

pam Customer Licence Agreement

Version 3 - Commercial in confidence

Last updated 8th March 2023

1. Definitions

Customer Organisation	The pam organisation account to which Customer's employees and representative Registered Users are associated.
Lead User	The Customer nominated name and email address that Alliantist has on file as the person it should engage with over Customer's use of the Platform. Usually also the same person who has Customer system administration rights and participates in reviews with Alliantist from time to time and as such is the authorised person who will be notified by Alliantist in the event of a data breach. Customer can split these roles and nominate others.
Customer Users	Registered Users who are employees of the Customer or generally operating in a capacity as representatives for the Customer and have accepted the User Registration Terms. Each Customer User will have their own unique login email address and password.
Partner Organisation	<p>An organisation added to pam by the Customer Organisation which can then be issued restricted user rights licences 'Partner Users' e.g. for where the Customer wishes to collaborate with the Partner Organisation for the Purpose (e.g. working with local partners to plan joint actions).</p> <p>Partner Organisations have their own obligations. The first Partner User will accept the online click through Partner Registration Agreement on behalf of its organisation. If the Partner Organisation is already a Customer Organisation then no further terms apply and the organisations simply collaborate together on the Platform under their normal Agreement terms (and they may have their own Information Sharing Agreement in place).</p>
Partner Users	Registered Users who are employees or representatives of a Partner Organisation and require access to pam. Partner Users are associated with a Partner Organisation and may only use the platform for the Customer Organisation Purpose. Partner Users accept the User Registration Terms and have limited access to pam. They are able to collaborate fully in Initiatives created by a

	Customer User but are unable to create new work initiatives themselves. Each Partner User will have its own unique login and password.
Partner Registration Agreement	The terms of registration for all Partner Organisations using pam.
Registered User	A Customer User or Partner User registered in pam.
Regular User	The default licence model for Registered Users which enables the User to access and engage in work on the Platform in accordance with the Purpose.
Occasional User	A supplementary lower cost licence model for Customers using our enterprise pricing who want larger volumes of Registered Users (but may only need those users to receive a) notification emails from the Platform or b) occasionally access the Platform. Occasional and infrequent typically means a limited log on in a period. It has a reasonableness test against it to ensure that the Occasional User licence is not being misused when a Regular User licence may be more appropriate.
Initiatives	Specific work areas either pre-configured as part of the Platform scope or created by Customer Users in the course of achieving their Purpose. Examples include 4P based OCG disruption plans, tracks for monitoring multi agency safeguarding referrals, Subject areas for lifetime offender management, supplier accounts, etc.
Proposal	The information contained in the proposal order that sets out the scope, fees, number and type of Registered Users, the duration and start date for access to pam by the Customer along with the relevant features, initiative types and tools or related solutions being provisioned as well as any other contextual Platform information.
Customer Organisation Data	All business content entered into pam by Customer Users for the Purpose including Personal Data.
Partner Organisation Data	All business content entered into pam by Partner Users for the Purpose including Personal Data.
Data	Customer Organisation and Partner Organisation Data.
User Registration Terms	The terms of registration including the acceptable use policy set out by Alliantist for all Registered Users of pam.
Personal Data and Sensitive Personal Data	Shall have the meaning as provided in the General Data Protection Regulations (EU) 2016/679 (GDPR).
Data Controller	The Customer Organisation or Partner Organisation that determines the purposes and means of the processing of Personal Data.

