

General Contract Details – ICT Products and Services

12 Month Subscription to Faethm data analytics
platform – PSC-04-2019

Public Service Commission

Faethm Pty Ltd

QITC General Contract Details – ICT Products and Services – Issued May 2018 - Version 1.0.1

Table of Contents

Table of Contents.....	2
1. General information	3
2. As a Service.....	10
3. ICT Professional Services	20
4. Forming the Contract.....	22
1. Acknowledgements and certifications	22
5. Agreement	23
1. Agreement by Supplier	23
2. Agreement by Customer	23
Schedule 1 – Price and Payment Terms.....	24

Released under RTI - PSC

1. General information

The [General Contract Conditions - ICT Products and Services](#) apply to these Details.

The definitions and rules of interpretation applicable to these Details are set out in the [General Contract Conditions - ICT Products and Services](#).

1. Customer

Name

The State of Queensland acting through the Public Service Commission

ABN or ACN

ABN 73 289 606 743

2. Customer contact details

Authorised Representative 1

Jenny Stephensen

Position title / role

Manager, Workforce Futures and Inclusion

Phone number

07 3003 2897

Street address

Level 27, 1 William Street, Brisbane, QLD 4000

Postal address

PO Box 15190, City East, QLD 4002

Email

Jenny.stephensen@psc.qld.gov.au

Authorised Representative 2

Sandra Lerch

Position title / role

Executive Director, Workforce Futures and Inclusion

Phone number

07 3003 2711

Street address

Level 27, 1 William Street, Brisbane, QLD 4000

Postal address

PO Box 15190, City East, QLD 4002

Email

Sandra.lerch@psc.qld.gov.au

3. Supplier

Name

Faethm Pty Ltd

ABN or ACN or ABRN

ACN 611 627 368

4. Supplier Contact Details

Authorised Representative 1

Carolyn Colley

Position title / role

Chief Operating Officer

Phone number

[REDACTED]

Street address

Level 27, Tower One, Barangaroo, Sydney, NSW 2000

Postal address

Level 12, 10 Spring Street, Sydney, NSW 2000

Email

[REDACTED]

Authorised Representative 2

John Rogers

Position title / role

Director, Strategic Partnerships APAC

Phone number

[REDACTED]

Street address

Level 27, Tower One, Barangaroo, Sydney, NSW 2000

Postal address

Level 12, 10 Spring Street, Sydney, NSW 2000

Email

[REDACTED]



5. Products and Services and documents that form part of the Contract Clause 1.3 and 5

Applicable Products and Services

- Hardware
- Hardware Maintenance Services
- Licensed Software
- Software Support Services
- Developed Software
- As a Service
- ICT Professional Services

Documents

In accordance with clause 1.3(f) of the General Contract Conditions, the following documents are incorporated into the Contract by reference:

- (a) The Supplier's response to the DPC questionnaire for As-a-Services+Cloud-Vendor dated 19 June 2019.
- (b) Software & Infrastructure Architecture Document (FAETHM-001) current as at 18 March 2019
- (c) Faethm 2.0 Onboarding and Data Requirements

In the event and to the extent of any inconsistency between the terms of the above documents, the order of hierarchy in descending order will prevail.

6. Additional Provisions Clause 1.4

For the purpose of this Contract "Platform" has the same meaning as "As a Service" and these terms are interchangeable.

7. Term Clause 3

Start date

The start date of the Term is the date this Contract is executed by the parties or if executed on different dates, the latter of those dates.

End date

The end date of the term is 12 months (365 days) from the start date.

Extension options

Not applicable.

Notice period for extension

Not applicable.

8. Policies, codes of conduct, rules, standards and procedures Clause 4(h)

Site Policies

The Supplier must comply with all building access and security policies when attending the Customer's premises.

Policies, codes of conduct, rules, standards and procedures

The Supplier will comply with the following policies, codes of conduct, rules, standards and procedures in providing the Deliverables:

- Any rules, standards or codes of practice referenced in documents that are incorporated into the Contract in accordance with clause 1.3 (f)
- Any security and access rules or policies when attending the Customer's premises.

9. Customer Inputs Clause 4(k)

Details of Customer Inputs to be provided

The Customer will provide:

- Customer Data in the form of anonymised workforce data
- Input and feedback during the configuration of the As a Service
- Coordination of and access to personnel for training purposes.

10. Documentation Clause 4(n)

The Supplier will provide product Documentation for the As a Service including online help and user guides.

11. Training Clause 4(o)

Insert details of any training requirement

The Supplier will provide a 3 x 1 hour remote training session (after data loading) to train up to 15 Customer users from participating agencies in Platform best practice, use cases, and answer outstanding questions on Platform, methodology, etc. via the Zoom online meeting platform.

Rates for additional training

Not applicable.

12. Insurance Clause 4(q)

Workers compensation insurance as required by law.

Insurer: [REDACTED]

Policy Number: [REDACTED]

Policy Expiry Date: 31 May 2020

Public liability and products liability insurance minimum amount

Insurer: [REDACTED]

Policy Number: [REDACTED]

Policy Expiry Date: 16 June 2020

\$10,000,000

Professional indemnity insurance minimum amount

Insurer: [REDACTED]

Policy Number: [REDACTED]

Policy Expiry Date: 20 November 2019

\$5,000,000

Other insurances

Not applicable.

Minimum period of insurance (for insurance on a "claims made" basis)

The Supplier must maintain all required insurance policies which are maintained on a "claims made" basis for a minimum period of 4 years after the Contract ends in accordance with Clause 4(q) of the General Contract Conditions for ICT products and services.

13. Authorisations

Clause 4(r)

Not applicable.

14. Security

Clause 4(s)

Not applicable.

15. Acceptance Testing

Clause 6

Will testing of Deliverables be required?

Yes

No

16. Subcontractor(s)

Clause 8

Not applicable.

17. Background checks

Clause 8.2(d)

Not required.

18. Key Personnel

Clause 8.3

Not applicable.

19. Price and payment

Clause 9

Maximum price

The maximum total price of services provided under this contract is \$66,500 (excluding GST).

20. Cap on liability

Clause 12 and 13

Supplier's liability cap

The Suppliers liability is capped to an amount equal to the maximum Price payable under this Contract.

Supplier's liability cap for loss of Customer Data

The cap on liability (in the aggregate) is the greater of:

- (a) \$1 million; or
- (b) 3 times the total of all Prices payable under the Contract,

or as limited by law.

Customer's liability cap

The Suppliers liability is capped to an amount equal to the maximum Price payable under this Contract.

21. Intellectual Property Rights in Pre-Existing Materials

Clause 15.1

Pre-Existing Material

The Customer's Pre-Existing Material includes:

- Customer Data
- Any findings, conclusions or trends identified through previous analysis of Customer Data.

The Supplier's Pre-Existing Material includes:

- Supplier Data
- Any findings, conclusions, or trends identified through previous analysis of Supplier Data.

Customer's use of Pre-Existing Material

Not applicable.

Sublicensees and cost

Not applicable.

22. Intellectual Property Rights in New Materials Clause 15.2 and 15.3**New Material**

New Material includes data analytics outputs and insights generated by the Platform using the Customer Data, including but not limited to, reports, graphs, trends and findings.

Ownership of New Material

Will Intellectual Property Rights in the New Material be owned by the Customer or Supplier?

- Customer (clause 15.2 of the General Contract Conditions applies),
 Supplier (clause 15.3 of the General Contract Conditions applies).

23. Intellectual Property Rights in Third Party Materials Clause 15.4

Will any Deliverables incorporate any Third Party Material?

- Yes
 No

24. Customer Data Clause 16

The Faethm Platform combines public data, Customer Data (including Metadata) with proprietary analytics and machine learning to deliver insights to leaders of companies and governments that drive economic and social value. The Customer agrees to grant rights to the Supplier to use an unidentifiable aggregated copy of the Customer Data to support the advancement of the model on the condition that Customer Data is never used nor published in an identifiable form.

25. Confidentiality and Privacy Deed Clause 17(d)

Not applicable.

26. Conflict of Interest Clause 19.2

Nil

27. Termination for convenience Clause 21.3

If the Customer exercises its right of termination for convenience, no additional amount is payable to the Supplier (which is additional to the fees for the work supplied but not yet invoiced).

28. Business Hours Clause 24.1

Business Hours are 9.00am – 5.00pm AEST on Business Days.

29. Designated Environment

Clause 24.1

The Customer's data and processing environment relative to the Deliverables is:

- Microsoft Windows 10
- Microsoft Office 365
- Internet browsers including, Microsoft Edge, Google Chrome, Mozilla Firefox and Safari.

2. As a Service

1. Subscription Period

Clause 5.6(a)

Start of Subscription Period

The start of the Subscription period is the start date of the Contract.

Duration of Subscription Period

12 Months.

Notice period for non-renewal of the Subscription Period

No less than 30 days prior to the end of the Subscription Period.

2. Description of As a Service

As a Service

The As a Service being acquired is:

- Software as a Service
- Infrastructure as a Service
- Platform as a Service

Description of As a Service

The Software as a Service to be provided by the Supplier is the Faethm Platform available at <https://platform.faethm.ai>.

The Software as a Service includes:

- hosting services for the test and production environments necessary;
- ongoing supply, management and enhancement of the Software as a Service;
- support services;
- backup services for the Customer Data;
- provision of professional and technical advice as reasonably required by the Customer from time to time during the Contract Term.
- ongoing infrastructure monitoring, support and maintenance;
- continuous optimisation of the platform, software and services;
- storage space for files and Customer Data exported to and from the Software as a Service;

- shared software environment;
- shared hardware environment;
- dedicated database schemas for the Customer Data;
- backups of the Customer Data;
- business continuity and disaster recovery services;
- virus protection;
- operational support and maintenance of the Supplier's hardware hosting the Customer Data and the software applications that constitute the Software as a Service;
- operational support and maintenance of the Supplier's software applications required to provide the Software as a Service, including operating system software, application software and databases, if applicable;
- operational support and maintenance of the Supplier's network interfaces which will facilitate the Customer's access to and use of the Software as a Service through a web browser; and
- configuration management of the Supplier's hardware, software applications and network interfaces to ensure optimal operability and performance of the Software as a Service.

The Supplier will enable access to and use of the software application for up to 15 under an enterprise licence at the website address <https://platform.faethm.ai>.

The Software as a Service which is to be provided by the Supplier to the Customer must be the most current version of the software.

The Supplier is solely responsible for hosting the Software as a Service.

The Price payable by the Customer includes the provision of the required infrastructure, platform, hardware and software necessary to host, operate, support, maintain and enhance the Software as a Service.

The infrastructure, platform, personnel, methodologies and resources utilised by the Supplier to provide the Software as a Service must be the equivalent of or superior to the infrastructure, platform, personnel, methodologies and resources used by the Supplier when providing similar cloud services to other customers.

Scheduled Maintenance of the Software as a Service

The Customer's users will receive electronic notification of planned, scheduled maintenance activities, including the outage duration and timing, plus links to release notes for the maintenance activities.

The scheduled maintenance activities will include all critical and most emergency patches and all bug fixes (including technical stack and application patch sets).

The scheduled maintenance activities will typically occur during one of the Supplier's scheduled maintenance periods.

The Supplier must notify the Customer at least three (3) Business Days prior to conducting any scheduled maintenance via application pop-up or email. The Supplier will provide the Customer with details of the expected outage duration and timing together with details about the maintenance activities to be conducted by the Supplier.

The Supplier must use its best efforts to maintain the availability of the Software as a Service during the conduct of any scheduled maintenance.

3. Requirements

Clause 5.6(b)

Specifications for As a Service (or annex specifications to the Details)

The Supplier will provide the As a Service that includes standard functionality of the Faethm Platform. The Customer does not have any additional requirements or specifications for the As a Service.

4. Minimum system requirements and usage requirements

Clause 5.6(c)

Minimum requirements for Customer's IT System and Network

The minimum requirements for the Customer's IT System and network are:

- Google Chrome (Version 63)
- Mozilla Firefox (Version 57)
- Microsoft Edge (Version 41)
- Safari (Version 11)

Usage requirements for use of the As a Service

The Customer acknowledges and agrees that it will not:

- a) make the Platform or content available to, or use the Platform or content for the benefit of, anyone other than entities representing the State of Queensland, unless expressly stated otherwise in this Contract,
- b) sell, resell, license, sublicense, distribute, make available, rent or lease the Platform, include the Platform or in a service bureau or outsourcing offering,
- c) use the Platform to store or transmit infringing, libellous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights,
- d) use the Platform to:
 - i. store or transmit Harmful Code,
 - ii. interfere with or disrupt the integrity or performance of the Platform or third-party data contained therein,
 - iii. attempt to gain unauthorised access to the Platform or content or its related systems or networks,
 - iv. permit direct or indirect access to or use of the Platform or content in a way that circumvents a contractual usage limit, or use the Platform to access or use any of the Supplier's intellectual property except as permitted under this Contract,
 - v. copy the Platform or any part, feature, function or user interface thereof,
 - vi. copy content except as permitted in this Contract,
 - vii. frame or mirror any part of the Platform or content, other than framing on the Customer's own intranets or otherwise for the Customer's own internal business purposes or as permitted,
 - viii. access the Platform or content in order to build a competitive product or service or to benchmark with a non the Platform product or service, or

- ix. reverse engineer the Platform (to the extent such restriction is permitted by law).

