant Personal Information***' means *Personal Information*:

(a) forming part of the *Uniting Inputs*;

(b) that is collected or otherwise acquired or compiled by the *Supplier* in connection with the *Services* and/or *Deliverables* or the *Agreement*; or

(c) that belongs to, or is held or provided by, any *Uniting Group Member*.

'***Service Levels***' means the service levels (if any) in respect of the *Services* and/or *Deliverable*s set out in any *Order* or otherwise agreed in writing between *Uniting* and the *Supplier*.

'***Services***' has the meaning given in the *PO Terms and Conditions* and includes for the avoidance of doubt) where applicable, the licensing of any *Software* to *Uniting*, or the provision to *Uniting* of any other right to use any *Software*.

'***Software***' means all operating system software, software applications, scripts, firmware and programs supplied under the *Agreement* as part of the *Services* or any *Deliverable* (including any "software as a service", under licence or otherwise).

'***Specifications***' means the specifications and other requirements relating to a *Service* or *Deliverable* set out in any *Order* or otherwise agreed in writing between *Uniting* and the *Supplier*.

'***Third Party***' means a person who is not a party to the *Agreement*.

'***Uniting Data***' means *Information* or data:

(a) provided to, or obtained or generated by the *Supplier*; or

(b) stored in, or accessed through, systems or products which the *Supplier* manages, supports, accesses or processes,

which relates to any of the following:

(c) any *Uniting Group Member*;

(d) any supplier of a *Uniting Group Member* (excluding the *Supplier*); or

(e) any client, customer or *Personnel* of a *Uniting Group Member* (excluding the *Supplier* or any of its *Personnel*).

'***Uniting Group***' means *Uniting* and its associated entities and related entities (excluding the *Supplier* and its *Personnel*).

'***Uniting Group Member***' means any member of the *Uniting Group*.

'***Uniting Inputs***' means all *Information* (whether or not *Confidential Information*), *Uniting Data*, documentation, assistance, facilities, instructions and/or any other items that are agreed in writing between *Uniting* and the *Supplier* as being inputs or the responsibility of *Uniting*, or that is otherwise reasonably required to be provided by *Uniting* to the *Supplier* (or that *Uniting* needs to give the *Supplier* access to) for the purpose of the *Supplier* providing the *Services* and/or *Deliverable*s under the *Agreement*.

'***Update***' means any change (for example, updates, upgrades, releases, versions, replacements, modifications, enhancements, including in respect of new features, functionality, technology or architecture improvements or to correct *Defect*s, whether or not they are major or minor) to or of any *Software*, and '***Updated***' has a corresponding meaning.

2. APPLICATION.

(a) This Annexure A sets out the *Special Conditions* for the purpose of the *PO Terms and Conditions*.

(b) Unless stated otherwise, in this Annexure A, references to clauses are references to clauses of this Annexure A.

(c) Except as provided otherwise in clause 2(d), all:

(i) representations and warranties given by the Supplier; and

(ii) obligations and liabilities assumed by the Supplier,

under this Annexure A are in addition to (and do not substitute or limit) any representations, warranties, guarantees, obligations or liabilities which the *Supplier* gives or assumes (or is required to give or assume) at law or under any other applicable provision of the *Agreement* (including, without limitation, under the *PO Terms and Conditions*).

(d) Without limiting clause 2(d) of the *PO Terms and Conditions*, clauses 3 and 5 of this Annexure A apply and take effect to the exclusion of clauses 11(a) and 11(b) of the *PO Terms and Conditions*.

3. PRIVACY.

The Supplier must:

(a) comply with all *Privacy Laws* and any other applicable laws (as well as any applicable policies provided to it by *Uniting*) in connection with its handling of any *Relevant Personal Information*, and the performance of its obligations under the *Agreement*;

(b) not do anything which impairs the accuracy, currency, or completeness of the *Relevant Personal Information*;

(c) ensure any *Personnel* of the Supplier (including employees, contractors, subcontractors and advisers who are required to access or handle *Personal Information*) are made aware of the obligations set out in this clause 3, and if requested by *Uniting*, sign written undertakings to comply with this clause 3 in the form required by *Uniting*;

(d) follow the reasonable directions of *Uniting* from time to time in relation to the use of any *Relevant Personal Information*;

(e) take all reasonable steps to assist *Uniting* to comply with, and not be in breach of, its obligations under *Privacy Laws* that may apply to *Uniting*;