Data Processor	Alliantist, which processes Personal Data on behalf of the Data Controller as part of its provision of the Services under the lawful basis of a contractual obligation. Unless explicitly added by the Customer for coaching on the Platform, or for the purpose of bug & issue support, Alliantist and its named sub-processors do not access any Data.
Sub-processors	Suppliers selected by Alliantist to complement its own delivery of the Services as regards Personal Data related work in line with GDPR obligations.
Help Documentation	User guides and online tours for pam in electronic or printable form also made available in the 'help' section of pam and updated from time to time.
pam Policies	An optional extra including policies and controls, or related guidance for the Customer to use as part of its work in the form of written notes documentation, files and other content presented in the pam system content. It is generally provided by Alliantist pre-configured with the Platform to help the Customer 'adopt, adapt and add to' very quickly and offer a head start in developing its work. Alliantist does not provide any warranties to the Customer as to their fitness for the Purpose given the specific goals of the Customer. Some clearly specified content added into the notes areas is reproduced with permission from the respective copyright holders and at the time of service commencement reflects that body's guidance. Alliantist is under no obligation to keep any of the policies, controls or guidance up to date after the service commencement date.
Virtual Coach	An optional extra virtual coaching service delivered through the Platform that includes guides, checklists, videos and presentations to help organisations understand more about a standard or approach and how they can implement it for their organisation. Alliantist does not provide any warranties to the Customer as to their fitness for the Purpose given the specific goals of the Customer.
Special Terms	Only available for organisations that require bespoke Platform development beyond the standard packaged services. These are special terms added to the proposal Order Form or otherwise documented and agreed in written or electronic auditable form and added to the Agreement e.g. by email exchange and take precedent over the standard Agreement terms.
Minimum Fee	The first-year fee for access to the Services or a specific minimum payment for access to the Platform, the Policies, Help Documentation, Virtual Coach and other valuable learning provided within the Services, as outlined in the order form or the Alliantist G-Cloud pricing policy.

Reseller Agreement	A separate agreement with Alliantist for specifically referring and reselling some or all of the Services.
Information Sharing Agreement:	Organisations that are collaborating on sensitive information sharing work may choose to have a separate Information Sharing Agreement between them that sets out any provisions for their information and data sharing on the Platform including data controller, processor, and other activity between them. See clause 3.

2. Licensing and IPR

- 2.1. Subject to the terms of this Agreement, and in consideration for payment of the Fees, Alliantist grants, and Customer accepts, a non-exclusive, non-transferable, revocable, license, to use and to permit the Registered Users to use the Services, without the right to grant sublicenses, during the Term.
- 2.2. Customer shall display and retain Alliantist's and/or its suppliers' copyright, trademarks, proprietary, or confidentiality statement or legends and other notices in pam or on any resources or materials printed or copied from the Platform.
- 2.3. Customer acknowledges that Alliantist retains all right, title and interest in and to the original, and any copies, of pam, pam Policies and the Help Documentation, Virtual Coach, Assured Results Method (and any other component of the Services) and ownership of all patent, copyright, trade secret, trademarks and other intellectual property rights (whether registered or not) pertaining thereto, shall be and remain the sole property of Alliantist (subject to the rights of any third party copyright holder that may be identified).
- 2.4. Without limiting the generality of the foregoing, Customer receives no rights to, and agrees that it will not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) decompile, disassemble, reverse engineer or attempt to reconstruct, identify or discover any source code, underlying ideas, underlying user interface techniques, processes or algorithms of the Services or any portion thereof, or otherwise derive its source code; (ii) modify, port, translate, localise or create derivative works of the Services; (iii) sell, lease, license, sublicense, copy, market, transfer, assign, distribute or otherwise commercially exploit or make available to any third party any aspect or component of the Services; (iv) permit use of the Services by anyone who isn't a Registered User; (v) encumber or suffer to exist any lien or security interest on the Services; or (vi) disclose the results of any performance tests or qualitative analysis on the Services to any

third party without the prior written consent of Alliantist.

- 2.5. Customer shall notify Alliantist immediately if it becomes aware of any unauthorised disclosure or use of the Services by a third party.
- 2.6. Where pam Policies are included in the Services, on condition that Customer is not in breach of any terms of this Agreement (or the Proposal), the Customer can continue to use such pam Policies (not the technology tools inside the Platform) internally even if it chooses not to renew or continue with the Platform when the Services are due for renewal.