5. Infrastructure

Clause 5.6(b)

Is the As a Service to be provided on public infrastructure?

- Yes
 No

Is the As a Service to be provided on private infrastructure?

- Yes
 No

Is the As a Service (including any Customer Data) to be hosted by a third party?

- Yes

If yes, insert name of the third party who will host the As a Service : Amazon Web Services (AWS)

- No

Specify the minimum standard for Infrastructure

The minimum standard for infrastructure must be sufficient to enable the Supplier to deliver the As a Service to comply with the availability, performance and operability standards set out in this Contract.

6. As a Service Location

Clause 5.6(d)

Will the Supplier store, host or process any Customer Data?

- Yes

If yes, complete the details set out below in this item.

- No

As a Service Location

Can the Customer select the As a Service Location?

- Yes

- No

If no, specify the As a Service Location: Sydney, Australia.

7. Customer Data

Clause 5.6(e)

Requirements for storage and back-up of the Customer Data

Is the Supplier required to provide storage and back-up of Customer Data?

Yes

If yes, specify the procedures and requirements for the storage and back-up of the Customer Data (including the frequency at which the Supplier is to provide the Customer with back-up copies of the Customer Data and the format in which the Customer Data must be provided to the Customer):

The Supplier is required to back up Customer Data daily and weekly for the purposes of maintaining the integrity and currency of the Customer Data and to enable restoration of the Platform.

No

Tools and mechanisms to enable the Customer to access and monitor the Customer Data

The Customer may access and monitor the Customer Data using the Faethm Platform.

Requirements for return or extraction of the Customer Data on expiry or termination of the Subscription Period

Is the Supplier required to return or allow the Customer to extract all Customer Data to the Customer?

The Supplier is required to return all Customer Data to the Customer on expiry or termination of the Subscription Period.

OR

The Supplier is required to allow the Customer to access the As a Service in order to extract the Customer Data.

The Supplier will provide the Customer with access to the As a Service in order for the Customer to extract the Customer Data for a period of 30 days after expiry or termination (and non-renewal).

Format in which the Customer Data must be returned or made available after termination or expiry (and non-renewal) of Subscription Period

- Comma Separated Value (.CSV); or
- Microsoft Excel (.XLS)

8. Security

Clause 5.6(f)

Specify the applicable security and encryption standards which apply to the As a Service and Customer Data

The Supplier warrants that the security and encryption standards detailed in its response to the DPC questionnaire for As-a-Service+Cloud-Vendor dated 19 June 2019 and the Software & Infrastructure Architecture Document (FAETHM-001) current as at 18 March 2019 are the minimum security and encryption standards that will apply to the As a Service and Customer Data for the Contract Term.

9. General Support

Clause 5.6(g)

- Service help desk available 8:30am to 5:30pm, Monday to Friday AEST.

The Supplier will provide the following support services to the Customer under this Customer Contract:

- operation of and access to a help desk during the Support Hours. The help desk functions are the single contact-point for the Customer's Incidents. Its first function is always to document ("create") an incident. If there is a direct solution, it attempts to resolve the Incident at the first level. If the service desk cannot solve the incident then it is passed to the 2nd/3rd level group within the incident management system;
- provision of regular Updates of the supported Software as a Service;
- provision of documentation accompanying all Updates which will be provided in advance to allow the Customer sufficient time to plan for implementation;
- provision of patches to rectify Incidents;
- maintenance of the accessibility, usability and security of the Software as a Service and the Customer Data;
- participation in review meetings with the Customer as required by the Customer to review the Supplier's performance of the support services;
- provision of monthly reports, including details of an outstanding issues concerning the provision of the support services;
- provision of minor assistance to all users of the Software as a Service;
- Incident logging on a 24x7x365 basis;
- Incident allocation;
- Incident action;
- Incident progression;
- Incident update;
- Incident management;
- Incident resolution or rectification;
- phone call and email forwarding;
- Incident request completion;
- technical escalation;
- daily and weekly backups of the Customer Data;
- ongoing business continuity and disaster recovery services; and
- continuous performance management, monitoring and administration of the Software as a Service.

The Customer may report incidents regarding the Software as a Service to the Supplier's help desk as follows:

- by website or email on a 24x7x365 basis.
- By telephone from 8:30am to 5:30pm, Monday to Friday AEST.

The contact details for the Supplier's help desk are as follows:

- email support: support@Faethm.ai

The Supplier may change the contact details of the Help Desk from time to time by notice to the Customer.

For the purposes of this Contract:

- "Incidents" includes any Defect, fault, error or other issue which adversely impacts the Customer's access to or use of the Software as a Service or the operation, performance and availability of the Software as a Service;
- "Support Hours" means the hours between 8:30am and 5:30pm on a day other than a Saturday, Sunday or a day that is a New South Wales statutory public holiday.

The Customer must provide the Supplier with the following details when notifying the Supplier of any Incident for resolution by the Supplier:

- the Customer's designated "client number";
- the name and telephone number of the Customer's nominated contact regarding the Incident;
- the Customer's assigned priority level for the Incident; and
- a full description of the Incident.

The Supplier acknowledges that Incidents may be notified to the Supplier by all users of the Software as a Service.

The Supplier will respond to each Incident notified by the Customer by:

- carrying out authorisation checks;
- allocating an Incident log number and advising the Customer of that number;
- providing initial advice by telephone, including advice as to any actions and checks to be carried out by the Customer to:
 - resolve the Incident; or
 - clarify the nature of the Incident to enable the Supplier to resolve the Incident; and
- referring the resolution of the Incident to the appropriate department within the Supplier for resolution in accordance with the service levels.

Workarounds

The Supplier may, before the response times and/or resolution times have expired, take such measures as are appropriate in all the circumstances, including the provision of a Workaround solution to enable the Customer to continue to productively use the Software as a Service until the reported Incident has been resolved by the Supplier to the satisfaction of the Customer.

Warranty

The Supplier warrants that any Incident notified to the Supplier by the Customer during the Contract Term will be rectified by the Supplier.

10. Service Levels

Clause 5.6(j)

Software as a Service Availability Rates

The Software as a Service must be available for access and use by the Customer over the internet in a state which meets the Customer's Requirements and Specifications at least 99% of the time as determined on a 24x7x365 basis.

The availability of the Software as a Service will be measured as follows:

Software as a Service availability = $(\text{Time Interval} - \text{Outage Time}) / \text{Time Interval} \times 100$

Where:

- Time Interval = Monthly;
- Outage Time = All periods of unavailability, excluding scheduled maintenance and emergency maintenance; and
- Available = All of the features and functionality of the Software as a Service are available to the Customer's users in a live production environment.

The availability of the Software as a Service will be calculated on a monthly basis commencing on the first day of each month.

If, during any rolling six (6) month period during the Contract Term, the Supplier fails to meet the system availability rate on three (3) or more occasions, then such failure will be deemed to be a

breach of this Contract the Customer will be entitled to issue the Supplier with a notice to remedy the breach in accordance with Clause 21.1 (a).

Software as a Service Response Times

The Supplier must promptly investigate any issues with the response and processing times of the Software as a Service notified to the Supplier by the Customer during the Contract Term and must promptly resolve any such issues where the resolution of such issues is within the reasonable control of the Supplier.

Support Services – Service Levels

The Supplier must ensure that the support services meet the following response and resolution times when the Supplier is notified of an Incident in the supported Software as a Service.

	Priority 1 Critical	Priority 2 Major	Priority 3 Minor	Priority 4 Non-essential
Priority Level – Definition	<ul style="list-style-type: none"> Software as a Service down or totally unavailable Serious impact on the Customer's use of the Software as a Service Prevents the timely and accurate use of the Software as a Service Occurs during a critical processing window 	<ul style="list-style-type: none"> Impacts the Customer's use of the Software as a Service No suitable workaround is available Customer cannot utilise the basic functionality of the Software as a Service and is impacting critical services 	<ul style="list-style-type: none"> Most functions of the Software as a Service are available to the Customer Low impact on the Customer's use of the Software as a Service 	<ul style="list-style-type: none"> Incidents that do not require immediate action Little or no impact on the Customer's use of the Software as a Service Examples: suggestions for enhancements to the Software as a Service; notification of documentation errors
Response Time	During business hours: Two (2) hrs Outside of business hours: Within two (2) hours of the start of the next business day	During business hours: 4 hrs Outside of business hours: Within four (4) hours of the start of the next business day	During business hours: 16 hrs Outside of business hours: Within 16 hours of the start of the next business day	During business hours: 72 hrs Outside of business hours: Within 72 hours of the start of the next business day
Resolution Time	Eight Working Hours	24 Working Hours	72 Working Hours or as agreed	Within a reasonable timeframe based on the Supplier's best endeavours

				to resolve the Incident
Frequency of Updates during Resolution Period	2 Hours	Every 12 hours	Every 24 hours or as agreed	Weekly or as agreed

For the purposes of this Contract:

- “Incident” has the meaning specified in item 9 of section 3 of these Contract Details;
- “Support Hours” has the meaning specified in item 9 of section 3 of these Contract Details;
- “Working Hour” means an hour within the Support Hours; and
- “Working Minute” means a minute within the Support Hours.

The Customer is responsible for assigning the Priority Level of each Incident at the time when the Incident is notified by the Customer to the Supplier. Any dispute regarding the Priority Level assigned by the Customer will be referred to the Escalation Procedures in this Contract. Until the dispute is resolved, the Supplier must deal with the Incident in accordance with the Customer’s assigned Priority Level for that Incident.

The Response is an acknowledgement by the Supplier of receipt of the notification of the Incident from the Customer and will be provided by the Supplier to the Customer by email and telephone.

The Update is an update by the Supplier regarding the resolution of the Incident, including a summary of what actions the Supplier has undertaken to attempt to resolve the Incident, and will be provided by the Supplier to the Customer by email and telephone.

The Response Time will be measured from the time when the Customer notifies the Supplier of the Incident, as recorded by the Customer, to the time when the Customer receives a response from the Supplier.

The Resolution Time will be measured from the time when the Customer notifies the Supplier of the Incident, as recorded by the Customer, to the time when the Supplier has resolved the Incident or provided an alternative workaround and the Customer has provided written confirmation to the Supplier of the Customer’s acceptance of the resolution or alternative workaround.

For the purposes of this Customer Contract, an Incident will not be classified as “resolved” unless and until the Customer has provided written confirmation to the Supplier of the Customer’s acceptance of the resolution or alternative workaround provided by the Supplier.

If, during any rolling six (6) month period during the Contract Term, the Supplier fails to meet the minimum Response Time for priority 1 and/or Resolution Time on (3) or more occasions, then such failure will be deemed to be a breach of this Contract the Customer will be entitled to issue the Supplier with a notice to remedy the breach in accordance with Clause 21.1 (a).

Support Services – Incident Logging

The Supplier must maintain a complete, accurate and up-to-date Incident Log for the duration of the Contract Term including the relevant details of all reported Incidents.

The format of the Incident Log must substantially comply with the following table:

Incident	Identification Number	Priority level	Tracking Number for Incident	Date Incident Notified by the Customer	Date Incident Successfully Resolved by the Supplier

The Supplier must, upon receipt of a request from the Customer, provide the Customer with a copy of the Incident Log.

Reporting

- The Supplier is required to measure its performance against the Service Levels and provide a report to the Customer.

The Supplier must report on its performance against the Service Levels every 3 months during the Contract Term if requested.

