Frequently Asked Questions and Useful Links (Technical/Not Product Usage Related)

Document Version 1.04 01 October 2019

Software Version PAMMS v 2019.2.0.023

Frequently Asked Questions and Useful Links

This document summarises key questions HAS Technology are asked regarding the technical specification, technical delivery, information security and service expectations regarding their Provider Assessment & Market Management Solution (PAMMS). For information about using PAMMS, see the PAMMS User Guides, How to Guides and FAQs.

Frequently Asked Questions

Where is PAMMS Hosted?

PAMMS services are hosted on Amazon Web Services (AWS). See Useful Links – AWS Hosting for further information. We plan to migrate this to Microsoft Azure at some point in the future. The Amazon Web Services data centre is hosted in Ireland, while the Azure data centre is hosted in London. As such, we can confirm that all data will be hosted in the European Economic Area (EEA) as required. Irrespective as to where the data is held, it's also worth noting that PAMMS does not contain any personally identifiable data (PID).

What is your data archiving and retention policy?

We do not currently archive data as information is retained indefinitely. Assessments are held in the solution for as long as they are current, when a new Assessment is made it overwrites the previous one. Please note that Assessments contain no sensitive personally identifiable information.

Are your Information Security arrangements certified to ISO27001 or Cyber Essentials?

Yes, HAS Technology are ISO27001 certified.

Are you DPA Registered?

Yes, our DPA Registration number is ZA249143.

What Information Security Systems and Policies do you have in place to ensure our data is safe?

We deploy an ISO27001-accredited Information Security Management System, which is comprised of multiple policies that are designed to ensure the security of every aspect of the system. Policies include our main Information Security Policy, our System Access Control Policy, Removable Media Policy, Equipment Disposal Policy, Data Protection Policy, Information Classification & Handling Policy and more. All documents are available on request. We employ a Group Data Protection and Compliance Officer, who is responsible for the re-auditing of our ISO27001 accreditation and continuously improving our policies and procedures throughout all business areas to ensure that information security is maintained as per the high requirements of our customers.

From our front-tier to the back-end of our solution, we apply the latest security techniques, devices and monitoring methods to manage our cloud services and ensure that our systems are not vulnerable to unauthorised access. This includes security monitoring and adhering to our comprehensive Incident and Patch Management processes.

What is the service model of the Cloud Service i.e. IaaS, SaaS, PaaS.

PAMMS is a SaaS service, fully hosted and managed by us.

Are any third-party partners involved in delivering the proposed system?

We work with numerous suppliers in the delivery of the solution, including Amazon, as PAMMS is hosted in its AWS environment. However, we are *fully responsible* for the successful delivery of the solution as well as for managing and supporting the solution.

For all locations used to provide the Cloud Services, we document the measures in place to protect against unauthorised access, tampering, theft or reconfiguration of systems.

How does the Cloud Service provide sufficient separation of PAMMS data and services from other consumers of that Cloud Service.

All customers are virtually segregated into distinct ADASS regions within PAMMS. This means that, as per our Data Sharing Agreement, data may be shared within Local Authority localities or ADASS regions. This is because PAMMS is designed to improve data sharing and to ensure Councils do not have to duplicate effort by assessing the same independent care provider (who is working cross-boundary) twice. PAMMS does not hold any sensitive personally identifiable information. Personal information such as name, telephone number and email addresses are always processed to meet our contractual obligation so users of PAMMS QA can access the solution securely to undertake key tasks and actions. As this personal information is not shared across local authorities, the PAMMS solution is an ideal method for sharing Assessment information between neighbouring councils.

Is the status, location and configuration of all components tracked throughout their lifetime within the service?

Yes, all components within the AWS environment are tracked extensively by Amazon. AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked. Assets undergoing maintenance are checked and monitored for ownership, status and resolution.

Are changes to the service assessed for any potential security impact? Describe how is this achieved.