3. Customer and Partner Organisation Data

- 3.1. Customer retains all right, title and interest to all Customer Organisation Data. Partner Organisation retains all right, title and interest to all Partner Organisation Data Subject except where:
- 3.1.a. Customer has its own Information Sharing Agreement with any Partner Organisations it adds to the Platform about any Partner Organisation Data shared on the Platform. Alliantist will only act in accordance with the Customer instructions, not the Partner Organisation;
- 3.1.b. The Partner Organisation is also a Customer of Alliantist in which case it would look to understand who owned the initiative in the Platform if there was any dispute and work collaboratively with the Customer and Partner Organisation in line with a relevant Information Sharing Agreement to help resolve any issues.
- 3.2. Data uploaded to the Platform and any processing of it must be in compliance with this Agreement along with all applicable laws and regulations. By uploading Data to the Platform, Customer authorises Alliantist to process the Data pursuant to 3.5 and 3.6 below. Alliantist will notify the Customer if it believes the Customer's processing instruction infringes applicable legislation and/or regulation. The Customer is responsible for ensuring that:
- 3.2.a. the Customer does not create, transmit, display or make otherwise available any Data that violates this Agreement, or in the sole opinion of Alliantist, the rights of Alliantist, other Customers, or Registered Users, persons or organisations or is harmful (including but not limited to viruses, worms, malware and other destructive codes), offensive, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, invasive of another's privacy,

defamatory, hateful or otherwise unlawful; and

3.2.b. the Customer has the necessary rights and lawful justifications to use the Data, including adding it onto the Platform and processing (either by the Customer or Alliantist) thereafter. Customer shall have sole responsibility for the accuracy, quality, and legality of all Data including Personal Data and the means by which Customer acquired said Data including Personal Data.

3.2.c. the Customer acknowledges that they are the Data Controller (or equivalent in their local jurisdiction under non-GDPR aligned privacy and data protection laws) and will comply with their Data Controller obligations in respect of every interaction with the Services.

3.3. Alliantist may without liability or prejudice to its other rights to Customer, disable the Customer's access to any material that breaches the provisions of clause 3.2 (a).

3.4. Alliantist does not (in the normal course of operation) access, monitor or proactively interact with Data held on the Platform. Circumstances in which Alliantist may access such Data includes when Alliantist is required to access the Platform for the provision of coaching to the Customer; or for the purpose of bug & issue support.

3.5. Personal Data Processing

For the purposes of Article 28 of GDPR (and any equivalent domestic law requirement) we set out below the terms of our data processing agreement.

Data Controller	Customer
Data Processor	Alliantist
Subject matter of processing	Alliantist provides pam for the Customer to achieve the goals it has described in the Purpose.
Lawful bases for the Controller	The controller will be operating under one of either: a) consent, b) contract, c) legal obligation, d) vital interests, e) public interest, f) legitimate interests
Lawful basis for the Processor	Contractual obligation in line with this Agreement.

Duration for the processing	Alliantist will process the Data on behalf of the Customer for the term of the Agreement and for such time as is required thereafter if the Customer continues with the Services.
Nature and purpose of the processing	Customer will collect, collaborate, coordinate, organise, share, record, store, amend, edit and delete information including appropriate Personal Data for the purpose of implementing, improving and managing its Platform. Alliantist will also process Personal Data as required to support and maintain the Services for the Customer.
Types of data held	<p>Customer is only required to add personal data of Registered Users such as organisation email address and first name, surname for users to access the Platform. Registered Users can choose to add more details such as an avatar picture and telephone, mobile and work address if they want to facilitate greater trust and collaboration between Registered Users. IP addresses are also held for the purpose of compliance with other legislation, protective monitoring, and delivery of support & maintenance.</p> <p>Depending on the Purpose the Customer may also decide to hold Personal Data and Sensitive Personal Data of individuals within their area of interest.</p>
Information Security and Data Protection safeguards in place	<p>Alliantist has several organisational and Platform related measures for the protection of all valuable information, not just personal data.</p> <p>Organisational measures include:</p> <ol style="list-style-type: none"> 1. UKAS certified ISO 27001: 2013 (Information Security) and ISO 27701:2019 (Privacy) at the organisation level, the software application pam, and the staff involved in the Services meet appropriate confidentiality, integrity and availability thresholds following a risk analysis. 2. Supply chain is certified to at least the same standard or an acceptable equivalent for infrastructure critical services (data centre hosting, code management etc). 3. Any smaller suppliers that work on the platform who don't hold ISO certifications themselves follow Alliantist IMS and are contracted on that basis. 4. All staff (and relevant suppliers) involved are regularly trained on information security and privacy. They agree to comply with the policies and controls, including confidentiality, as part of their recruitment,