Exclusions from Service Levels

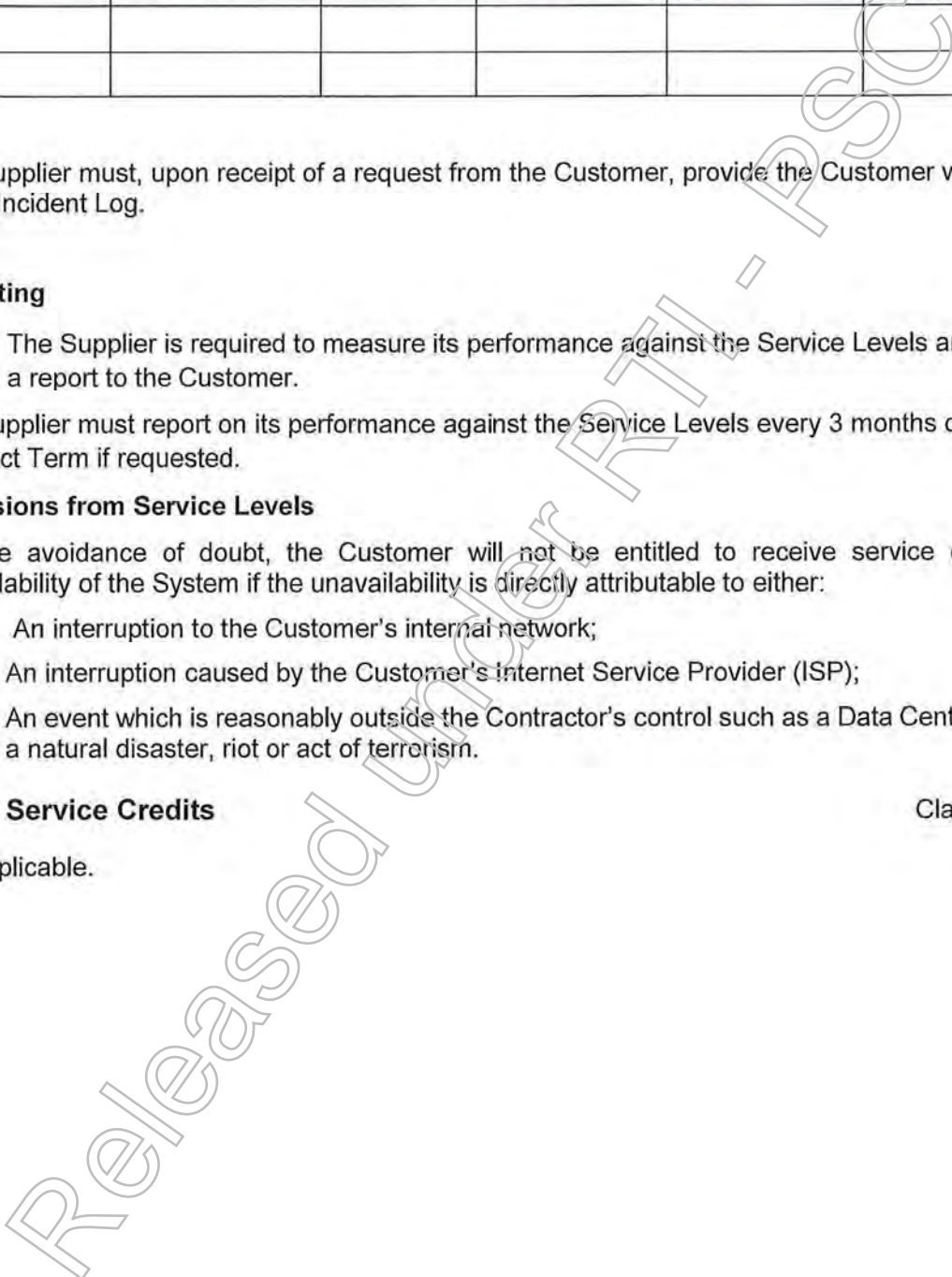
For the avoidance of doubt, the Customer will not be entitled to receive service credits for unavailability of the System if the unavailability is directly attributable to either:

- a) An interruption to the Customer's internal network;
- b) An interruption caused by the Customer's Internet Service Provider (ISP);
- c) An event which is reasonably outside the Contractor's control such as a Data Centre outage, a natural disaster, riot or act of terrorism.

11. Service Credits

Clause 5.6(k)

Not applicable.



3. ICT Professional Services

The following Details to be completed if the Customer is procuring ICT Professional Services (refer clause 5.7 of the General Contract Conditions).

1. ICT Professional Services

Description of ICT Professional Services

The supplier will provide strategic consulting services that include but are not limited to:

- Advanced Onboarding and strategic Consulting including:
 - Initial data mapping of role names
 - 45 minute remote introductory meeting with Customer Success Manager to discuss business goals, onboarding process, workforce data and questions via the Zoom online meeting platform.
 - 3x 60-minute remote Platform & insights training sessions with the Supplier's Customer Success Manager via the Zoom online meeting platform
 - Quarterly workforce data refresh/uploads
 - Up to 8 additional workforce data uploads
 - Product documentation.
- 8 days of professional consulting services (blended rate across Executive Director 10%, Director 50% & Senior Consultant 40%), to be used as required. Options include:
 - Data interpretation and PMO advice
 - Attendance of steering committee meetings
 - Presentation to executives
- Up to 15 Customer specific custom roles created in the "Job Neighbourhood"

Deliverables

Specific deliverables in relation to the provision of ICT professional services will be agreed in writing between the Customer and the Supplier from time to time during the Service Period.

2. Service Period

Clause 5.7(a)

Start of Service Period

The Service Period will commence on the Contract start date.

End of Service Period

Until the ICT Professional Services have been fully performed by the Supplier in accordance with the Contract.

3. Delivery Date

Clause 5.7(b)(ii)

Specify any Delivery Date(s) applicable to the ICT Professional Services

The Customer and the Supplier will agree on specific Delivery dates applicable to the ICT professional Services from time to time during the Service Period.

Specify the hours and days during which the Supplier must provide the ICT Professional Services

The ICT Professional Services will be provided during Business Hours unless otherwise agreed.

4. Professional standards

Clause 5.7(b)(iii)

Specify any professional standards which apply to the performance of the ICT Professional Services

Nil.

5. Notification Period

Clause 5.7(e)(ii)

The default notification period of 30 days applies.

6. Warranty Period

30 Days from the AAD of any deliverable.

Released under RTI - PSC

4. Forming the Contract

1. Acknowledgements and certifications

The Supplier:

- (a) agrees to provide the Products, Services and other Deliverables to the Customer on the terms described in the Contract.
- (b) certifies that it has read, understands, and complies with all the requirements of the Contract.
- (c) represents that all the information provided by it and referenced in the Contract is complete, accurate, up to date and not misleading in any way.
- (d) acknowledges that the Customer is relying on the information provided by the Supplier and referenced in the Contract in entering into the Contract.
- (e) acknowledges that the Customer may suffer damage if any of that information is incomplete, inaccurate, out of date or misleading in any way.

Released under RTI/PSA

5. Agreement

1. Agreement by Supplier

The Supplier will sign in this section. By signing, the Supplier is offering to enter the Contract on the terms set out in this document. If the Supplier does not execute this document itself, it must (if the Customer requests) provide adequate evidence that the signatory is properly authorised to execute this agreement.

If the parties agree any changes to this document after the date of the Supplier's signature (but before the Customer accepts the Supplier's offer as described below), the Supplier and Customer will prepare a new version of the document incorporating the agreed changes, which will replace this document. The Supplier will sign the new document, offering to enter the Contract on the amended terms.

Date
24 August 2019

EXECUTED for and on behalf of:)

Faethm Pty Limited)

Name of Supplier)

by its Authorised Representative, in)

the presence of:)

Signature of witness)

Carolyn Colley)

Name of witness (block letters))

Signature of Authorised Representative)

By executing this agreement the signatory warrants)

that the signatory is duly authorised to execute this)

agreement on behalf of the Supplier)

Greg Miller)

Name of Authorised Representative (block letters))

Executive Director)

Position of Authorised Representative)

2. Agreement by Customer

Date 26/8/19

EXECUTED for and on behalf of:)

Public Service Commission)

Name of Customer)

by its Authorised Representative, in)

the presence of:)

Signature of witness)

NIKOLA J. NEHRING)

Name of witness (block letters))

Signature of Authorised Representative)

By executing this agreement the signatory warrants)

that the signatory is duly authorised to execute this)

agreement on behalf of the Customer)

MEGAN BARRY)

Name of Authorised Representative (block letters))

DEPUTY COMMISSIONER)

Position of Authorised Representative)

Schedule 1 – Price and Payment Terms

1.1 Price

Description	Unit Price	GST component	Total Price (including GST)
12 Month subscription for the Faethm platform As a Service			
Strategic Consulting Services			
Total			\$73,150

1.2 Expenses

Nil.

1.3 Price reviews (including during any extension period(s))

Not applicable.

1.4 Payment plan/milestones

The Supplier may invoice the Customer after successful achievement of the milestones as follows:

- For the As a Service subscription: annually in advance.
- For the provision of ICT Professional Services:
 - 25% upon contract execution and
 - 75% upon completion.

All invoices are payable within 30 days of receipt.

1.5 Rates for additional Products and Services (if applicable)

Not applicable.

1.6 Payment methods

The Customer will pay via Electronic Funds Transfer. The Supplier must include banking details with its invoices.

1.7 Discounts or rebates

Not applicable.

1.8 Address details for invoice

Invoices are to be submitted by email to pscadmin@psc.qld.gov.au.

1.9 Other pricing information

The subscription pricing above is for a data set of up to 2,303 employees for the ^{Agency 1} [redacted] and ^{Agency 2} [redacted].

Sarah Partosh

From: Megan Barry
Sent: Tuesday, 14 May 2019 5:20 PM
To: Sandra Lerch; Nikolai Nehring
Cc: Clifford Paterson
Subject: FW: Procurement query for engagement of Faethm
Attachments: Faethm PSC Procurement Exemption Form 01.docx; Faethm Procurement - Risk Assessment.XLSX

Follow Up Flag: Follow up
Flag Status: Flagged



Approved – please let Cliff know if you need an electronic signature.

Megan Barry
Acting Deputy Commissioner
Public Service Commission

P 07 3003 2829 M [REDACTED]
E megan.barry@psc.qld.gov.au W psc.qld.gov.au
Level 27, 1 William Street, Brisbane QLD 4000

From: Sandra Lerch <Sandra.Lerch@psc.qld.gov.au>
Sent: Monday, 6 May 2019 3:23 PM
To: Megan Barry <megan.barry@psc.qld.gov.au>
Cc: Nikolai Nehring <Nikolai.Nehring@psc.qld.gov.au>; Jenny Stephensen <Jenny.Stephensen@psc.qld.gov.au>
Subject: FW: Procurement query for engagement of Faethm

Hi Megan

Attached for your approval are two documents to support the engagement of Faethm:

- Risk assessment
- Procurement exemption form (for authorisation to obtain only one quote).

I have made minor changes to the exemption form prepared by Jenny (originally emailed to you on 26/4), which now includes a reference to the foundational work completed by Data61.

For your consideration and approval.

Kind regards
Sandra



Sandra Lerch
Acting Executive Director
Workforce Futures and Inclusion
Public Service Commission

P 07 3003 2711 M [REDACTED]
E Sandra.Lerch@psc.qld.gov.au W psc.qld.gov.au
Level 27, 1 William Street, Brisbane QLD 4000

From: Nikolai Nehring <Nikolai.Nehring@psc.qld.gov.au>

Sent: Thursday, 18 April 2019 9:47 AM

To: Jenny Stephensen <Jenny.Stephensen@psc.qld.gov.au>

Cc: Sandra Lerch <Sandra.Lerch@psc.qld.gov.au>; Natalie Driscoll <Natalie.Driscoll@psc.qld.gov.au>; Adam Stein <Adam.Stein@premiers.qld.gov.au>; Leigh Wilmot <Leigh.Wilmot@premiers.qld.gov.au>; Julie Dainty <Julie.Dainty@psc.qld.gov.au>

Subject: RE: Procurement query for engagement of Faethm

Hi Jenny,

I have provided some advice below separated into the different parts of the process.

Information technology considerations

- As you are buying access to software this will need to be treated as an IT purchase.
- To cover off the risks associated with procuring technology services, you will need to ask the supplier to complete the attached technology and security questionnaire and then seek advice on the responses from Adam Stein and/or Leigh Wilmot from the DPC IT team.
- Adam and Leigh will be looking to ensure that the technology is secure (strength of passwords required, multifactor authentication, underlying technology architecture etc) and the treatment of data complies with information management and information privacy requirements (where the data is stored, how is it handled, does the supplier retain a copy etc). The responses to the technology questionnaire will also provide some of the information we will need for the contract.
- As part of the IT assessment the supplier may need to provide copies of penetration test reports to DPC IT, or DPC IT may need to engage a third party to undertake a penetration test of the system (which would carry an additional cost).

Please note that not all sections of the questionnaire will be relevant for this specific purchase so please ask the supplier to only complete the sections that are relevant to their product/ service offering.

Procurement

- Complete the attached risk assessment template; and
- As our procurement policy requires at least 3 quotes for any purchase over \$50,000 (including GST), you will need to complete the attached procurement exemption form outlining the reasons for not seeking 3 quotes and have it approved by Megan along with overarching approval to engage the supplier and total contract value/expenditure. Please include the name of the supplier somewhere in the 'reason for exemption' section of the form.
- Your contract number for this purchase is PSC-04-2019.

Contracting

- Based on the value of the contract and type of services, I would recommend using the standard Queensland Government General Contract Conditions for ICT products and services (attached) and the corresponding ICT contract details (attached for information only).
- Once you get to this stage I can assist with completing the contract; however, I would recommend that you send the terms and conditions to the supplier to review, advising them that if we proceed with the engagement, these are the terms and conditions that will govern the contract.
- Do you have a proposal or quote that you can send me to review and to inform the contract development? Depending on the level of detail we have already, we may need to seek additional information from Faethm to complete the contract details.



Please let me know if you would like to catch up to discuss any of this in more detail.

Kind regards

Nikolai

Nikolai Nehring

Senior Advisor, Governance and Procurement
Governance and Business Services
Public Service Commission

P Tue-Thurs 07 3003 2843

P Mon & Fri 07 3003 9177

E nikolai.nehring@psc.qld.gov.au W psc.qld.gov.au

Level 27, 1 William Street, Brisbane QLD 4000

The different faces of impairment
– building an inclusive and diverse workforce

www.forgov.qld.gov.au/people-impairment



From: Jenny Stephensen <Jenny.Stephensen@psc.qld.gov.au>

Sent: Wednesday, 17 April 2019 11:47 AM

To: Nikolai Nehring <Nikolai.Nehring@psc.qld.gov.au>

Cc: Sandra Lerch <Sandra.Lerch@psc.qld.gov.au>

Subject: Procurement query for engagement of Faethm

Hi Nikolai

Welcome back!