HAS Technology operate a comprehensive Change Management Policy before any changes are made to our systems. As part of our Change Management Policy, HAS Technology has comprehensive Risk Assessment and Change Advisory processes in place.

We can confirm that we have a Change Advisory Board for all software releases and an Emergency Change Advisory Board (ECAB) for any patches required who make decisions based on the severity and the urgency of the patch we are rolling out to our solutions.

The ECAB is also chaired by the organisation's Group Technical Officer, who is imperative and instrumental to any changes that are made to our products and services, as well as any potential security impact these might have on the Service.

Are changes managed and tracked through to completion?

All changes are fully managed from beginning to end as part of our Change Management Process.

Once an initial Change Request has been made, this must be approved by a Technical representative, an Operational representative and a Change Management representative before the change can be made.

Once the change has been made, this is fully reviewed and documented throughout the various stages using HAS Technology's online ticketing system on the Customer Portal.

How are potential new threats, vulnerabilities or exploitation techniques that could affect the service assessed and how is appropriate corrective action is taken?

Any evolving vulnerabilities are monitored against industry-leading resources, such as the OWASP Top 10. Any vulnerabilities then identified within PAMMS are assessed for risk and resolved in line with our comprehensive Patch Management Process. We operate a Penetration Testing Policy which ensures that software is penetration tested prior to release after all major updates or major technological changes. This occurs in addition to regular, scheduled periodic penetration testing which occurs *at least* once a year.

Are the sources of information relating to threat, vulnerability and exploitation technique monitored?

Our Development Team proactively monitor against industry-leading sources such as the OWASP Top 10.

Are the severity of threats and vulnerabilities considered within the context of the service?

Yes, any vulnerabilities identified will be assessed and a risk level assigned to them. Vulnerabilities will generally be mitigated according to HAS Technology's Patch Management Policy, which states that patches are generally prioritised and mitigated as follows:

- **Emergency patch**: A patch that fixes a known security vulnerability that presents a real, publicised/well-known threat
- **Critical patch:** A patch that fixes a security vulnerability that presents an unpublicised threat or resolves another important issue within the software program.
- **Medium:** targets a security vulnerability or other software issue that is important to resolve but not imminently
- **Not Critical (Low):** a standard patch release update

Are known vulnerabilities within the service tracked through a suitable change management process until appropriate mitigations have been deployed?

Known vulnerabilities are tracked through HAS Technology's Change Management Process until appropriate mitigations have been deployed as follows:

- Change Requests are raised, which include change details, back-out plans and impact to the customer
- Change Requests are reviewed by a Change Management Board. This includes stakeholders from all areas of the business

- In the rare occurrence of an emergency change, the Emergency Change Board will be assembled. This consists of senior members of staff who can analyse the change impact and approve as necessary

Changes are tracked throughout using HAS Technology's online ticketing system, creating a full audit trail of each stage of the process as required.

Do you have an up to date Vulnerability Management policy? Does it include timescales for implementing mitigations to all vulnerabilities found during the above process?

We can confirm that we do have a regularly updated Vulnerability Management Policy. This includes timescales for implementing mitigations to any vulnerabilities found according to their priority level:

- **Emergency patch:** A patch that fixes a known security vulnerability that presents a real, publicised / well-known threat
- **Critical patch:** A patch that fixes a security vulnerability that presents an unpublicised threat or resolves another important issue within the software program
- **Medium:** targets a security vulnerability or other software issue that is important to resolve but not imminently
- **Not Critical (Low):** a standard patch release update

What analysis system do you have in place to identify and prioritise indications of potential malicious activity?

Our Development Team proactively monitor PAMMS' audit trail and log files to determine if there are any indications of potential malicious activity and take appropriate action.

Is an Incident Management policy in place for the service to ensure that security incidents are acted upon?