	<p>induction, in-life monitoring, at least annually and if appropriate when undertaking change of role.</p> <ol style="list-style-type: none"> 5. Where appropriate data protection impact assessments, policy reviews and internal audits are undertaken regularly alongside management reviews in line with ISO 27001/27701. 6. The software application and related infrastructure is penetration tested annually or on significant change events, all independently CHECK tested. 7. Data in transit between the end user and the service uses TLS. The SSL Certificate in use by the service uses a 2048 bit RSA Key with a SHA256 algorithm. The TLS terminator is configured to prefer more recent versions of protocols and more secure options first and is configured to not revert to an older standard after initial negotiation. The minimum version of the TLS protocol supported is TLS1.2. ISMS.online has been rated A+ by independent checks using the Qualys review process for SSL inspection. 8. For data at rest, the shared filesystem and database filesystem is encrypted to AES-256 using HSM technology using the Amazon KMS service. Passwords are salted and hashed when stored. The database is not shared with other services nor is it publicly accessible – it is firewalled off in our private cloud and is only accessible by our application servers. 9. All backups are encrypted/decrypted at source with AES256 level encryption and are encrypted in transit. 10. All staff that are involved in the service delivery have been vetted, follow strict protocols and all the services they use are (where appropriate) enabled by 2 factor authentication, and other security controls such as password management services to ensure strong and suitable passwords. 11. Alliantist follows Cyber Essentials to the IASME standard. 12. Alliantist has strong permissions and controls management to ensure that only authorised users following strong security protocols can only access the relevant parts of the backend of the platform in the event of a support issue. All access is logged and if appropriate can be forensically analysed in the unlikely event it needs to be. 13. Alliantist holds appropriate insurance cover for Professional Indemnity, Cyber Breach, Public Liability and Employment. <p>Platform measures made available for Registered Users include:</p>
--	--

	<p>14. 2 factor authentication is included for all users - at no additional cost to the core service and implemented from within the User preferences area.</p> <p>Customer administrators can see who has and hasn't implemented it.</p> <p>15. Strong passwords and other forced security measures that can be set at an organisation level e.g. timeouts, forced password change etc.</p> <p>16. Role based permissions and access control measures for different jobs / different Registered User requirements.</p> <p>17. Privacy controls and permissions management at Initiative levels, controlled by the team admin to prevent unauthorised access to Data.</p> <p>18. Administrator reports and measures to help monitor activity without breaching user privacy (and ensure Customer investments in Registered Users are optimised).</p> <p>19. Alliantist personnel or subcontractors acting in a coaching or support capacity inside the pam instance of the Customer are only added by the Customer for the time required and then removed by the Customer.</p> <p>Customer is expected to take advantage of the Platform measures added for its benefit. Alliantist will not be responsible for any security incident or event that may occur because the Customer has failed to implement any or all of the Platform measures listed above. This includes Registered Users being responsible for maintaining the confidentiality and security of their password and login details and using the provided two factor authentication service.</p>
Sub-processors	<p>Sub-processors are used for a range of jobs and managed according to their role and risk around the personal data.</p> <p>Sub-processors in our role as Data Processor</p> <p>AWS is the primary Sub-processors for core service delivery (e.g. hosting) in Alliantist role as Data Processor is UK hosted with no international transfers.</p> <p>Sub Processors In our role as Data Controller</p> <p>AWS, Microsoft, Google, Jira, FreshWorks, Hubspot, Xero, Fresh Financials, Ring Central, Wordpress, CloudGateway (PSN access), CJSM, Qwilr, Quotient.</p> <p>Where Personal Data is transferred outside the UK, it will only be transferred to countries that have been identified as providing adequate protection for UK data or</p>

	<p>to a third party where we have approved transfer mechanisms in place to protect Personal Data such as the European Commission's Standard Contractual Clauses with the UK's International Data Transfer Addendum.</p> <p>By agreeing to these Terms, Customer grants Alliantist a general authorisation in the meaning of Article 28 (2) of GDPR to engage sub processors for the purposes of providing the Services. Alliantist will inform the Customer of material changes in such sub-processors in accordance with the Agreement and in line with Clause 7.1.</p>
Plan for the safe return of data or its destruction at the end of the Agreement	<p>At any point Customer can remove its Data through a range of reports, exports and mechanisms on the Platform. Subject to the scope, style and nature of what it wants and in what format, Alliantist will also assist the Customer with its end of life exit activity including the relevant aspects of personal data portability and transfer if required.</p> <p>On conclusion of the Agreement and payment for the Services, Alliantist operates a Customer exit process in line with ISO 27001 where it ensures the Customer has, as Data Controller, removed what it wants from the Platform and then goes through the safe erasure and deletion of the Customer Data. This takes 30 days to conclude as the back-up information is erased and replaced during that cycle. Where the Customer is collaborating in Initiatives with other organisations on the Platform that remain Customers of Alliantist it acknowledges that some Customer Data may be retained on the Platform in Initiatives owned by other Customers and only erased when those Initiatives are erased.</p>