We are in the final stages of firming up a pilot project to Faethm to use their proprietary tools to better understand the impact of automation at the occupational level.

Could you let us know what approvals are needed to enter into an agreement with them as a sole provider without going to market and what the process is from here? It will be for around \$75K.

Many thanks

Jenny Stephensen
Workforce Futures and Inclusion
Public Service Commission

P 07 3003 2897 M [REDACTED]

E jenny.stephensen@psc.qld.gov.au W psc.qld.gov.au

Level 27, 1 William Street, Brisbane QLD 4000

I work flexibly. A response is not expected outside of your work hours.

Released under RTI - PSC

Exemption from procurement process

This form must be completed for every proposed exemption from standard procurement procedure, and returned to Governance and Business Services

BUSINESS UNIT	Workforce Futures and Inclusion
---------------	---------------------------------

RFQ/ITO/SOA NUMBER	Contract number PSC-04-2019
TITLE OF PROJECT	Faethm: Predictive analytics for emerging technology and the future of work
PROJECT MANAGER	Sandra Lerch
SUMMARY DESCRIPTION OF PROJECT	Understanding the impact of automation on the Queensland public sector at the occupational level.
ESTIMATED VALUE	\$75,000

EXEMPTION BEING SOUGHT (check all that apply)	
Exemption from competitive process (e.g. sole supplier, limited supply)	<input checked="" type="checkbox"/>
Exemption from seeking quotes from Queensland based suppliers (only to be used where there are not Queensland based suppliers offering the required goods or services)	<input checked="" type="checkbox"/>
Exemption from Queensland Information Technology Contracting (QITC) requirements (approval to use supplier terms and conditions)	<input type="checkbox"/>
Genuine urgency	<input type="checkbox"/>
REASON FOR EXEMPTION	
Faethm combines public and client data with their unique proprietary analytics and machine learning.	



BACKGROUND	<p>Faethm's product delivers insights to leaders of government. The Platform underpins scenario planning and delivers predictions and commercial information that are specific to the Queensland economy, industry, geography, business unit, team, role or individual.</p> <p>The proposed pilot will build on the research work recently completed by CSIRO Data61, that analysed the trends, challenges and opportunities associated with the impact of automation in the Queensland public sector. Faethm's product will provide a more granular analysis of impacts at the occupational level, and identify potential 'job corridors' for occupations that may be affected by automation in the future.</p>
------------	--

CONSULTATION	<p>NSW Public Service Commission undertook a similar pilot with Faethm in late 2018 between NSW PSC, Treasury, Premier and Cabinet and Transport. Feedback from their pilot was positive to the extent that Faethm has now been engaged for a further 12 months with all but one NSW Government Department as they develop strategic workforce planning scenarios to respond to work of the future impacts on the sector. We continue to consult with NSW to understand impacts and lessons.</p>
--------------	--

PROCESS TO BE UNDERTAKEN	<p>Once Faethm have been engaged a four week pilot will commence with three Queensland Government agencies (likely Agency 2, Agency 1 and Queensland Police) to test the viability of the product.</p>
--------------------------	--

Approved / Not Approved / Noted

Megan Barry
Deputy Commissioner
 23 April 2019

(Please use electronic signature to reduce the need for printing. This section may also be deleted if email approval is attached)

Released under RTIPSC

PROCUREMENT RISK ASSE

Question	Answer
Is this procurement recurring or a one-off?	One-off
Will the goods/services be sourced off a Standing Offer Arrangement?	No
Is the spend over \$250,000 (including GST)?	No
Does the procurement have an IT component?	Yes, the procurement has an IT component (e.g. a digital platform, application or IT system)
If procuring a consultant, will they require access to confidential/Cabinet-in-confidence documents?	No
Are the goods/services critical to the department and/or its core operations?	No, the goods/services will have a minor effect on the department's core operations (e.g. back-office functions)
If the supplier defaults, will there be a significant disruption to the department due to engaging an alternative supplier?	No, there would be an insignificant disruption to the department and an alternative supplier would not be immediately required
What is the financial risk to the department if the supplier defaults?	Insignificant - a small financial loss that can be absorbed
What is the risk to people (e.g. health, welfare, safety) if the supplier defaults?	Insignificant - injury not requiring treatment
What is the reputational/social/media risk to the department if the supplier defaults?	Minor - limited damage to reputation
Have any risks (unique to the supplier) been identified that need to be managed? (e.g. past performance issues, financial viability, start-up company, previous disputes, difficult dealings with supplier, issues raised in contract negotiations)? How would you classify the supplier risk?	Minor - a small unique supplier risk has been identified
What is the department's risk for exposure to litigation?	Insignificant potential of exposure to litigation

Extreme	CONTACT PROCUREMENT SERVICES – Risks with a residual rating unacceptable and must be treated except where the department allows this level of tolerance.
High	CONTACT PROCUREMENT SERVICES – Risks with a residual rating generally unacceptable without further treatment depending on the specific activity and objective.
Moderate	CONTACT PROCUREMENT SERVICES – Risks assessed with a residual rating MODERATE may be accepted without further treatment but must be managed. These risks will be managed as 'business as usual' by business units. These risks will be monitored by executive management
Low	

	Insignificant	Minor	Moderate	Major
Almost Certain	Moderate	Moderate	Extreme	Extreme
Likely	Low	Moderate	High	Extreme
Possible	Low	Moderate	High	High
Unlikely	Low	Low	Moderate	High
Rare	Low	Low	Moderate	Moderate



FAETHM

Platform Architecture

Version 2.0

Released under RTIPSC

Table of Contents

1. Introduction.....	4
2. Platform Architecture.....	5
2.1 Presentation.....	5
2.2 App Server.....	6
2.3 Data Persistence.....	6
2.4 Third Party API Integration.....	6
3. Platform Infrastructure.....	6
3.1 Application Server.....	6
4.2 Database.....	6
4.3 Non-database file storage.....	6
4.4 Scale.....	7
4.5 Backup and Restoration.....	7
4.6 Disaster Recovery.....	7
4. Client Requirements.....	8
5. Security.....	9
5.1 Physical Security.....	9
5.2 Network security.....	9
5.3 Monitoring.....	9
5.4 Application Security.....	9
5.5 Data Encryption and Storage.....	9
5.6 Application Accessibility.....	9
5.7 Role-level Security.....	9
5.8 Data-level Security.....	9
5.9 Application Logging.....	10
5.10 Password Policies.....	10
5.11 Verifying our Security.....	10

Document Status Sheet

Document Title	Software & Infrastructure Architecture Document
Document Identification	FAETHM-001
Author(s)	Owen Craig, Enda Mahoney
Version	2.0
Document Status	draft / internally accepted / conditionally approved / approved

Version	Date	Author(s)	Description
1.0	13-Jun-2018	Enda J Mahoney	Initial documentation of the platform architecture
2.0	18-Mar-19	Owen Craig	Update to reflect architectural changes

Released under RTIPSC

1. Introduction

This document provides the reader with a detailed understanding of the Faethm (Faethm) platform architecture and infrastructure design.

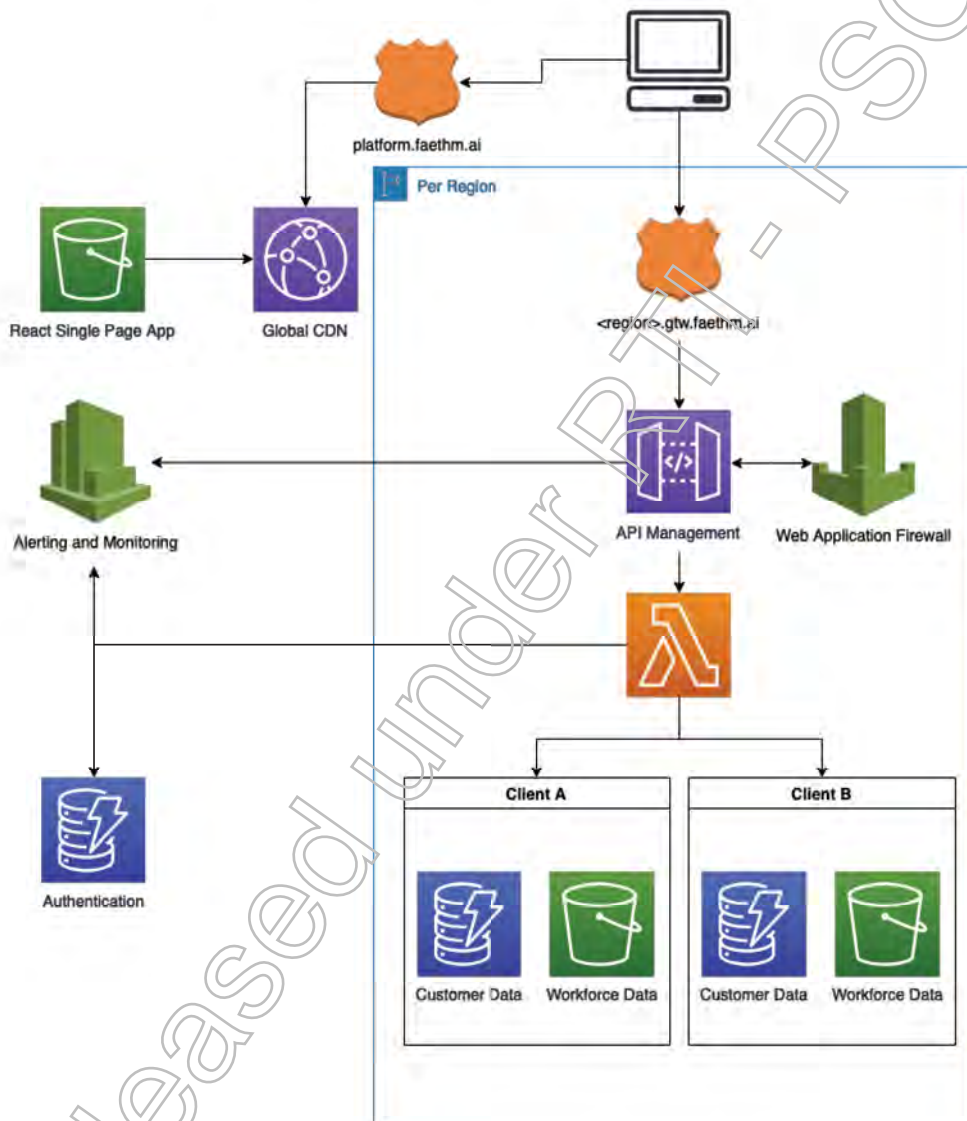
The purpose of this document is to

- 1) Provide a factual overview of the platform architecture from software to infrastructure, security, scale and release management.
- 2) To help prospects and new clients satisfy technical and security concerns when assessing the Faethm platform

Released under RTI - PSC

2. Platform Architecture

Faethm is built on a multi-region auto-scalable architecture. The front end applications are served through a globally distributed content delivery network (CDN), with the persistence and application logic hosted within a specific region per customer.



2.1 Presentation

The Presentation Tier (User Interface) leverages React, JavaScript, HTML5 and CSS3. All communications between the front-end application and the web services/APIs are secured by industry standard TLS.

2.2 App Server

The application offers a suite of public and private API's with users authenticating by JWT (JSON Web Tokens).

2.3 Data Persistence

All transactional data is persisted within AWS DynamoDB tables with data being encrypted at rest. All workforce data is persisted in region specific S3 buckets independent of other clients' data.

2.4 Third Party API Integration

The Faethm platform currently integrates with the following 3rd party APIs:

- MapQuest open search (<https://developer.mapquest.com/documentation/open/nominatim-search/>) to fetch boundary information for regions
- MapBox (<https://www.mapbox.com/>) for rendering of maps
- Rollbar (<https://rollbar.com/>) for deidentified error reporting

3. Platform Infrastructure

Faethm is hosted on Amazon Web Services (AWS). AWS provides highly reliable and scalable infrastructure to support computing power, database management, load balancing, data storage, backup and other related services.

Faethm is hosted in four regional Datacentres in Sydney - Australia, Dublin - Ireland, London - England and Ohio - USA.

3.1 Application Server

The application APIs are hosted on Amazon Lambda which provides scaling and isolation to grow with client demand. Client data that is within a specific region is served by API servers within that region, providing data sovereignty within a country from persistence through to when it reaches the client's machine.

4.2 Database

The database is served from Amazon's DynamoDB, a Platform as a service (PaaS) Key-Value and document database. Client data is stored independently in separate tables specifically for that client which are secured by application level access controls.

4.3 Non-database file storage

Non-database file storage Data that sits outside the database such as query result sets are stored on Amazon S3 storage. Like the application and database servers, data on S3 is redundantly stored

across multiple devices across multiple facilities within a region with automatic cutover in the event of any issues.

4.4 Scale

Utilising Amazon Web Services, Faethm has the ability to scale systems and services to ensure that application performance is consistent irrespective of the number of clients and users of Faethm. As system load increases additional capacity is added or removed to adjust to changing client demands.

4.5 Backup and Restoration

Standard weekly backups of the client database are stored in an AWS S3 bucket and encrypted at rest. Backups are compressed and encrypted before uploading to S3 bucket.