In line with our ISO27001:2013 accredited Information Security Management System, we have an extremely comprehensive Incident Management Process in place for any technical incidents:

1. If an incident is reported from an external source, this will be recorded in our online Customer Porta and our EQMS system as a 'security issue'. If an incident is reported from an internal source, this will be recorded in our EQMS system as a 'security issue'.
2. If the incident is a security weakness, a technical security breach or a physical security breach there is an obligation on us to take immediate action to secure and contain the issue and reduce the risk of further breach or incident. If the incident is a data/privacy incident, this will invoke the Data Incident Notification and Management Procedure. A copy of this procedure can be provided on request.
3. If it's not a data incident, then there will be verbal communication with the required stakeholder (internal or external) ASAP. This is backed up with email evidence.
4. The incident will also be categorised as either a Major Incident, a Minor Incident or a Security Weakness. If it is a Major Weakness it is immediately escalated to our Infrastructure Team (whom are on-call 24/7/365). They will then initiate an incident investigation with immediate effect. If the incident is a Minor Incident, our dedicated Infrastructure Team will investigate and manage the incident within normal office working hours. If the incident is a Security Weakness, this will be logged in our Incident

Management System. Volumes of activity will then be reviewed quarterly to identify trend patterns and implement corrective action (such as re-training or communication updates).

5. Irrespective of which categorisation of incident it is, on completion of incident/breach correction activities, the Lead assigned to the incident will conduct Root Cause Analysis and identify corrective actions to prevent further incident activity. A detailed incident report will also be written which will be shared with the relevant stakeholders as required.
6. The incident will be closed, the Root Cause Analysis (RCA) log completed and corrective actions will be closed after the Infrastructure Manager has provided his approval for incident closure.

We take technical incidents extremely seriously and undertake comprehensive processes and procedures to ensure that all incidents are dealt with sufficiently, in the shortest amount of time possible and that lessons are learned from any incident are applied to ensure that they are not repeated.

Our Incident Management Policy includes pre-defined processes for responding to common types of incident and attack. Incident reports are also written following the event, to ensure that common incidents are handled correctly. Any lessons learned from the handling process are documented fully.

Does your Incident Management policy include a defined process and contact route for customers to report security incidents?

Customers should contact our Support Team via the online Customer Portal so that the incident can be reported in our ticketing system in the first instance. The incident will be assigned an internal lead and will be recorded in our EQMS system as a 'security issue' and the Incident Management procedure will be instigated immediately.

A detailed incident report will be written and shared with the customer and all relevant stakeholders.

Is all development of the service carried out in line with industry good practice regarding secure design, coding, testing and deployment?

Our Development Team have a full source code and release control system, which is implemented with Jira, SVN and TeamCity. All changes to code are rigorously documented.

What processes do you have in place to review new and evolving threats when developing PAMMS?

New and evolving threats are proactively reviewed by our Development Team for every major release. The Development Team then take mitigating actions against all identified threats. We also ensure that we upgrade the Apache Tomcat components to the latest versions, as per our own Patch Management Policy. Additionally, we review the SSL ciphers used using Qualys SLL Labs.

What configuration management processes do you have in place to ensure the integrity of the solution through development, testing and deployment? Do you follow any frameworks for this?

All code is stored in SVN and built afresh by TeamCity to generate a release. Bugs and issues are tracked in Jira and can be tracked from original files checked into SVN through to the final deployment.

What internet protocol do you use to ensure that data is kept secure?

We use https. PAMMS also has boundary protection from a firewall. This restricts access to port 443.

Is all data in transit protected between all end user devices and internally within the Cloud Service?

Yes, all data in transit is protected via HTTPS and secure ciphers between all end user devices and the Cloud service.

Are controls in place to identify all connecting users and services set to an appropriate level to ensure that they only access the data or function they are authorised for?

Our PAMMS solution has role-based access controls to restrict the functionality and data availability to the level required to perform a role. Users are required to enter valid login credentials to gain access to the solution, unauthorised users will automatically be denied access. All connecting users are also recorded within the audit log for PAMMS. Audit information is available from PAMMS Analytics. Customers who have not subscribed to PAMMS Analytics can request an audit log via our Customer Portal.