(f) take reasonable technical, operational, and physical steps necessary for all

Relevant Personal Information held or controlled by it or any of its *Personnel* in connection with the *Agreement* to be protected against misuse, loss and unauthorised access, interference, modification or disclosure;

(g) use *Relevant Personal Information* only to fulfil its obligations under the *Agreement*;

(h) not disclose any *Relevant Personal Information* except in connection with performing the *Supplier's* obligations under the *Agreement* or as required by law;

(i) not, and must ensure that its *Personnel* do not, unless required for the purposes of the *Agreement* (or otherwise agreed by the parties in writing), transfer or disclose outside Australia, or allow any other person to transfer or disclose outside Australia, any *Confidential Information* or any *Relevant Personal Information*;

(j) notify *Uniting* immediately in writing if the *Supplier* becomes aware of any:
   (i) request regarding access to, or correction of, any *Relevant Personal Information*;
   (ii) any complaint about the handling of any *Relevant Personal Information*; or
   (iii) disclosure of any *Relevant Personal Information* required by law; and

(k) have in place adequate policies, processes and systems for monitoring and ensuring compliance with its obligations under this clause 3.

4. DATA SECURITY.

4.1 Security

(a) In providing the *Services* and *Deliverable*s, the *Supplier* must implement and maintain, to *Uniting's* reasonable satisfaction:
   (i) established technical vulnerability management and patching capabilities and procedures in relation to all information technology systems and platforms used to provide any *Services* or *Deliverable*s;
   (ii) established controls around the implementation and management of cryptographic keys in relation to *Uniting Data*; and
   (iii) procedures to ensure compliance with:
      (A) *Uniting's* data security policies and procedures, as notified by *Uniting* to the *Supplier* from time to time;
      (B) all applicable laws and industry standards; and
      (C) up-to-date, industry best practice standards, processes and procedures for information security frameworks in Australia.

(b) Without limiting clause 4.1(a), the *Supplier* must:
   (i) establish and maintain safeguards against the destruction, loss or alteration of *Uniting Data* in the possession or control of the *Supplier* that comply with all laws, applicable industry standards, and any specific requirements of *Uniting* set out in the *Specifications*;
   (ii) ensure that *Uniting Data* is stored separately from that of any other customer or client of the *Supplier*, specifically ensuring logical separation for data stored electronically, and separate physical storage for data which is not stored electronically; and
   (iii) implement and maintain appropriately configured firewalls, intrusion detection/prevention technologies and other network security measures to protect *Uniting Data*, including ensuring that a multi-factor authentication security procedure is required for log-ins and access to *Uniting Data* (requiring at least 2 different factors of authentication to enable any person to log in and/or access any *Uniting Data*).

(c) Where any *Uniting Data* is hosted in a cloud environment as part of the *Services*, the *Supplier* must ensure that:
   (i) *Uniting Data* is logically isolated from other clients or customers of the *Supplier*; and
   (ii) the *Supplier's* cloud service is physically or logically isolated or encapsulated from other cloud tenants.

(d) The *Supplier* must ensure that all information technology systems and platforms used in the provision of *Services* and *Deliverable*s have deployed industry standard virus protection software and other measures to protect against the introduction of computer software routines intended or designed to affect the confidentiality, integrity or availability of *Uniting Data*.

(e) Without limiting *Uniting's* rights under clause 4.7, the *Supplier* must, promptly after being requested to do so by *Uniting*, provide evidence to *Uniting* of the *Supplier's* compliance with this clause 4.1.

4.2 Notification of *Data Breach*

Without limiting clause 3, if either party becomes aware of, or suspects that there has been:

(a) any loss of, or unauthorised access to, use of or disclosure of, *Relevant Personal Information*; or

(b) a breach of security relating to the *Services* (including relating to any *Relevant Personal Information*), including where any loss or unauthorised access to, use of or disclosure of *Relevant Personal Information* is likely to occur,

(each a '***Data Breach***'), then that party must immediately notify the other party in writing and provide a description of all relevant details of the *Data Breach* including its nature and scope, potential risks and impacts, and any remedial measures taken or proposed.

4.3 Obligations on occurrence of *Data Breach*

Where a *Data Breach* occurs, the *Supplier* must:

(a) immediately take all necessary steps, and bear any costs, required to prevent further unauthorised access or disclosure of the affected data, including but not limited to implementing appropriate technical and organisational measures;

(b) co-operate and comply with all reasonable written directions of *Uniting* in relation to the *Data Breach*;

(c) conduct a thorough investigation of the *Data Breach* within 20 days of becoming aware of the *Data Breach* in order to determine whether it is an *Eligible Data Breach* and provide a full, unredacted copy of the report of the investigation to *Uniting* on completion;

(d) promptly take all reasonable steps to rectify or remedy the *Data Breach*, including steps to mitigate any harm to individuals resulting from the *Data Breach*; and

(e) only notify the Office of the Australian Information Commissioner ('***OAIC***') or affected individuals of the *Data Breach* in accordance with clause 4.4.