Databases can be restored from standard or archived backups when a complete system failure of Faethm instance occurs. Restoration from a system failure is completed by Faethm, however, clients can send a restoration request to Faethm based on their own needs (extra charges apply). Fee is outlined in the Service Level Agreement and Order Statement.

A restoration from an archive can take up to 5 hours.

4.6 Disaster Recovery

Faethm's hosting partner AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of data and infrastructure within service level agreement timeframes.

4. Client Requirements

Access to Faethm UI and API's is via web browsers. The list below provides a minimum requirement for the web browsers we support today,

- Google Chrome (Version 63)
- Mozilla Firefox (Version 57)
- Microsoft Edge (Version 41)
- Safari (Version 11)

Faethm will have the user interface optimised on the above web browsers.

Released under RTI - PSC

5. Security

Faethm has also been designed with security in mind to ensure that only authorised users have access to the service.

5.1 Physical Security

The Faethm platform is housed in the AWS datacentres where state-of-the-art electronic surveillance and multi-factor access control systems manage physical access. Datacentres are staffed 24 x 7 by trained security guards and access is restricted to authorised personnel.

5.2 Network security

Faethm leverages Amazon's extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection and password brute-force detection on AWS Accounts. Access to the AWS infrastructure that Faethm utilises is secured by Multi-Factor Authentication (MFA) as well as being network IP address locked (Application Tier and Data Persistence Tier).

5.3 Monitoring

Faethm utilises centralised account and account management to manage and monitor all registered AWS account and billings. Code changes and features updates are monitored by deployment tools. Instance monitoring is managed using AWS CloudTrail and CloudWatch.

5.4 Application Security

Faethm has been designed to ensure that only authorised users can access the information as specified by the account administrator.

5.5 Data Encryption and Storage

All data transmitted to and from the Faethm application is encrypted using industry standard HTTPS protocol. This means that the information can only be viewed by the end user's computer and the Faethm application. Data encryption algorithms such as SHA512 are implemented for some sensitive data. For instance, end user's login password is hashed using the bcrypt algorithm with an added salt and finally saved in database in format of encrypted characters. Data is never stored on an end-user's computer, and all data is encrypted at rest. All data remains within the Faethm datacentre and only the data that is actively in use by a user is displayed in the web browser.

5.6 Application Accessibility

Only users that have been approved by the client's account administrator are able to access your Faethm account and data therein. This may include third parties if the licence arrangement allows and Faethm whose access must be specifically approved and controlled by the client.

5.7 Role-level Security

Faethm provides control over who can access information, perform actions, access files or produce reports. Access to some screens, action, report, look up or enquiry can be defined within a security role that is configurable. Users can be assigned to one or more roles.

5.8 Data-level Security

In addition to role-level security, Faethm provides capabilities to control API access at the data via organisational id's.

5.9 Application Logging

All access to Faethm is audited so you have the confidence of knowing who accessed your account and when that was.

5.10 Password Policies

Faethm supports NIST Digital Identity Guidelines to standardise and enforce password standards within the platform. In order to assist in keeping the system secure, Faethm highly recommends that usernames and/or passwords are not shared in any way with persons other than the one who has been assigned that login.

5.11 Verifying our Security

We know that security is highly important to our clients and as such we engage a range of external, 3rd party security consulting organisations to audit our systems and processes to rigorously ensure that your data is safe. We use a partner firm Indusface to perform architectural security reviews, penetration security tests and code analysis testing to ensure data security is at the highest level.

Released under RTIPSC

Vendor Technology and Security Questionnaire for As-A-Service and Cloud Services

Document Owner	Corporate and Government Services, Information Services
TRIM Reference	
Issue Date	October 2017
Review Date	October 2018
Related documents	Information Standard IS18 – Information Security Information Security Policy
Classification	Security-in-confidence

Released under RTI - PSS

Table of Contents

X-AS-A-SERVICE AND CLOUD QUESTIONNAIRE.....	3
TECHNOLOGY.....	3
1. Overview of Solution Architecture	3
2. Data Storage	4
3. Client Environment.....	5
4. Network	6
5. Integration Interfaces.....	6
6. Service Hosting Environment.....	7
7. Reporting	9
8. Change Management	9
9. System Support	10
10. Transition Out.....	11
11. Other Strategic Considerations.....	12
SECURITY CONTROLS QUESTIONNAIRE	13
SECURITY CONTROLS.....	13
1. Information Asset Management.....	13
2. Internet-facing systems, encryption and cryptographic ciphers.....	13
3. Human Resource Management.....	14
4. Security and operations management	14
5. Access management.....	16
6. Information security incident management	17
7. Backup and Disaster recovery.....	17
8. Compliance	18

Instructions for completion

Most questions are designed to be a simple yes or no with optional comments in the “Click here to enter text box” For example,

Yes No. If yes, describe access requirement – Enter the information here.

X-AS-A-SERVICE AND CLOUD QUESTIONNAIRE

TECHNOLOGY		
1. Overview of Solution Architecture		
1.1	Specify the name of the Solution being offered, including version number (if applicable).	Faethm Platform
1.2	Does your Solution deployment model use public, private, community or hybrid cloud for delivery to the Customer?	<input checked="" type="checkbox"/> public <input type="checkbox"/> private <input type="checkbox"/> community <input type="checkbox"/> hybrid cloud
1.3	Is your Solution being offered as SaaS, PaaS, or IaaS?	<input checked="" type="checkbox"/> SaaS <input type="checkbox"/> PaaS <input type="checkbox"/> IaaS <input type="checkbox"/> DaaS
1.4	Please provide a very brief description of the Solution architecture of the proposed system, or attach relevant information.	The Faethm Platform is a SaaS Platform which is hosted in Amazon Web Services in Sydney.
1.5	Include any diagrams to provide a visual overview of the proposed service offering. (ATTACH).	Architecture document attached.
1.6	How many Customer utilise this version of the system?	54
1.7	How long has the offered version above been in production usage?	Jan 2019
1.8	Can customisations be made to the Solution by the Customer? If yes, describe the extent of customisation available, and the effect on future maintainability:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No The Platform does not require customisation.
1.9	Is source code and other installation / configuration files located at the cloud service hosting site available to the Customer on request? If yes, how does the vendor manage these items?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Platform and Content including, but not limited to, statistics, metrics, information relating to best practices, research, question sets, taxonomy, templates, text, photographs, illustrations, audio clips, video clips, artwork, graphic material, or other copyrightable elements, the selection and arrangements thereof, and trademarks, service marks, trade names and any other intellectual property related to the Platform and Content is our property and is protected, without limitation, pursuant to copyright and trademark laws.

1.10	<p>Are there any software dependencies inherent in the Solution that may require purchase or lease of another supplier's software?</p> <p>If yes, please detail:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>There are no dependencies on any other providers software</p>
1.11	<p>Are there any different modes of operation i.e. interactive real-time integration, access to portal, off-line, batch etc.</p> <p>If yes, please detail:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>The Platform is available real time.</p>
1.12	<p>Is an on-premise version of the Solution available?</p> <p>If yes, please detail:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>The platform is hosted in AWS in Sydney.</p>
1.13	<p>Is the customer able to run a paid proof of concept for a period of not less than 3 months without purchasing ongoing licencing/Solution?</p> <p>If yes, please detail:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
2. Data Storage		
2.1	<p>Where (geographic locations) and in what format are the data records and attached files being stored?</p>	<p>Amazon Web Services in Sydney</p>
2.2	<p>Detail any Database Management Systems (name and version number) used.</p>	<p>n/a</p>
2.3	<p>Are there any limitations to the amount of data capable of being stored in the Solution in various formats?</p> <p>If yes, describe the nature of these formats.</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>The Platform does not have any limitation our largest client data set is 10M rows.</p>
2.4	<p>Can the amount of storage be grown on-demand in a flexible automated manner?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Amount of data storage is unlimited</p>
2.5	<p>Is data encrypted in transit, during processing and/or at rest?</p> <p>If yes, describe how:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using Cryptographic controls. https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanism All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B.. All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated</p>

		hardware security modules.
3. Client Environment		
3.1	What user/client interactive interfaces are available for users to access the system functionality? Please include all workstation and mobile client interfaces (Apple IOS, Android, Windows Phone) on any types of devices.	The faethm Platform is accessible via the internet and our secure web front end and is mobile responsive but best operated on a PC or Mac.
3.2	Do the workstations in the Solution perform any processing functions beyond a thin browser interface? If yes, describe the nature and extent of these processing functions.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Click here to enter text.
3.3	Will the client software components function in the customer managed operating environment (MOE), which contains (but is not limited to) common software products such as:	Windows 10. <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If not, state version supported: Internet Explorer 11- <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No. If not, state version supported. Microsoft Edge, Google Chrome, Firefox and Safari Office 2016 - <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If not, state version supported: Adobe Reader DC - <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If not, state version supported: Microsoft System Centre Endpoint Protection - <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If not, state version supported: Microsoft SCCM (Deployment and Monitoring Tool) - <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If not, state version supported:
3.4	Does the Solution require additional software or configuration settings to be installed on the client machine? If so, list the software including version numbers:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None Required
3.5	Are there any minimum hardware requirements on desktop? If so, identify Clock speed (GHz) Memory (GB) Hard-disk space required by the application (KB, MB or GB)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None required
3.6	Are there any other specific additional hardware requirements e.g. any peripheral devices required, specific screen requirements etc. If so, list:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None required
3.7	Does the Solution support multiple barcode formats and types of OCR devices, such as light pens and laser scanners?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No n/a

	If so, list:	
3.8	Can the application be run remotely using Citrix or Windows Terminal Services software to access a client running in a remote workstation?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Not required
3.9	Is the Customer required to install any components within the Customer's internal client environment? If yes, describe the degree of complexity involved in installing the application client environment. Identify if an install file is used (e.g. msi) and what the install file actually installs?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No No none required
3.10	Is there an administrative interface available for customer's staff to administer/ fully manage the configuration of the Solution? If no, detail the limitations of the administrative interface:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None required
3.11	Does any feature available in the proposed cloud service require installing an infrastructure component in the client local network environment in order to take advantage of the functionality (such as background email processing, bandwidth compression or other)? If yes, describe:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None required
4. Network		
4.1	Is there a minimum communications links' bandwidth requirement; both recommended speed for optimum performance, and minimum requirement? If yes, describe:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None required
4.2	Is there implications for the customer fire wall ie. is there a need to open ports for traffic? If yes, describe which ports are open in the firewall in the service end?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None required
5. Integration Interfaces		
5.1	Are there any interfaces available for other systems to interact with this system? If yes, describe web services, API, file transfer, ODBC etc. include all means available to interact with the data either at presentation, business or data layer integration level.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No None Required
5.2	Does the customer have access to the raw data e.g. for analytics purposes?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Data can be down loaded in CSV or PDF format

	If yes, describe:	
5.3	Can the Solution utilise existing infrastructure capabilities e.g. email, identity providers, web conferencing, telephony, collaboration, records management software available on-premises at the customer environment? If yes, please provide examples of integration scenarios your other clients have implemented:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Only internet access required
5.4	Are initial data migration facilities if applicable? If yes, what formats of data are supported e.g. XML, ASCII text, Excel (csv) etc:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No A simple CSV file of depersonalised non identifiable employment data only.
6. Service Hosting Environment		
6.1	Where (geographic locations) is the Solution being hosted?	Amazon Web Services Sydney
6.2	What is the technology platform of the hardware infrastructure underpinning the Solution (Windows, Linux, describe other)?	AWS Serverless Technology
6.3	Does the vendor own and control the complete hardware infrastructure used to provide the service i.e. servers, network connectivity, firewalls, log file management, web application firewalls and access and identity management etc? If no, outline how the proposed service depends on offerings by a third party?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No The Faethm Platform and client data is hosted in Amazon Web Services.
6.4	How is the hosting environment implemented to ensure good connectivity, security, capacity, load balancing, and redundancy of components, encryption and quality of service? Please include also relevant diagrams if possible.	We have selected AWS as our hosting provider. We have ensured that AWS provides and meets our required security standard. AWS is ISO27001, ISO27017, SOC 1, SOC 2, SOC 3, and IRAP certified.
6.5	Are there full disaster recovery and business continuity arrangements in place to safeguard service continuity? If no, outline customer responsibilities:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Faethm's hosting partner AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of data and infrastructure within service level agreement timeframes. Standard backups of the database are automatic and stored on AWS S3 bucket and archived to AWS Glacier after 30 days. Backups are compressed and encrypted before uploading to S3 bucket. Archived backups in Glacier are stored for 12 months. Database can be restored from standard or archived backups when a complete system failure of Faethm instance occurs.