3.6. Alliantist as the Data Processor will assist the Customer as the Data Controller in meeting the Customer's obligations under Regulation (EU) 2016/679 and allowing data subjects to exercise their rights under Regulation (EU) 2016/679. To that end Alliantist has a range of policies, procedures and approaches such as:

3.6.a. Data Protection Officer (DPO) – Alliantist has nominated an appropriate DPO and they can be contacted at dpo@pam-it.com. Alliantist also has data protection, information security and a range of other Policies and Controls in line with ICO GDPR recommendations as well as ISO 27001:2013 and ISO 27701:2019, to UKAS independent certification standards.

3.6.b. Data Subject Rights Request – contact support@pam-it.com Alliantist will process the request in line with GDPR obligations and will only process valid request. Any information

requests sent direct to Alliantist by external parties that should be for the Customer as Data Controller will be redirected back to originating party and alerted to the Customer. No information will be shared with any other party without that Customer first approving it in writing. Alliantist also operates lawful policies and processes for all individuals rights; right to be informed; right of access; right to rectification and data quality, right to erasure, retention and disposal, right to restrict processing; right to object; rights to data portability and rights related to automated decision making.

3.6.c. Security Incidents and breach notifications - outbound: Alliantist operates a security incident process that also complies with ISO 27001. In the event that Alliantist suffers a breach that has a potential impact on the rights and freedoms of data subjects it will notify the Customer's Lead User within 24 hours of the breach or as soon as it becomes aware and work with the Customer to address the consequences including its legal obligations and those as a responsible supplier.

3.6.d. Security Incidents and breach notifications – inbound: Customer will report any Platform security incidents, events or weaknesses within 24 hours or as soon as it becomes aware of them to support@pam-it.com and Alliantist processes will commence. Alliantist will not be liable for any loss or damage arising from Customer's failure to comply with these requirements.

3.6.e. Alliantist undertakes to make available to Customer information necessary to demonstrate compliance with these obligations including, subject to the confidentiality obligations in this Agreement and that the Customer, or the Customer's representative, is not a competitor of Alliantist, sharing results of relevant audits, independent certifications and standards obtained.

3.6.f. Alliantist will assist Customer if requested with reasonable cooperation, taking into account the cost of the Services, to fulfil its obligation to carry out a data protection impact

assessment related to Customer's use of the Services.

3.6.g. Alliantist is registered to the UK Supervisory Authority (ICO) as a Data Processor (and a data Controller for its own business).

4. Billing, Payment, Term and Termination

- 4.1. Fees payable by the Customer for the Services are set out in the Proposal. Fees include access to the Services as described and include Platform maintenance with technical support for the Customer Lead User and authorised administrators as may be further detailed in the Proposal. The fees also include automatic access to relevant Platform releases and enhancements for the functionality in scope on the Proposal. Registered User support is covered in the fees through the Help Documentation and includes tours, videos and other support materials on the Platform.
- 4.2. Unless otherwise stated in the Proposal this Agreement shall last for the initial term of one year (Initial Term). Unless stated otherwise in the Proposal, the fees are invoiced annually in advance. All payments from the Customer are due 7 days of the date of invoice.
- 4.3. After the end of the Initial Term (or any Renewal Term), unless terminated in accordance with the terms of this Agreement, the Agreement will automatically continue for a further period of one year (Renewal Term). Unless agreed otherwise, fees for the Renewal Term shall be payable in the same manner (monthly, quarterly, annually) as for the Initial Term. Alliantist will be entitled to revise the fees in line with RPI upon renewal. Any further increase to the fees will only take effect if the Alliantist gives the Customer 30 days' written notice and during such notice period the Customer will be entitled to immediately terminate without liability.
- 4.4. Either party may terminate this Agreement on a minimum of 30 days' notice, such notice to expire at the end of the Initial Term or any Renewal Term.
- 4.5. Additional Registered Users or increases to the Services scope e.g. adding an optional extra such as policy packs or supply chain accounts may be agreed between the parties at any time subject to the relevant fee payment as set out in the Proposal or the price as quoted at the time of request. Registered User numbers are reviewed quarterly or at other intervals as needed and paid pro rata for any period added then aligned with the usual payment period thereafter. Subject to the fees in the Initial Term not falling below the Minimum Fee any of the Services can be

adjusted accordingly and fee changes reflect the ongoing change in use.