4.4 *Eligible Data Breach*

If either party has reasonable grounds to believe that there has been an *Eligible Data Breach*, the parties must co-operate with each other in relation to the *Eligible Data Breach*, including:

(a) providing all necessary information, documents and assistance reasonably requested by the other party in order to investigate the *Eligible Data Breach* and to prepare the required statements and notifications to individuals and the OAIC under Part IIIC of the *Privacy Act* (if required); and

(b) if the *Supplier* reasonably determines that it is required to issue a statement (or make a notification) under Part IIIC of the *Privacy Act* in relation to that *Eligible Data Breach*, the *Supplier* must provide a draft copy of the proposed statement or notification to *Uniting* before issuing that statement or notification to individuals or the OAIC under Part IIIC of the *Privacy Act*, give *Uniting* a reasonable opportunity to request amendments to that draft statement or notification and take any reasonable requests for amendments into account before finalising and issuing the relevant statement or notification.

4.5 Indemnity

Except to the extent caused or contributed to by the negligent act or omission, wilful misconduct, or breach of the *Agreement* by any *Uniting Group Member*, the *Supplier* must indemnify and hold harmless each *Uniting Group Member* from and against any and all:

(a) losses, claims, damages, liabilities, costs, and expenses; and

(b) all interest, penalties and legal costs (calculated on a full indemnity basis),

arising out of or in connection with:

(c) any *Data Breach* caused by the *Supplier* or its *Personnel*; or

(d) any breach or threatened breach of this clause 4 by the *Supplier*.

4.6 Termination

If a *Data Breach* is caused by the *Supplier's* negligence or wilful misconduct, then without limiting any other rights *Uniting* may have under the *Agreement* (including, without limitation, under clause 14 of the *PO Terms and Conditions*) or at law or in equity, *Uniting* may immediately terminate the *Agreement* by written notice to the *Supplier*, without *Uniting* incurring any penalty or liability to the *Supplier* in respect of such termination.

4.7 Compliance audits

(a) *Uniting* may, subject to this clause 4.7, audit and inspect the facilities, processes, procedures, systems and documentation of the *Supplier* to determine whether the *Supplier* is complying with this clause 4.

(b) The audit may include, but is not limited to, an examination of the *Supplier's* information security policies, physical security measures, logical access controls, data protection measures, incident response procedures, and any other controls relevant to the *Services*, the *Deliverable*s and the protection of *Uniting Data*.

(c) *Uniting* will provide the *Supplier* with reasonable notice before initiating an audit, except in cases where an immediate audit is necessary due to a suspected security breach (including a suspected *Data Breach* or *Eligible Data Breach*), or other similar circumstances which require immediate or urgent action. The parties will coordinate the timing, scope, and duration of each audit in good faith and acting reasonably.

(d) *Uniting* may designate representatives (including *Third Party* auditors) to conduct an audit. The *Supplier* must reasonably cooperate with *Uniting's* designated representatives during the audit, and provide them with access to all necessary facilities, personnel, systems and documentation.

(e) *Uniting* must comply with clause 5 in relation to any *Confidential Information* of the *Supplier* which is disclosed or obtained by *Uniting* or its representatives as part of an audit (with those representatives being *Uniting's Recipient*s for the purposes of that clause).

(f) If an audit reveals that the *Supplier* has not complied with, or is not complying with, any of its obligations under this clause 4, then without limiting *Uniting's* other rights under the *Agreement* or at law in relation to the non-compliance, the *Supplier* must promptly address and remedy

such non-compliance to *Uniting's* reasonable satisfaction. *Uniting* and the *Supplier* will collaborate in good faith to develop a mutually agreeable plan to address and rectify any identified security vulnerabilities.

(g) Subject to this clause 4.7(g), unless otherwise agreed in writing by the parties, *Uniting* will bear the costs associated with each audit, including the fees of any *Third Party* auditors engaged by *Uniting* (if applicable). Notwithstanding the foregoing, if any material breach of this clause 4 is identified as part of an audit, the *Supplier* must promptly pay *Uniting* any *Third Party* auditor's fees payable in connection with the audit.