6.6	<p>Is the proposed offering isolated from the impacts on performance from other organisations/consumers of the same offering?</p> <p>If no, outline to what extent the customer would be impacted:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Whilst client data is hosted in the region in which the client operates. The Faethm platform is replicated across 5 other regions and the databases are backed up nightly are archived for 30 days allowing for a restore in the event of a catastrophic event in a particular region.</p> <p>The platform operates on AWS serverless and therefore is not impacted by the performance of other clients.</p>
6.7	<p>Are there limits to the number of users being able to access the system (total number of users/ concurrent users)?</p> <p>If yes, outline the limitations:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>There is no limit on the number of users, however the contract provides for 50 users in the standard subscription agreement.</p>
6.8	<p>Will the performance be affected by increasing number of users?</p> <p>Is so, at what point and to what extent?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>There is no performance impact from the number of users</p>
6.9	<p>Does the service offer any flexibility (server load balancing) or automatic elasticity in terms of performance and/or storage capacity in case demand increases suddenly and unexpectedly?</p> <p>If yes, please provide details:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>The Faethm Platform operates on AWS serverless and is elastic in its provisioning to be scalable to client demand</p>
6.10	<p>Does the customer have access to the complete set of data, configuration files, design/as-built specifications in an on-going manner (availability of access and format of data)?</p> <p>If yes, please provide details:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>None required</p>
6.11	<p>Does the customer have access to the complete set of data, configuration files, design/as-built specifications in an on-going manner (availability of access and format of data)?</p> <p>If yes, please provide details:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>Repeat of above question</p>
6.12	<p>Is there any scheduled downtime period?</p> <p>If yes, please provide details:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>There is no scheduled downtime period. However should schedule downtime be required clients will be advised no less than 7 days in advance of scheduled downtime which will take place outside of operating hours</p>
6.13	<p>Is the customer immediately notified when there are unscheduled downtimes?</p> <p>If yes, please detail the method of advice:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>The clients Master User is the point of contact for unscheduled downtime and will be advised as soon as the issue is known.</p>

7. Reporting		
7.1	Describe the extent of reporting functionality available in the software system.	The Faethm Platform provides extensive Scenario Planning capability and these scenarios can be exported in either PNG or CSV format.
7.2	Which reporting tool has been used to create the reports?	The reporting tool utilizes Highcharts however as the data can be exported in CSV from Faethm and imported into any reporting tool that supports CSV upload.
7.3	Is it generally expected that the system provides all necessary reports, or are users able to create additional ad-hoc reports when the need arises? If so, how flexible report generation is?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No The Faethm Platform provides extensive Scenario Planning capability which generally supports the large majority of client reporting needs and is supported by the CSV export above for any other reporting needs,
7.4	Does the application provide facilities to export results to other formats e.g. PDF, Excel, Word, RTF and ASCII delimited? If not, list the formats:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Yes exports in CSV
7.5	If the customer wishes to utilise the data stored in the system for cube/pivot-table type reporting (e.g. similar as using Power BI, MS Analysis Services or SAS cubes), does the system offer this functionality? If not, what would you recommend as customer approach to providing that functionality to the users?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Exports in CSV which can be uploaded into other BI tools
7.6	Is there any kind of reporting available to the customer IT staff regarding the cloud service performance metrics? If yes, describe:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Not generally available but available on an ad hoc basis on request.
8. Change Management		
8.1	Please describe which environments are being recommended to be established eg. Production, training, test.	Clients only have access to the production version of Faethm. Faethm however maintains development, test and production environments.
8.2	Would all the environments be available permanently, or established on-demand?	<input checked="" type="checkbox"/> Permanently <input type="checkbox"/> Established on-demand
8.3	Is the customer notified of regular patching of the proposed software solution and other underlying software (Operating System, DBMS etc.)? If yes, describe lead-times:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Clients are not required patch. The Faethm platform leverages the automated monitoring and patch management capabilities provided by the AWS Systems Manager Patch Manager.
8.4	Are upgrades to the solution compulsory? If so, what planning and communication methods does the vendor use to allow time for planning of these, how much lead-time will the vendor give the	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No New releases of the Platform are required to be adopted by all clients. No less than 30 days notice will be provided of an

	customer of upcoming change, and what is the customer's role during these changes?	upcoming release and customer success managers will advise and discuss the content of the release and the rollout process with the client.
8.5	What is the proposed governance process to managing customer initiated changes arising from configuration and customisation requests to alter the proposed solutions functionality?	Clients will work with the dedicated customer success manager to communicate future new feature development and any other product support requirements.
9. System Support		
9.1	What warranty is offered for the product ie. is it > or < 90 days, and what does it cover?	<p>Our Warranties. We warrant that during an applicable subscription term:</p> <p>(a) this Agreement, the Order and the Documentation will accurately describe the applicable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data,</p> <p>(b) We will not materially decrease the overall security of the Platform,</p> <p>(c) The Platform will perform materially in accordance with the applicable Documentation, and</p> <p>(d) We will not materially decrease the overall functionality of the Platform. For any breach of a warranty above, Your exclusive remedies are those described in 12.3 (Termination) and 12.4 (Refund or Payment upon Termination).</p> <p>Disclaimers. Except as expressly provided herein, neither party makes any warranty of any kind, whether express, implied, statutory or otherwise, and each party specifically disclaims all implied warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, to the maximum extent permitted by applicable law. The Platform and Content are provided as is, exclusive of any warranty whatsoever. Each party disclaims all liability and indemnification obligations for any harm or damages caused by any third-party hosting providers.</p>
9.2	Does the vendor offer on-going services for the proposed application? List description and associated costs for services including:	<p><input checked="" type="checkbox"/> Dedicated hosting of the application. <input checked="" type="checkbox"/> Included <input type="checkbox"/> Extra Cost</p> <p><input checked="" type="checkbox"/> 1st level help desk for user support. <input checked="" type="checkbox"/> Included <input type="checkbox"/> Extra Cost</p> <p><input checked="" type="checkbox"/> 2nd level support for problem solving that were not able to be resolved by a business based application administrator initially. <input checked="" type="checkbox"/> Included <input type="checkbox"/> Extra Cost</p> <p><input checked="" type="checkbox"/> 3rd level support - technical trouble-shooting. <input checked="" type="checkbox"/> Included <input type="checkbox"/> Extra Cost</p> <p><input checked="" type="checkbox"/> Software Maintenance. <input checked="" type="checkbox"/> Included <input type="checkbox"/> Extra Cost</p> <p><input checked="" type="checkbox"/> System Administration. <input checked="" type="checkbox"/> Included <input type="checkbox"/> Extra Cost</p>

		<input type="checkbox"/> Solution configuration and customisation. <input type="checkbox"/> Included <input type="checkbox"/> Extra Cost <input checked="" type="checkbox"/> Other? Please specify: Advanced onboarding and additional services extra cost
9.3	Is there a support or account representative assigned to each customer? If yes, are there regular meetings:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Each client is assigned a Customer Success Manager
9.4	Does the vendor require remote access to customer infrastructure in order to provide support? If yes, describe access requirement:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No No access to client systems required
9.5	What skill sets are customer resources expected to have in order to operate/maintain the proposed vendor offering?	No specific skill set required
9.6	Is training is available for technical support, super users and standard users of the system? If yes, describe training required:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No All training provided through user guides and via customer success manager
9.7	Are there any user, technical and system manuals (tick any) that will be provided with the proposed application? Disclose all costs associated with the provision of additional manuals.	<input checked="" type="checkbox"/> user <input type="checkbox"/> technical <input type="checkbox"/> system manuals <input type="checkbox"/> other documentation (please specify): User guides provided and Customer Success Managers provide client on boarding
9.8	Is this material updated with new releases of the software? If so, detail any associated costs:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Updated with each new release
9.9	Does the application provide on-line help?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Context Sensitive help is available in the application
9.10	Can coverage for phone support be offered 8:30am to 5pm (Queensland time)? If not, detail coverage hours in Queensland time:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Coverage is provided during Queensland hours.
9.11	Is the help content customisable by users? If so, detail any associated costs:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Not required as standard but could be POA if required
10. Transition Out		
10.1	Describe the features, tools and data formats provided in the service to ensure that customers can easily and quickly migrate to alternative services if they wish.	Client retain their source data file and can export CSV files from the platform as required. The Faethm Platform is globally unique and therefore there is currently no alternative service of which we are aware.

		All data is securely disposed of when no longer required by the company, regardless of the media or application type on which it is stored. When a customer terminates their agreement with the company, data on the Faethm platform is rendered unrecoverable when electronically wiped using AWS standard processes.
10.2	Are there any termination or penalty fees for the above? If so, briefly explain:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Faethm Platform is provided under an annual subscription payable in advance non-refundable, there are no termination or penalties.
11. Other Strategic Considerations		
11.1	Outline the plans and policies for the release of enhanced versions of the application.	Faethm maintains a product roadmap which includes regular (generally six monthly) updates to the modeling and release of new features and UX enhancements
11.2	Describe future plans for the cloud offering in terms of new functionality.	As above
11.3	Describe future plans for the cloud offering in terms of new technologies.	The cloud offering operates in a stable AWS environment and there are no new technologies proposed at this time
11.4	List any useful links to other resources describing the system e.g. internet URL's etc.	https://www.faethm.ai

Released under the
Official Information Act

SECURITY CONTROLS QUESTIONNAIRE

SECURITY CONTROLS		
1. Information Asset Management		
1.1	What is the highest level of Information Security classified information (refer Information Standard 18) that the vendor is equipped to handle?	<input type="checkbox"/> Unclassified <input type="checkbox"/> X-in-confidence <input checked="" type="checkbox"/> Protected <input type="checkbox"/> Highly Protected AWS is certified for protected data
1.2	Is a procedure in place to audit access controls in the system (user roles vs admin etc)? How often are access controls reviewed? (should be reviewed at least twice yearly).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No All accounts are provisioned with Unique user ID's. Roles are define as admin and standard users. . A register of users and system access is maintained. Access is removed immediately on termination of employment and the register is reviewed quarterly.
2. Internet-facing systems, encryption and cryptographic ciphers		
2.1	Are security headers in place across the system? If not, can they be added?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No - Content Security Policy <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No - Server Resource Integrity <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No - X-Frame-Options <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No - X-Xss-Protection <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No - X-Content-Type-Options <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No - Referrer-Policy <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No - HTTP Strict Transport Security Sub resource integrity can be added if required.
2.2	Is an SSL certificate used?	We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using Cryptographic controls. https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanism All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B. All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated hardware security modules.
2.3	What encryption ciphers are used?	We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using Cryptographic controls. https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanism All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B. All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated hardware security modules.

		<p>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)</p>
2.4	<p>Is the system compliant with NIST minimum requirements for TLS implementation? https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-52r1.pdf</p>	<p>We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using Cryptographic controls. https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanism All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B..</p> <p>All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated hardware security modules.</p>
3. Human Resource Management		
3.1	<p>Are vendor employees/sub-contractors who have access to customer restricted data formally vetted? (e.g. Law enforcement background checks etc.)</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Police checks</p>
3.2	<p>Do vendor staff have remote access to systems that store customer restricted data?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Employees only have access to the information they require to carry out their role. As the application is access via the internet by all authorised uses then the system can be access remotely.</p>
3.3	<p>Do confidentiality agreements for employees and sub-contractors extend beyond tenure?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Confidentiality clause in employment contract survive beyond tenure</p>
4. Security and operations management		
4.1	<p>Is the vendor a Star Alliance (https://cloudsecurityalliance.org/star/) registrant?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
4.2	<p>Does the vendor test its software for security vulnerabilities, including conducting software penetration tests? If so, provide details of testing and frequency:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Faethm has partnered with Indusface to conduce daily scanning of the platform for OWASP vulnerabilities, penetration and malware monitoring. Indusface also conduct extensive manual penetration tests on a biannual basis.</p>
4.3	<p>Can you provide evidence of penetration tests that have been performed on the solution? If yes, please detail when they were performed</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Attached last manual test performed March 2019</p>
4.4	<p>Is the Customer able to engage a third-party to perform vulnerability or penetration testing on the vendors supplied solution to the Customer?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
4.5	<p>Does the vendor perform virus and malware scanning on a real-time or nightly basis?</p>	<p><input type="checkbox"/> Real-time <input checked="" type="checkbox"/> Nightly basis?</p>

4.6	Does the vendor quarantine infected records automatically and report these to the Customer?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If applicable
4.7	How often does the vendor patch systems or networks for non-critical updates?	<input type="checkbox"/> Monthly <input checked="" type="checkbox"/> Other: The Faethm platform leverages the automated monitoring and patch management capabilities provided by the AWS Systems Manager Patch Manager
4.8	Is all the following information captured in system logs (e.g. Successful/unsuccessful log-on and log-off attempts; identification and authentication failures; failed attempts to access information, records of change and/or access to functions within the system by any user or administrator)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Yes, the Faethm platform uses AWS native services to automatically generate audit logs and Datadog to analyse and explore log data in context. All critical infrastructure access requires 2FA authentication with Time-based One-Time Password (TOTP) along with RSA 4096 SSH Key. Faethm also leverages Amazon's extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection and password brute-force detection on AWS Accounts. Access to the AWS infrastructure that Faethm utilises is secured by Multi-Factor Authentication (MFA) as well as being network IP address locked (Application Tier and Data Persistence Tier).
4.9	Are exceptions (including risks or vulnerabilities) identified by data validity checks, audits or activity logging be communicated to the customer?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If applicable
4.10	How long are logs kept for?	Indefinitely
4.11	How often does the vendor review event and security logs?	Daily via alerts
4.12	Is the logged information available to the customer under the terms of the agreement either directly or on request? If yes, are there any costs for this or can the Customer directly access this information?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Can be provided on request
4.13	How does the service manage the transmission of security classified information?	The Faethm platform uses depersonalised unidentifiable employment data only
4.14	Are there any physical security measures that the vendor has implemented to protect the service e.g. physical access to facilities, backups etc. Please list:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No The Faethm platform is hosted in the AWS datacentres where state-of-the-art electronic surveillance and multi-factor access control systems manage physical access. Datacentres are staffed 24 x 7 by trained security guards and access is restricted to authorised personnel. The Faethm business operations are in One International Towers Barangaroo, a state of the art office tower with Security Guards, Security card access to lifts, floor and office and 24x7 CCTV coverage.
4.15	Can you provide a security whitepaper or equivalent security documentation for the solution? If yes, please detail:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