Will the system be configurable to suit the needs of our organisation's password policy?

PAMMS has its own Password Policy, which is designed to meet the vast majority of Local Authority and Care Provider's rigorous password requirements. The rules around passwords are as follows:

- Minimum 8 characters
- Password must contain character(s) from at least 3 of the following groups: upper case letters, lower case letters, numbers, special characters
- When changing a password, the new password must be different from the last 4 passwords
- Passwords must be changed after a minimum period of 90 days

If locked out, users can request to reset their password via email by entering their username at the PAMMS website. They will then get a secure email linking them to this functionality.

Are system timeouts configurable to log the user out after periods of inactivity?

System time-outs are fully configurable within PAMMS. You can set these in the **Systems** tab of PAMMS.

We have a policy that all external applications are security tested by staff or independent security consultants before we purchase. We are considering purchasing PAMMS, would we be able to do this prior to purchase?

We are happy for organisations to carry out their own, independent testing. We kindly request a minimum of four weeks' notice prior to the testing period. Should any vulnerabilities be identified, these will be resolved prior to purchase at no cost.

What measures are in place within the Cloud system to protect against unauthorised access, tampering, theft or reconfiguration of systems?

Amazon Web Services (AWS) feature extensive security to protect against unauthorised data access, tampering, theft or reconfiguration of the systems. These include:

- Network firewalls built into Amazon VPC and web application firewall capabilities in AWS WAF. These let us create private networks and control access to instances and applications
- Customer-controlled encryption in transit with TLS across all services
- Connectivity options that enable private or dedicated connections from the office or on-premises environment
- Automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities

To ensure its data centres are physically secure, Amazon also ensure that they are protected by the following measures:

- **Employee data centre access:** AWS provides physical data centre access only to approved employees. All employees who need data centre access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access. Each access is time-bound. Requests are reviewed and approved by authorised personnel and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions
- **Third-party data access:** Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access. These requests are time-bound. These requests are approved by authorized personnel and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorised staff
- **CCTV:** Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements
- **Data centre entry points:** Physical access is controlled at building ingress points by professional security staff utilising surveillance, detection systems and other electronic means. Authorised staff utilise multi-factor authentication mechanisms to access data centres. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open
- **Intrusion detection:** Electronic intrusion detection systems are installed within the data layer to monitor, detect and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where someone exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centres for immediate logging, analysis and response

What technologies and strategies are used to ensure that data stored in the Cloud system are not accessible by local, unauthorised parties?

Data at rest can be encrypted in AWS if and where required. It's possible within AWS to create an encrypted file system so that data and metadata is encrypted at rest using an industry-standard AES-256 encryption algorithm.

While we do not do this as standard, we would be more than happy to discuss this further on request. Please note that *data is extremely secure* and PAMMS does *not contain any personally identifiable data* (PID). As such, encryption of data at rest has not been required by any of our customer base thus far.

We are considering purchasing PAMMS. Is there a requirement to install any client software?

There is no requirement to install client software as PAMMS is a browser-based solution. The only requirement to run PAMMS is to have JavaScript enabled within the user's browser. This is required so as to enable offline working within the solution.

Can you provide us with a support statement for browsers?

We recommend using the latest (but not beta or test version) releases of Chrome or Firefox. The following browsers are currently supported:

- Internet Explorer v11 or above with compatibility mode disabled
- Google Chrome v56.0 and above
- Mozilla Firefox v51.0 and above
- Safari running on iOS device version 12.0 and above can be used to *view information only* and should not be used to complete tasks, Assessments or Action Plans

PAMMS may work on older versions of these browsers or other browsers but we can't verify or support those installations. HAS Technology always recommends using newer browsers as they are more secure. The currently deployed version of PAMMS is not supported on the Microsoft Edge browser.

You should ensure that browser properties are set to allow JavaScript to be run by sites that you visit. This setting is accessed in a different way for each browser type.