(h) *Uniting* may conduct no more than one audit in any 6 month period under this clause 4.7 (excluding any immediate audit referred to in clause 4.7(c)). The parties may, if proposed by *Uniting* at any time, agree for audits to be conducted more frequently, having regard to the nature of particular *Services* or *Deliverable*s, and to any changes in the risk landscape. The *Supplier* will act reasonably and in good faith in considering whether to agree to any such proposal.

(i) This clause 4.7 survives termination or expiry of the *Agreement*.

5. CONFIDENTIALITY.

5.1 Obligations of confidentiality

Subject to the other provisions of this clause 5, in relation to *Confidential Information* of or relating to a *Disclosing Party*, each *Receiving Party* must:

(a) keep that *Confidential Information* secret and confidential and not directly or indirectly disclose, divulge or communicate any of that *Confidential Information* to, or otherwise place any of that *Confidential Information* at the disposal of, any other person without the prior written approval of the *Disclosing Party*;

(b) take all reasonable steps to secure and keep secure all of that *Confidential Information* coming into its possession or control;

(c) not use, modify, reverse engineer or make copies, notes or records of that *Confidential Information* for any purpose other than in connection with the performance by the *Receiving Party* of its obligations under the *Agreement*; and

(d) take all reasonable steps to ensure that any person to whom the *Receiving Party* is permitted to disclose that *Confidential Information* under this clause 5 complies at all times with the terms of this clause 5 as if that person were the *Receiving Party*.

5.2 Disclosure required by law

The obligations of confidentiality under this clause 5 do not apply to any disclosure by a *Receiving Party* of *Confidential Information* of or relating to a *Disclosing Party* that is strictly and necessarily required to comply with any court order, laws or applicable rules of any financial market, provided that, to the extent practicable and as soon as reasonably possible, the *Receiving Party*:

(a) notifies the *Disclosing Party* of the proposed disclosure;

(b) consults with the *Disclosing Party* as to its content; and

(c) uses reasonable endeavours to comply with any reasonable request by the *Disclosing Party* concerning the proposed disclosure.

5.3 Authorised disclosure

A *Receiving Party* may disclose *Confidential Information* of or relating to a *Disclosing Party* to a related entity or *Personnel* of the *Receiving Party* (each a *Recipient*) only if the disclosure is made to the *Recipient* strictly on a "need to know basis" and, before the disclosure:

(a) the *Receiving Party* notifies the *Recipient* of the confidential nature of that *Confidential Information* to be disclosed; and

(b) the *Recipient* undertakes to the *Receiving Party* (for the benefit of the *Disclosing Party*) to be bound by the obligations in this clause 5 as if the *Recipient* were the *Receiving Party* in relation to that *Confidential Information* to be disclosed to the *Recipient*.

5.4 Return or destruction of *Confidential Information*

(a) Immediately on the written request of a *Disclosing Party* or on the termination of the *Agreement* for any reason, the *Receiving Party* must:

(i) cease using and disclosing all *Confidential Information* of or relating to the *Disclosing Party* (or any related entity of the *Disclosing Party*);

(ii) deliver to the *Disclosing Party* (or as directed by the *Disclosing Party*) all documents and other materials in the possession or control of the *Receiving Party* or any of its *Recipient*s containing, recording or constituting that *Confidential Information* or, to the extent directed by the *Disclosing Party*, destroy, and certify to the *Disclosing Party* that it has destroyed, those documents and materials; and

(iii) for any such *Confidential Information* stored electronically, permanently delete, and certify to the *Disclosing Party* that it has permanently deleted, that *Confidential Information* from all electronic media on which it is stored, so that it cannot be restored.

(b) Clause 5.4(a) does not apply to:

(i) information stored as electronic back-up data in the usual operations of the *Receiving Party* that cannot be readily accessed;

(ii) the directors' papers or minutes of the board or other governing body of the *Receiving Party*, to the extent that such papers and minutes contain the level of detail consistent with the normal practices of the *Receiving Party*; and

(iii) documents that are created or retained by any professional adviser to the *Receiving Party* which contain *Confidential Information* of or relating to a *Disclosing Party*, to the extent those documents are required to be held by law or to comply with any professional standards, insurance policies or reasonable audit requirements of that adviser,

provided that those items are not subsequently used or retained other than for their primary purpose, and in any event, the *Receiving Party* must ensure that all *Information* used or retained under this clause 5.4(b) is kept confidential in accordance with the terms of the *Agreement*.