4.6. All fees assume a fair and acceptable use of the Services by the Customer and the Registered Users. In the event that the use of the Platform or the Services by the Customer exceeds fair and acceptable use Alliantist will alert Customer to the issues in writing and give the Customer the opportunity of easing use or paying for the extra service requirements.

4.7. All fees exclude VAT and other government taxes.

4.8. Either party may terminate this Agreement and any Proposal immediately upon written notice if the other commits a material breach of the Agreement and which (in the case of a breach capable of remedy) shall not have been remedied within 30 days. A material breach includes (i) a failure by Customer to make payment in accordance with this Agreement; or (ii) the other party has a liquidator, receiver, administrator or administrative receiver appointed in respect of the whole or any part of its undertaking or assets; or (iii) the other party ceases or threatens to cease to carry on business; or (iv) the commencement of negotiations with all or any class of that party's creditors with a view to rescheduling any of its debts, or making a proposal for or entering into any compromise or arrangement with its creditors other than for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party; or (v) a data breach that increases risks to the rights and freedoms of data subjects' information held on the Platform.

4.9. On termination for any reason:

4.9.a. All rights granted to the Customer under this Agreement including without limitation the license to use the Services shall cease and the Customer shall cease all activities authorised by this Agreement;

4.9.b. The Customer shall immediately pay to Alliantist any sums due to Alliantist under this Agreement, except where any sum of money shall be recoverable from or payable by Alliantist, the Customer may deduct same from any sum then due to Alliantist under this Agreement;

4.9.c. Customers can remove Customer Organisation Data from the Platform at any time.

5. Warranties, Indemnities and Liability

- 5.1. Alliantist warrants that the Platform shall perform substantially in accordance with the specifications set out in the proposal, Help Documentation and reflect the features and services expressed from the pam website.
- 5.2. Customer hereby acknowledges and agrees that access to the Services may be affected by local network telecommunications activity; government networks, electronic mail failure, capacity and compatibility with third party communication equipment, communication software, web browsers and internet (or intranet) enabled software. Alliantist hereby disclaims and Customer hereby waives any and all Alliantist responsibility for any failures in connection with local market network telecommunication activity, government networks, electronic mail failure, capacity and compatibility with third party communication equipment, communication software, web browsers and internet (or intranet) enabled software.
- 5.3. Alliantist shall not be liable for any failure to perform its obligations under this Agreement because of circumstances beyond its control which such circumstances shall include (without limitation) natural disaster (including widespread infectious disease, including epidemics and pandemics), terrorism, labour disputes, war, declarations of governments, transportation delays, telecommunications failure and misuse of the Services by Customer.
- 5.4. Alliantist agrees, subject to the limit of its insurance cover to indemnify Customer against all claims, demands, suits, liabilities, costs, expenses (including reasonably incurred legal fees), damages and losses suffered or incurred by Customer arising out of a third-party claim against Customer in respect of infringement of a third party's intellectual property rights arising out of Customer's use of pam. This indemnity shall not apply to the extent that a claim under it results from Customer's negligence, wilful misconduct, or modification from the specification. It is subject to Customer immediately notifying Alliantist of any claim and in any event within 3 months; Customer not admitting any fault or making any offer to settle and Alliantist having sole control of the claim with reasonable assistance as required from the Customer.
- If Customer is prevented from using the Platform thereafter Alliantist will at its sole discretion and cost either: source the rights to continue use; replace the disputed intellectual property and modify pam such that the purpose is still served; or terminate the Agreement and refund

Customer any unused but prepaid fees.

- 5.5. Other than to the extent prohibited by law, or liability in relation to clause 5.4, in no event shall the total aggregate liability of Alliantist exceed the annual fees paid in the previous year by the Customer.