HAS Technology recommend using a 4G mobile connection (though a 3G connection will still work) if running PAMMS on a Mobile Device such as a smart phone or tablet.

Any devices should have a *minimum* screen size of 4 inches.

What process do you use for informing us of support depreciation for browsers and equipment?

Our standard policy is in line with Microsoft End of Life support unless we notify you otherwise. You will be informed of future depreciation in advance by means of the Customer Portal and email notifications. Depreciation information and upgrade instructions will also be included in any Release Notes.

What approach do you take to releasing product upgrades?

Upgrades and patches are initially applied to our internal Test environments for validation. Depending on the nature of the upgrade or patch, it may be released on a Test environment for User Acceptance Testing by representatives from our customer base. Once approved for release, the upgrade or patch is applied to the Live environment and automatically becomes available to all organisations accessing the system. Upgrades and patches are usually applied outside of normal working hours.

How are application updates rolled out?

Customers are informed in advance of upcoming upgrades and release notes are published via email message and via the Customer Portal. Release notes are made available to all customers and documentation and user guides are updated to reflect any changes.

Do you have a PAMMS Training database as we are concerned that new staff may accidentally make modifications to our data?

We have a centralised training environment that all customers can use.

How does the PAMMS Portal cater for the addition and deletion of users?

One or more members of staff are given Locality Administrator permission. These Administrators can add accounts and remove or block access.

What happens to our data if our contract ends?

Our Standard Terms and Conditions cover the standard procedure regarding what happens when a contract ends - including data securitisation, interim data storage, data handover and disposal arrangements. These terms will be amended to include any product-specific and future product Terms and Conditions.

Are we able to access audit logs in case we have legal disputes with suppliers or need to perform case reviews?

Audit logs can be retrieved through our reporting engine PAMMS Analytics. If you do not subscribe to PAMMS Analytics, you can request an audit log through the Customer Portal.

Are any Software Escrow Arrangements in place?

We can provide a Software Escrow arrangement as a purchase option.

What backup arrangements are in place?

Data is backed up at 3:00 am each day and copies of old assessments can be recovered. We aim to restore data within 4 hours.

What support and response times can we expect under our Service Level Agreement?

Support is primarily self-service through the HAS Technology Customer Portal.

Service Level Definition	Priority	Response Time in Core Service Hours	Response to Fix Time in Core Service Hours (elapsed time in brackets)
Defined as a service failure which, in the reasonable opinion of the Customer, has the potential to have a critical adverse impact on one or more end users and/or the Customer's ability to use the Licensed Software Product. For example: • causes significant financial loss and/or disruption to the Customer • adversely impacts the Customer's public image or may result in media comment which will impact adversely upon the Customer • result in any material loss or corruption of data belonging to the Customer, or in the provision of incorrect data presented to the Customer	Urgent (Priority 1)	0 – 2 hr	8 hrs (i.e. 1 working day)
Defined as a service failure which, in the reasonable opinion of the Customer, could have a major adverse impact on critical end users and/or the Customer's ability to use the Licenced Software Product or have a moderate adverse impact on all end users and/or the Customer's ability to use the Licenced Software Product. For example: • PAMMS solution still accessible however assessments cannot be submitted or synchronised	High (Priority 2)	0 – 8 hrs	3 working days
Defined as a service failure affecting certain areas of the product, which, in the reasonable opinion of the Customer, are not critical and do not impact normal use or where a valid work-around has been provided to the Customer and/or end user. For example: • system performance is reduced but it is still possible to fully use the system	Medium (Priority 3)	2 working days	3 working months
Defined as a service failure comprising of a cosmetic flaw affecting only the presentation of the Licenced Software Product, which	Low (Priority 4)	2 working days	3 working months or next product release

does not undermine the Customer's and/or end user's confidence in the information being displayed. For example: • icons or text unaligned or misspelt			

What additional controls are in place to ensure that only authorised individuals are able to perform actions affecting our service and data through support channels?