5.5 Liability for breach by *Recipient*

Each *Receiving Party* is liable for any breach of this clause 5 by a *Recipient* of that *Receiving Party* as if the *Recipient* were a *Receiving Party* in relation to the *Confidential Information* disclosed to the *Recipient*.

6. SUPPLIER'S WARRANTIES.

6.1 Warranties

The *Supplier* represents and warrants to *Uniting* as at the date of the *Agreement* and at all times after the date of the *Agreement* that:

(a) any *Deliverable*s consisting of goods are legally and beneficially owned by the *Supplier* and are free and clear of any liens, charges, security interests, encumbrances or other *Third Party* interests or rights;

(b) it is entitled to provide the *Services* and *Deliverable*s to *Uniting*;

(c) the *Software* and all *Updates* do not contain any virus or other destructing or disabling code;

(d) its *Personnel* will at all times be suitably qualified and experienced, and the *Supplier* and its *Personnel* will exercise due care and skill in performing the *Services*;

(e) all *Services* and *Deliverable*s will comply with the applicable requirements of the *Agreement*, including any applicable *Specifications* for *Services* and *Deliverable*s; and

(f) it is not aware of any fact which would prevent any insurance policy taken out under the *Agreement* covering a claim made in the context of the supply of any *Services* or *Deliverable*s (including any non-compliance with conditions precedent to the operation of any such insurance policy).

6.2 Reliance

The *Supplier* acknowledges that *Uniting*, in entering the *Agreement*, has relied on the *Supplier's* warranties and representations set out in the *Agreement*.

6.3 Notification

If the *Supplier* becomes aware of any breach of the warranties in clause 6.1, the *Supplier* must immediately notify *Uniting* in writing.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY.

The *Supplier* must:

(a) maintain business continuity and disaster recovery procedures to protect any work it carries out as part of the provision of *Services* and *Deliverable*s (including any systems or networks used to provide the *Services* and any *Deliverable*s) and its ongoing ability to perform its obligations in the event of a *Disaster* ('***BCDR Procedures***');

(b) regularly, and at least once per calendar year, test and update the *BCDR Procedures*;

(c) on request by *Uniting*, provide documentation of the *BCDR Procedures* and results of any testing of the *BCDR Procedures*;

(d) if a *Disaster* occurs, promptly implement the *BCDR Procedures* and keep *Uniting* updated about its business continuity and disaster recovery activities, as well as any actual or anticipated impact of the *Disaster* on the performance of its obligations; and

(e) if a failure of, or disruption to the *Services* occurs due to a *Disaster*, the *Supplier* must ensure that normal *Services* are restored and available in the shortest practicable time (without limiting clause 8).

8. SERVICE LEVELS AND MAINTENANCE.

8.1 *Service Levels*

(a) The *Supplier* must meet or exceed the *Service Levels* and report to *Uniting* on performance against the *Service Levels* in accordance with any applicable *Order* or as otherwise agreed in writing between *Uniting* and the *Supplier*. [If the *Supplier* fails to meet a *Service* Level, it must pay *Uniting* any applicable amounts calculated in accordance with [*]].

(b) The *Supplier* must provide the *Services* such that the fault response, workaround and fix times will be short enough to provide an uptime of a minimum of [[*]% over any 12 month period], excluding any planned downtime (subject to clause 8.2(b)).

8.2 Planned downtime and maintenance

(a) The *Supplier* must give *Uniting* at least [*] hours' notice in writing of any planned downtime in respect of the provision of (and *Uniting's* use of) the *Services* (including any *Software*). Any such planned downtime must not exceed [*] hours per calendar month in respect of any *Services*.

(b) Provided that the *Supplier* complies with the requirements set out in clause 8.2(a), then the availability uptime in clause 8.1(b) will exclude any planned downtime.

(c) The *Supplier* may carry out regular service and maintenance on any *Software* provided as part of the *Services* between the hours of [5pm and 7pm on Saturdays (Australian Eastern Time)]. For the avoidance of doubt, this regular service and maintenance forms part of any planned downtime under clause 8.2(a).

8.3 *Updates* and *Defects*

(a) The *Supplier* must maintain the *Software* with the latest *Updates* and

ensure that the *Software* (as so *Update*d) is available for use by *Uniting* as part of the *Services*.

(b) If *Uniting* notifies the *Supplier*, or the *Supplier* becomes aware, of any *Defect* in any *Services* (including *Software*) or *Deliverable*s, then the *Supplier* must rectify any such *Defect* as soon as practical and, in any event, in compliance with any applicable *Service Levels*.