6. Confidentiality

- 6.1. pam, pam Policies, Virtual Coach and the Help Documentation are proprietary to Alliantist and contain valuable trade secrets. The Customer shall at all times keep the software, policies, documentation, technical or commercial information, inventions or processes and any and all information concerning Alliantist's business or products and which have been disclosed to the Customer by Alliantist and which are of a confidential nature in strict confidence and shall not permit the same to be used, copied, disclosed or disposed of except in accordance with this Agreement.
- 6.2. The Proposal along with any Special Terms of this Agreement are confidential and may not be disclosed by either party without the prior written consent of the other party.
- 6.3. Where Customer discloses confidential information to Alliantist, Alliantist agrees to protect the Customers confidential information with the same standards and integrity as it uses in respect of its own confidential information.
- 6.4. The receiving party may disclose information of a confidential nature to such of its employees as need to know the same for the purpose of discharging the receiving party's obligations under this Agreement and shall ensure that such employees are subject to obligations of confidentiality corresponding to those set out in this Agreement.
- 6.5. The provisions of this section 6 shall: (i) not apply to information which is already public knowledge or becomes so at a future date (other than by breach of this Agreement); (ii) not apply to information which is known without restriction to the receiving party at the time of disclosure without breach of any obligation of confidentiality; (iii) not apply to information which is shown to the reasonable satisfaction of the originating party to have been generated independently by the receiving party; (iv) remain in full force and effect notwithstanding termination of this Agreement

for any reason.

7. Contract Management

7.1. The Customer shall provide a nominated name and email address being the Lead User to deal with Alliantist over the Customer's use of the Platform. The Lead User will be granted system administration rights and will participate in reviews with Alliantist from time to time. Alliantist will notify the Lead User in the event of a data breach. The Customer can nominate a replacement Lead User on written notice to Alliantist. The role of Lead User may be shared between multiple people, provided that Alliantist is entitled to treat each person as being fully authorised to represent the Customer independently.

8. General

8.1. As is common for all SaaS ('software as a service') vendors, Alliantist may from time to time need to alter the terms. Therefore, we reserve the right to alter this Agreement at any time by posting such changes to the Customer at its nominated Lead User email address and through the Alliantist website. If these changes may have an adverse effect on Customer's business where it may want to object to such change, the Customer should raise such concerns with the relevant Alliantist customer success manager in the first instance.

8.2. The Customer's continued use of the Services after changes to these terms, as detailed in clause 8.1 above constitutes your binding acceptance of such changes. Such amended Agreement will become effective upon the earlier of your continued use of the Services, or 30 days from notification of the changes. Customer warrants that it shall be deemed to have reviewed the most up to date version of these terms at the start of each Renewal Term; or upon any variation to the Services.

8.3. The Platform may contain links to other third-party web sites. Alliantist is not responsible for the privacy practices or the content of these other web sites. Registered Users will need to check the policy statement of these other web sites to understand their policies. Registered Users who access a linked site may be disclosing their private information. It is the responsibility of the

Registered User to keep such information private and confidential.

- 8.4. Unless otherwise specified in the Proposal, service and support shall be provided subject to the terms set out in the support policy available in the footer of the Platform and on the website.
- 8.5. Unless specifically agreed otherwise, by entering into this Agreement Customer grants Alliantist permission to use the Customer's name and logo in its marketing and promotional materials including without limitation its website and social media channels.
- 8.6. This Agreement will be governed by and construed in accordance with English Law, without giving effect to its conflict of law provisions or Customer's actual state or country of residence. Any claims, legal proceeding or litigation arising in connection with pam will be brought solely in England, and Customer consents to the exclusive jurisdiction of such courts provided that each party shall have the right to enforce a judgment of the English Courts in a jurisdiction in which the other party is incorporated or in which any assets of the other party may be situated.
- 8.7. A person who is not a party to this Agreement may not rely upon or enforce any rights pursuant to the Contracts (Rights of Third Parties) Act 1999.
- 8.8. This Agreement including the Proposal, privacy policy and support policy constitutes the entire agreement between Customer and Alliantist.

Any questions or issues should in the first instance be dealt with using the normal pam support channels support@pam-it.com and then escalated if required thereafter.