Your organisation will nominate staff to be given User Account Administrator privileges to login to our Customer Portal. These staff can add additional users and apply roles and access levels to these users. These staff are also responsible for disabling Customer Portal access.

What escalation procedures are in place if we report an issue?

Our escalation procedures are included within the Terms and Conditions of our contract and, as a standard, follow the procedure below.

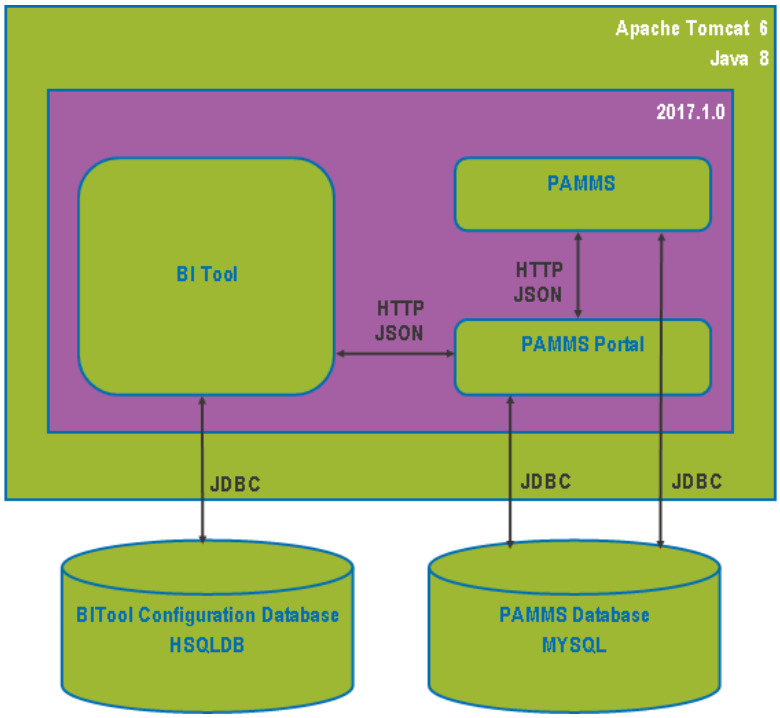
Escalation Level	Escalation Rationale	Contact	Escalation Timescales
1	A Ticket is logged with the Service Helpdesk via the Has Technology Customer Portal. The first point of contact is at Level 1.	2nd Line Support Analyst	As per Service Level Agreement
2	If the Service Helpdesk does not respond within the agreed time specified, the Ticket will be escalated to Level 2.	Support Team Leader	Within 2 working days (16 hours) of Level 1
3	If the Support Team Leader does not respond within the agreed time specified, the Ticket will be escalated to Level 3.	Operations Director	Within 2 – 3 working days of Level 2
4	If the Support Manager does not respond within the agreed response time specified, then the Ticket will be escalated to Level 4.	Managing Director	Within 2 – 3 working days of Level 3

What dispute resolution procedures are in place if we escalate an issue?

Our dispute procedures are included within the Terms and Conditions of our contract.

What technology stack is being used for the PAMMS solution?

An overview of the Stack Technology Configuration is shown below:



The PAMMS application and MySQL are run on a hosted server. The firewall is provided by AWS and we mask out all incoming ports except port 443 and ports to remotely administer PAMMS. The hosted system is very self-contained. Backups are provided using Skeddly. Each server has a single IPv4 address which links to the domain name via the DNS.

I work with a partner in a different region. Would they be able to use PAMMS?

As PAMMS is offered as a Software Service (SaaS or Cloud) it is accessed via an internet connection. Service providers who work across regions can also utilise PAMMS, though the Templates and practices may differ slightly between regions.

Are there any requirements to integrate with any in-house systems or software such as online payment systems or Microsoft Office?

There is no requirement to integrate with any in-house systems.

How is local printing achieved?

Printing is achieved through an export to pdf option within the solution. Users can select their printer of choice from those available.

How does the application segregate information from the other customer's information if they are hosted on the same database or platform?