5. Access management		
5.1	What authentication mechanisms are used on the vendor's solution offered to the customer e.g. multifactor or password (specify password complexity rules):	<p>All accounts are provisioned with Unique user ID's. Roles are defined as admin and standard users. Users are only given access to the systems and information they require to perform their role. Sessions time outs are in place. A register of users and system access is maintained. Access is removed immediately on termination of employment and the register is reviewed quarterly. All critical infrastructure access requires 2FA authentication with Time-based One-Time Password (TOTP) along with RSA 4096 SSH Key.</p> <p>Minimum length 8 characters one upper case, alpha, numeric and a special character Automatic blocking/locking mechanisms (i.e. limitation of the number of access attempts to an account) Enforces set duration for password changes (90 days) Enforces requirements to prevent password re-use (last 5 passwords) Enforces a set number of invalid login attempts before an account is locked out (5 attempts)</p>
5.2	Are there methods of federating customer identity store (active directory) with the service offering exist? Please list - e.g. Microsoft ADFS or other for single sign on.	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>Due to the relatively small number of users at client sites SSO is not currently available</p>
5.3	Is there an automated password recovery process for the customer's users? If yes, specify process:	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Enforces set duration for password changes (90 days) Enforces requirements to prevent password re-use (last 5 passwords) Enforces a set number of invalid login attempts before an account is locked out (5 attempts) Users are able to request a password reset that will send an email with a recovery code</p>
5.4	What authorisation mechanisms are used to access the system?	Authorised users access via username and password
5.5	What security encryption protocols are used by default and what are offered optionally e.g. is SSL 2.0 or 3.0 supported?	<p>We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using CryptoGraphic controls. https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanism All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B. All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated hardware security modules.</p> <p>TLSv1.2 is available by default</p>

5.6	How is user access invoked and revoked?	All clients nominate a Master User who provides the users requiring access to the system and advises Faethm when a user's access should be revoked.
5.7	Can the customer assume full control of provisioning user access, or does the vendor need to fulfil some continuous role in invoking and revoking user access?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No The Customer advises the customer success manager of the user access requirements and the CSM actions the request
6. Information security incident management		
6.1	Does the vendor have an information security incident management policy and procedures?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Attached
6.2	Does the vendor perform on-going 24/7 monitoring to detect unusual activity with an automated intruder detection system?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Faethm also leverages Amazon's extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection and password brute-force detection on AWS Accounts. Access to the AWS infrastructure that Faethm utilises is secured by Multi-Factor Authentication (MFA) as well as being network IP address locked (Application Tier and Data Persistence Tier).
6.3	Is the customer advised of details of any information security incidents? If yes, specify:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No We comply with the Privacy Amendment (Notifiable Data Breaches) Act 2017 and also notify clients of any detected incidents that impact client data
6.4	When was the last serious security incident breach?	There have been no security incidents to date since the inception of Faethm
6.5	What is the external party's process for disclosing to the customer, any data requests, such as subpoenas or warrants, from a third party?	No specific procedures are in place as Faethm does not utilize any third parties.
7. Backup and Disaster recovery		
7.1	State how data is backed up daily, weekly and monthly. How long are these backups of Customer data retained for? How is backup data stored? Are offline copies kept?	Continual point in time backups of client data re kept for 35 days, in addition to this, standard nightly backups of data are automatic and stored on AWS S3 bucket and archived to AWS Glacier after 30 days. Backups are compressed and encrypted before uploading to S3 bucket. Archived backups in Glacier are stored for 12 months.Database can be restored from standard or archived backups when a complete system failure of Faethm instance occurs.
7.2	Are disaster recovery arrangements and business continuity plans in place?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Faethm has its own BCP plan which is tested annually last test 11/18. Faethm's hosting partner AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of data and infrastructure within service level agreement timeframes.
7.3	Does the Vendor's out of box / standard service offering backup allow for point-in-time recovery in case of failure? If not, supply details including costings for this option.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No As above

7.4	Are backup arrangements in place for installing new patches and upgrades to the service offering? If not, supply details including costings for this option	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No The Faethm platform leverages the automated monitoring and patch management capabilities provided by the AWS Systems Manager Patch Manager.
7.5	Does the vendor test the integrity of the backups? If not, supply details including costings for this option:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Reliance is placed on AWS
7.6	Can the vendor ensure system availability consistent with the customer's disaster recovery objectives for its clients? If not, supply details including costings for this option:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No The Faethm Platform is not considered to be a financial or mission critical system and therefore should meet the requirements of a clients DRP plan.
7.7	Does the vendor test disaster recovery process and procedures? If not, supply details including costings for this option.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No BCP procedures are tested.
7.8	Is the infrastructure dispersed; are the primary site and the disaster recovery site geographically separated?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Whilst client data is hosted in the region in which the client operates. The Faethm platform is replicated across 2 other regions and the databases are backed up nightly are archived for 30 days allowing for a restore in the event of a catastrophic event in a particular region.
8. Compliance		
8.1	Is the vendor QASSURED? If yes state number. If no, are there future plans to become accredited?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No There are no current plans to become QASSURED
8.2	Is the vendor GITC accredited for Module Order 10? If yes state number. If no, are there future plans to become accredited?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No There are no current plans to become GITC accredited
8.3	Does the vendor comply with AS/NZS ISO/IEC 27002:2013: Information Technology – Security Techniques – Code of Practice for information security? Please provide Statement of Applicability	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Whilst our information security policy is not yet ISO27001 certified it has been developed in line with the principals of ISO 27001. In addition, we have selected AWS as our hosting provider as AWS meets our required security standard. AWS is ISO27001, ISO27017, SOC 1, SOC 2, SOC 3, and IRAP certified. We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using Cryptographic controls. All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B (https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanisms). All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated hardware security modules.
8.4	Does the vendor comply with the emerging AS/NZS ISO 27017: Information Technology – Security Techniques – Code of Practice for information security controls for cloud computing services based on ISO/ICE27002?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown Whilst our information security policy is not yet ISO27001 certified it has been developed in line with the principals of ISO 27001. In addition we have selected AWS as our hosting provider as AWS meets our required security standard. AWS is ISO27001, ISO27017, SOC 1,

		SOC 2, SOC 3, and IRAP certified. We use strict end to end encryption using TLS RSA/AES-GCM. We follow industry standard NIST Guidelines for using Cryptographic controls. All data at rest is encrypted by AWS in accordance with the NIST Special Publication 800-175B (https://www.nist.gov/publications/guideline-using-cryptographic-standards-federal-government-cryptographic-mechanisms). All encryption keys are stored on AWS KMS which uses the AES-GCM with 256-bit secret keys in FIPS 140-2 validated hardware security modules.
8.5	Does the vendor comply with the PCI DSS (current version)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Unknown N/A
8.6	Does the proposed offering comply with the <i>Privacy Act 1988</i> and the <i>Queensland Information Privacy Act 2009</i> in regards to dealing with privacy information? Explain the practices and procedures you have in place that govern how personal information may be held, used or disclosed by your organisation (by reference to the IPPs and NPPs in the <i>Queensland Information Privacy Act 2009</i>).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown The Faethm platform uses depersonalised unidentifiable employment data only therefore no personal or private data is provided by the client to Faethm.
8.7	If data is stored outside Australia - regarding storage of privacy information according to the <i>Queensland Information Privacy Act 2009</i> , part 3: section 33 - if data is stored overseas, is the facility used to store privacy information subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the Information Privacy Principles described in the <i>Queensland Information Privacy Act 2009</i> , Schedule 3?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown No data is stored outside of Australia.
8.8	Does the cloud service provider comply with National Institute of Standards and Technology (NIST) SP800-53: Security and Privacy Controls for Federal Information Systems and Organizations?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown
8.9	Does the cloud service provider comply with US Federal Risk and Authorization Management Program (FedRAMP) requirements?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown Click here to enter text.
8.10	Does the cloud service provider comply with Statement on Standards for Attestation Engagements (SSAE)16 requirements?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown Click here to enter text.
8.11	Regarding any files uploaded to the proposed solution, does the system comply with relevant record keeping standards listed below? <ul style="list-style-type: none"> • <i>Public Records Act 2002</i> • Queensland Government, <i>IS40 Recordkeeping Policy</i> http://www.qgcio.qld.gov.au/products/electronic-document-and-records-management/548-qgea/products/qgea- 	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown Not applicable, the only data uploaded is depersonalised unidentifiable employment data

	<p>documents/information/2357-recordkeeping-is40)</p> <ul style="list-style-type: none"> • Queensland State Archives, <i>Queensland recordkeeping metadata standard and guideline</i> (http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/QRKMS.pdf) • Queensland Government Enterprise Architecture, <i>IS31 Retention and disposal of public records</i> (http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2360-retention-and-disposal-of-public-records-is31) • Queensland Government Enterprise Architecture, <i>IS34 Metadata</i> (http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2458-metadata-is34) 	
8.12	<p>What other Security Compliance Standards or Certifications does the vendor comply with?</p>	<p>Whilst the Faethm Platform is not yet ISO27001 certified it has been developed in line with the principals of ISO 27001. In addition we have selected AWS as our hosting provider as AWS meets our required security standard. AWS is ISO27001, ISO27017, SOC 1, SOC 2, SOC 3, and IRAP certified.</p>

Released Under RTI - PSC

General Contract Conditions - ICT Products and Services

These General Contract Conditions - ICT Products and Services are to be used in connection with the Details.

1 The Contract

1.1 When Contract is formed

A Contract will be formed between the Customer and the Supplier on the date when the Authorised Representatives of both parties have signed the appropriate section of the Details.

The Contract may consist of a number of counterparts and if so, the counterparts taken together constitute one document.

1.2 Interpretation

The definitions and rules of interpretation for the Contract are set out in clause 24.

1.3 Hierarchy

If there is any inconsistency between the documents which make up the Contract, then the following will prevail in descending order of precedence:

- (a) these General Contract Conditions - ICT Products and Services;
- (b) the Details (excluding any Additional Provisions and any document which the Details state will form part of the Contract or is otherwise expressly incorporated by reference in the Contract);
- (c) any Additional Provisions;
- (d) any statement of work formed under clause 7;
- (e) any schedules (excluding any document which the Details state will form part of the Contract or is otherwise expressly incorporated by reference in the Contract); and
- (f) any document which the Details state will form part of the Contract or is otherwise expressly incorporated by reference in the Contract.

1.4 Additional Provisions

- (a) Subject to clause 1.4 (b), the Customer and the Supplier may agree to include Additional Provisions.
- (b) Additional Provisions take effect only to the extent they are additional to, and do not detract from the parties' rights and obligations under, the terms and conditions of the General Contract Conditions, provided that any Additional Provisions included to enable the Customer to comply with applicable legislative or policy requirements are deemed not to detract from the parties' rights and obligations.

2 Non exclusivity

Unless expressly stated otherwise in the Details, the Customer may engage other suppliers to (or itself) provide products, services and other deliverables the same as or similar to the Deliverables.

3 Term

The Contract starts on the start date specified in the Details and continues for the period set out in the Details unless any extension options are exercised under this clause 3.

The Customer may extend the Term on the same terms and conditions for any extension period(s) specified in the Details by giving the Supplier written notice by at least the period as specified in the Details before expiry of the then current Term.