User accounts are tied to the organisation to which the user belongs. On authentication, the user is presented with a view based on their own organisation and based on their role. Security is also implemented to support the approval and sign-off elements of the application functionality. These security measures are implemented to support the solution workflow

rather than to protect the data. A key purpose of the solution is to *share* information between organisations that utilise the PAMMS platform and the process results in information being made publicly available.

No personal or sensitive data about application subjects is held within the solution.

Does PAMMS provide open APIs (conforming to open standards) so that we can integrate it with our other systems?

Yes, though a charge will be made for this. We would need to discuss this during a thorough Business Needs Analysis (BNA) prior to implementation. If feasible, we would typically develop the solution after fully specifying the integration, through either SFTP or Web Services. The cost would depend on the number of days required to develop the solution. Please contact HAS Technology to discuss this.

If changes are made to Social Care Legislation, will these be reflected on the portal?

Yes, HAS Technology are fully committed to ensuring legislative changes are reflected in the PAMMS model.

What measures are taken to protect customer data if the service has to be re-provisioned, migrated or de-provisioned during the supply of the Cloud Service. For example, is all of the data securely erased when resources are moved or re-provisioned?

Should customer data need to be re-provisioned, migrated or de-provisioned during the supply of the Cloud service, this will be handled to ensure secure sanitisation at all times. If resources need to be moved or repositioned, a back-up copy of the data will be taken and the remaining data securely erased.

Is all of the storage media used to hold data sanitised or securely destroyed at the end of its life?

Amazon have a comprehensive Media Destruction Process to ensure that any storage media used to hold customer's data will be sanitised and securely destroyed at the end of its life.

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service and eventually destroy the devices when they are no longer useful.

When a storage device has reached the end of its useful life, AWS decommissions media using industry-leading techniques. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

Is all equipment potentially containing data, credentials or configuration information for the Cloud Service identified at the end of its life? Are components containing sensitive data sanitised, removed or destroyed as appropriate?

Yes. AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance and descriptive information for AWS-

owned assets. Following procurement, assets are scanned and tracked and assets undergoing maintenance are checked and monitored for ownership, status and resolution. Once equipment has reached the end of its life, it undergoes a Media Destruction process by AWS.

What availability is the Cloud Service provider committed to? How long does it take them to recover from outages?

As PAMMS is hosted in Amazon AWS, we can agree to strong availability commitments on behalf of our customers and are happy to commit to a service level target of 99.9%.

With regard to recovering data in PAMMS, back-ups from the previous night can be restored within a couple of hours. With regard to data loss, this would be limited to anything added between the time of the previous night's backup and the time of the system outage. The system backups can be restored to a separate instance to recover individual files if required.

Useful Links – AWS Hosting

Compliance and Certification Standards

https://aws.amazon.com/compliance/programs/

Statement of data centre certification levels

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

How access control is organised

http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

How data at rest is stored and secured

https://aws.amazon.com/compliance/data-privacy-faq/

What Disaster Recovery is in place

A daily backup is used to recover to a new environment if a catastrophic failure occurs.

https://aws.amazon.com/disaster-recovery/

Compliance and Certification Standards

https://aws.amazon.com/compliance/programs/

Useful Links SSL Deployment

Qualys SSL Labs

https://www.ssllabs.com/

Useful Links and Contacts

Queries about the assessment methodology

Guy Pettengell, ADASS Eastern Region - guy.pettengell@hertfordshire.gov.uk

Key Account Information and Technical Support

Ben Chance, HAS Technology Limited – ben.chance@hastec.ltd

HAS Technology Limited Customer Portal

Training will be provided on the usage of the Customer Portal.

https://has-customer-portal.assist.com/portal

HASTEC Limited
Four Oaks House
160 Lichfield Road
Sutton Coldfield
West Midlands
B74 2TZ

Tel: 0121 308 3010
Email: ben.chance@hastec.ltd
Web: www.pamms.co.uk