4 Supplier general obligations

The Supplier:

- (a) **(time)** must meet all Delivery Dates specified in the Details or as otherwise agreed in writing, and perform all other obligations in a prompt, diligent and competent manner;
- (b) **(delay)** will promptly notify the Customer if it believes it will not be able to meet any Delivery Date;

- (c) (**Deliverables**) must provide the Deliverables in accordance with the Contract and ensure that the Deliverables comply with all Laws;
- (d) (**Requirements**) must meet, and ensure that the Deliverables meet, the Requirements;
- (e) (**Service Levels**) must meet or exceed the Service Levels (if any);
- (f) (**quality**) must ensure that all Deliverables are of a high quality, professional standard and fit for their usual purpose;
- (g) (**interference**) must, when present at the Site, avoid unnecessary interference with the Customer's business and activities;
- (h) (**policies**) must, where relevant to the Supplier's obligations under the Contract, comply with all Customer policies, codes of conduct, rules, standards and procedures (including in respect of work health and safety and security) which apply to the Site, the Customer's IT System, the Customer's Personnel or use of the Customer Inputs listed in the Details, and all other Customer policies, codes of conduct, rules, standards and procedures listed in the Details. If the Customer amends a relevant, or introduces a new, policy, code of conduct, rule, standard or procedure relevant to the Supplier's obligations under the Contract, it will notify the Supplier and the Supplier must comply with the amended or new policy, code of conduct, rule, standard or procedure from the date of notification. Copies of the relevant policies are available on request;
- (i) (**access to Customer's IT System**) must, where access to the Customer's IT System is required to provide the Deliverables or is otherwise granted to the Supplier by the Customer:
- (i) only access and use that part of the Customer's IT System for which the Supplier is authorised, and only for the purpose of performing the Contract and to the extent necessary to perform the Contract; and
- (ii) not tamper with, hinder the operation of (except as expressly permitted by the Contract) or make unauthorised modifications to the Customer's IT System or maliciously or negligently introduce any Harmful Code to the Customer's IT System;
- (j) (**directions**) must comply with all reasonable directions of the Customer in relation to the Supplier's performance of the Contract;
- (k) (**Customer Inputs**) must take care of Customer Inputs and only use Customer Inputs for the purpose of performing the Contract, to the extent necessary to perform the Contract, and in accordance with the requirements specified in the Details. The Supplier must promptly inform the Customer of any loss, destruction or damage (other than fair wear and tear) to any Customer Input. If the Supplier loses or damages any Customer Input (other than fair wear and tear), the Supplier must, at the election of the Customer, promptly replace such Customer Input or pay the Customer the reasonable replacement cost of such Customer Input. As between the Supplier and the Customer, the Customer retains all right, title and interest (including all Intellectual Property Rights) in the Customer Input. As soon as practicable after termination or expiry of the Contract, the Supplier must return to the Customer all equipment, records, documents and materials (including Customer Inputs) provided by the Customer for the purposes of the Contract, except to the extent that such documents and records are required by Law to be retained, or for the Supplier's reasonable internal credit, risk, insurance, legal and professional responsibilities. This clause 4(k) does not apply to any Customer Input which comprises Customer Data;
- (l) (**cooperation**) must cooperate with the Customer's Personnel and other suppliers to the Customer who provide goods and services relating to the Deliverables;
- (m) (**Laws**) must comply with all Laws in performing its obligations under the Contract;

- (n) **(Documentation)** must during the Term supply all Documentation to the Customer, and at no additional cost, any revisions, replacements or additions to the Documentation so that the Documentation includes the most current and up-to-date versions generally available to customers of the Supplier;
- (o) **(training)** must provide to the Customer the training (if any) specified in the Details;
- (p) **(records)** must create and maintain records of its performance of the Contract in accordance with applicable Laws and usual industry practice for provision of products and services similar to the Deliverables;
- (q) **(insurance)** must at its cost and by the start date of the Contract, take out and maintain or be insured under, the insurance policies described in the Details with an insurer authorised and licensed to operate in Australia or otherwise with an insurer with a security rating of A- or better from AM Best (or equivalent rating organisation), on terms that are reasonably commercially available. The Supplier must promptly notify the Customer if any policy is cancelled or there is any significant change in any of those policies which may impact the Supplier's ability to meet its obligations under the Contract. The Supplier must maintain all required insurance policies which are maintained on a "claims made" basis for a minimum period of 4 years after the Contract ends, or such other period specified in the Details. The Supplier must, on request, provide to the Customer an insurance certificate of currency confirming that the Supplier has effected and renewed or is insured under the insurance policies described in the Details. The Customer may at its sole discretion, agree to the Supplier being self-insured provided that the Supplier provides the Customer with such supporting documentation as may be required by the Customer, including the Supplier's financial records (limited to publically available financial records where the Supplier or its Related Body Corporate is publically traded);
- (r) **(authorisations)** must obtain and maintain the authorisations described in the Details and any other licences, permits, permissions and authorities necessary for the Supplier to perform the Contract. The Supplier must, upon request, provide evidence that it has complied with this clause;
- (s) **(security requirements)** must, if specified in the Details, provide a bank guarantee, performance guarantee and/or other specified security **(security)** to guarantee the proper performance of the Supplier's obligations under the Contract. The security must be in a format reasonably acceptable to the Customer. The security must meet all additional conditions specified in the Details. The Customer will not have any liability to the Supplier in connection with the Customer's enforcement of the security;
- (t) **(further assurances)** must do anything and execute any document that the Customer reasonably requests, to give effect to the Contract;
- (u) **(reports)** must provide reports in the timeframe and format specified in the Details and such other reports as and when reasonably requested by the Customer;
- (v) **(meetings)** must attend the meetings at the frequency set out in the Details and at such other reasonable times, if the Customer requests;
- (w) **(competitive neutrality)** must if the Supplier is a government owned business, local government, or Commonwealth, State or Territory or authority, price its offer to comply with the competitive neutrality principles of the Supplier's jurisdiction;
- (x) **(expertise)** warrants that it has the necessary skills and expertise to properly perform the Contract, and all its Personnel performing duties in relation to the Contract are competent and have the necessary skills and expertise to properly perform the duties allocated to them concerning the Contract; and
- (y) **(access and inspection)** on reasonable prior written notice from the Customer, must give the Customer reasonable access during Business

Hours to the Supplier's premises where the Deliverables (excluding As a Service supplied under clause 5.6) are being performed or produced, and to the Supplier's documentation, records and Personnel, to enable the Customer to verify that the Supplier is complying with its obligations under the Contract, and will promptly address any non-compliance identified by the Customer and notified to the Supplier. Nothing in this clause 4(y) requires the Supplier to provide the Customer with access to any documents or records of or in respect of a third party.

5 ICT terms and conditions specific to Deliverables

5.1 Hardware

The following terms and conditions apply to the supply of any Hardware under the Contract:

- (a) **(delivery)** the Supplier must deliver the Hardware to the Site by the Delivery Date, in accordance with the Details and the Customer's instructions;
- (b) **(packaging)** the Supplier must adequately pack and protect the Hardware to withstand transit and storage, and provide a packing note or manifest with the Hardware which identifies the items of Hardware and quantities in the delivery package;
- (c) **(installation)** if specified in the Details, the Supplier must install the Hardware at the Site in accordance with the requirements set out in the Details;
- (d) **(condition)** all items of Hardware must be new, unused and of recent origin unless otherwise specified in the Details;
- (e) **(risk)** risk in the Hardware will transfer to the Customer when delivered to the Site in accordance with the Details and the Customer's delivery instructions;
- (f) **(title)** unless specified otherwise in the Details, title in the Hardware will transfer on the earlier of its delivery to the Site or payment of the applicable Price;
- (g) **(ancillary services)** the Supplier must provide the ancillary services (if any) in connection with the Hardware as specified in the Details;
- (h) **(warranties)** the Supplier warrants that the Hardware:
 - (i) will, during the Warranty Period, comply with and perform in accordance with the Requirements;
 - (ii) will, during the Warranty Period, be compatible and inter-operate with, and will not detrimentally affect the operation or performance of, the Designated Environment, when used in accordance with the Documentation;
 - (iii) may be used in accordance with the Documentation without risk to health or safety; and
 - (iv) will not be subject to any encumbrance or interest, except for an encumbrance or interest which arises by operation of a Law that cannot be excluded by contract;
- (i) **(manufacturer warranties)** if the Supplier is not the original equipment manufacturer, the Supplier must:
 - (i) ensure the Customer receives a copy and is fully advised of and approves all manufacturer's warranties prior to any order or commitment being made in respect of any Hardware; and
 - (ii) assign or otherwise provide the benefit of any manufacturer's warranty to the Customer;
- (j) **(Defects)** subject to clause 5.1(k), during the Warranty Period the Supplier must, at no cost to the Customer:
 - (i) remedy all Defects in the Hardware either by repair, replacement or modification; and
 - (ii) take all reasonable measures (including providing a Workaround) to enable the Customer to continue to productively use the Hardware while remedying Defects; and
- (k) **(exceptions)** the Supplier is not required to remedy any Defect in the Hardware to the extent the Defect arises as a result of:

- (i) any failure of the Customer to comply with its obligations under the Contract;
- (ii) modifications to the Hardware that were effected or attempted by a person other than the Supplier, its Personnel or a person authorised by the Supplier;
- (iii) damage caused by operation of the Hardware other than in accordance with the Documentation and the Contract; or
- (iv) damage caused by use of consumables or parts with the Hardware which are not authorised by the Supplier.

Where the Supplier, acting reasonably, determines that the Defect arises as a result of circumstances set out in this clause 5.1(k), then if the Customer requests the Supplier to remedy the Defect, the Supplier is entitled to charge the Customer for the costs and expenses (calculated using the rates set out in the Schedule 1 – Price and Payment Terms, or if none are stated, at the Supplier's then current commercial rates) that arise out of or in connection with identifying and attempting to remedy that Defect.

5.2 Hardware Maintenance Services

The following terms and conditions apply to the supply of any Hardware Maintenance Services under the Contract:

- (a) **(maintenance period)** the Supplier must provide the Hardware Maintenance Services for the period specified in the Details;
- (b) **(replacement parts)** where specified in the Details, the Supplier must maintain a stock of frequently required Supported Hardware parts as may be necessary to meet the Service Levels;
- (c) **(general support)** the Supplier must provide the general support specified in the Details during the hours of support specified in the Details;
- (d) **(preventative maintenance)** the Supplier must provide preventative maintenance services on a scheduled basis as set out in the Details;

- (e) **(remedial maintenance)** after being notified of a Defect or possible Defect in the Supported Hardware, the Supplier must provide remedial maintenance services as set out in the Details.

Where the Supplier replaces parts of the Supported Hardware:

- (i) the replacement parts will be new unless otherwise specified in the Details;
- (ii) title and risk in the replacement parts will transfer to the Customer on installation unless otherwise specified in the Details; and
- (iii) title and risk in the replaced parts will transfer to the Supplier on its removal of the replaced parts;

- (f) **(Service Levels)** the Supplier must measure its performance against the Service Levels and provide a report to the Customer at the frequency specified in the Details;

- (g) **(Service Credits)** subject to clause 5.2(j), if the Supplier fails to meet the Service Levels, it must apply the Service Credits against the next invoice issued after the relevant Service Credits accrue, or in accordance with the process specified in the Details. If the Contract has terminated or expired, the Supplier must promptly pay the amount of the Service Credits to the Customer;

- (h) **(engineering changes)** the Supplier must, at no additional cost to the Customer, implement any Mandatory Engineering Changes to the Supported Hardware;

- (i) **(warranties)** the Supplier warrants that the Hardware Maintenance Services will be performed:

- (i) using appropriate materials of high quality;
- (ii) by appropriately qualified and trained Personnel; and
- (iii) to a standard that ensures continuity of performance of the Hardware Maintenance Services in accordance with the Service Levels (or if no service levels are agreed, in a reasonable time and manner) and the Contract; and

- (j) **(exceptions)** the Supplier is not required to provide the Hardware Maintenance Services and is not responsible for any failure to meet the Service Levels to the extent that the Defect or failure to meet the Service Levels arises as a result of:
- (i) any failure of the Customer to comply with its obligations under the Contract;
 - (ii) damage arising from changes, alterations, additions or modifications effected or attempted by a person other than the Supplier, its Personnel or a person authorised by the Supplier;
 - (iii) damage caused by operation of the Supported Hardware other than in accordance with the Documentation and the Contract; or
 - (iv) damage caused by use of consumables or parts with the Supported Hardware which are not authorised by the Supplier.

Where the Supplier, acting reasonably, determines that the Defect or failure arises as a result of circumstances set out in this clause 5.2(j), then if the Customer requests the Supplier to remedy the Defect or failure, the Supplier is entitled to charge the Customer for the costs and expenses (calculated using the rates set out in Schedule 1 – Price and Payment Terms, or if none are stated, at the Supplier's then current commercial rates) that arise out of or in connection with identifying and attempting to remedy that Defect or failure.

5.3 Licensed Software

The following terms and conditions apply to the supply of any Licensed Software under the Contract:

- (a) **(licence)** subject to clause 5.3(e), the Supplier grants the Customer a non-exclusive licence to:
 - (i) install, use and copy the Licensed Software for the Customer's functions and activities, or such other purposes specified in the Details, and otherwise in accordance with the terms of the Class of Licence;
 - (ii) adapt and modify the Licensed Software to the extent necessary to enable it to be used on the Designated Environment; and
 - (iii) make necessary copies of the Licensed Software for back-up, disaster recovery and security purposes;
- (b) **(licence period)** unless the Details specify a perpetual licence, the licence period for the Licensed Software is the period specified in the Details;
- (c) **(sublicensing)** the Customer may sublicense any of the rights granted under clause 5.3(a) to the Licensed Software to:
 - (i) on one or more occasions, on a limited time basis to a contractor that is providing outsource services to the Customer that includes the operation of the Licensed Software, provided that the Licensed Software is used solely for use of the Customer as is permitted under this clause 5.3, is limited to the period of the outsource arrangement and the sublicense automatically terminates at the end of the period of the outsource arrangement; or
 - (ii) any entity specified in the Details at no additional cost, unless the additional cost is specified in the Details;
- (d) **(restrictions on use)** the Customer agrees, except to the extent permitted by the Contract or applicable Law, not to:
 - (i) distribute, sublicense or otherwise transfer all or any part of the Licensed Software to any other person; or
 - (ii) attempt to disassemble, decompile or otherwise reverse engineer the Licensed Software;
- (e) **(additional conditions and restrictions)** the Customer must comply with any additional licence conditions and restrictions on use of the Licensed Software specified in the Details;