

**Market Assessment (Tender Document)**

Firewall Support and Maintenance

The University of Chichester

**Submissions can be made until**

**17:00 (GMT) 12 December 2024**

Copyright © 2024 by The University of Chichester. All rights reserved. This document is supplied purely for the purpose of assisting suppliers to respond to this procurement, no part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) for any other purpose.

|  |  |  |
| --- | --- | --- |
| University of Chichester  College Lane  Chichester  West Sussex  PO19 6PE | Telephone:  Date:  Revision:  Email | 01243 816000  11/11/2024  1.0 Final  [Tenders@chi.ac.uk](mailto:Tenders@chi.ac.uk) |

A close-up of a sign

Description automatically generatedA black and white logo with text

Description automatically generated with medium confidenceA logo with text on it

Description automatically generated

**Contents**

[1. Market Testing Firewall System Provision and Support 1](#_Toc182307616)

[1.1 Aims of this document 1](#_Toc182307617)

[1.2 The University 1](#_Toc182307618)

[1.3 The University’s Firewall 1](#_Toc182307619)

[1.4 Critical Success Factors 1](#_Toc182307620)

[1.5 Background to this market testing process 2](#_Toc182307621)

[1.6 Seeking clarification – Questions and Answers 2](#_Toc182307622)

[1.7 Market Assessment Timetable 3](#_Toc182307623)

[1.8 Submitting an Expression of Interest (EOI) – and a request to meet via tenders@chi.ac.uk 3](#_Toc182307624)

[1.9 Clarifications regarding the Invitation to submit an Expression of Interest 3](#_Toc182307625)

[1.10 Evaluation of Submissions 4](#_Toc182307626)

[1.11 Evaluation Criteria 4](#_Toc182307627)

[1.12 How the University assesses a tender 5](#_Toc182307628)

[1.13 Consortia and Subcontracting 5](#_Toc182307629)

[1.14 Confidentiality and Freedom of Information 5](#_Toc182307630)

[2. Some General Questions 6](#_Toc182307631)

[2.1 General service and cost questions 6](#_Toc182307633)

[2.2 Organisational experience and capability 7](#_Toc182307634)

[2.3 Compliance with the Social Value Model 7](#_Toc182307635)

[3. Costed Proposal 9](#_Toc182307636)

[Appendix 1: Contact Details 1](#_Toc182307637)

[3 Appendix 2: The Firewall and its broad context 2](#_Toc182307638)

[3.1 Schematic of components and integrations 2](#_Toc182307639)

[3.2 Firewall Services as-is 2](#_Toc182307640)

[Appendix 3: Social Value Model: 3](#_Toc182307641)

[Appendix 4: Minimum Security Standards 6](#_Toc182307642)

[Appendix 5: Supply Chain Risk Management Strategy 8](#_Toc182307643)

1. Market Testing Firewall System Provision and Support
   1. Aims of this document

The purpose of publishing this document is to invite expression of interest from suppliers who have the capability to provide the next iteration of the University’s Firewall. The current provision is based on Palo Alto, and although this is not a given, we anticipate that new services must be able to integrate seamlessly with our estate and various interconnected services.

We anticipate that through this tendering process we will enable fair competition, and that we will identify a partner to deliver and maintain our services. We expect a 3-5 year initial contract term, with potential to extend, but foremost is our need to secure and commence our new services before the end of December 2024.

* 1. The University

The University of Chichester is a forward-looking institution with a rich history that goes back to 1839 ([See ‘about us’ link](https://www.chi.ac.uk/about-us/)). The University has a broad academic portfolio and a widening participation ethos, serving around 5500 students through around 1400 full time, part time and associate lecturer personnel. Our student population comprises of undergraduates, research students, and an increasing number of Degree Apprentices.

The University employs the leading HE systems to enable its information ecosystem. This includes the suitable, proven supply arrangements for learning and teaching but also for managing the organisation with integrity.

* 1. The University’s Firewall

The appendices set out details of the security and firewall components. We expect that you will understand why these are presented in high-level, and we will be pleased to elaborate in the Q&A meetings we have set out in the procurement process. Our services are protected by (and need to be compliant with) common security technologies and methods, including delineated VLANs, Role Based Access, Insider Protection / Firewalling, Multi Factor Authentication, Mobile Device Management and a Virtual Private Network for off-site access.

The University is amongst the first of HEIs to achieve institution wide ISO27001, and also has Cyber Essentials and Cyber Essentials Plus Accreditation, where this is required (with additional security protocols) for Defence Contactor work. We would expect our Firewall partners to embrace these standards, to recognise their role in our Information Security Management System (ISMS) and to work collaboratively with our excellent and highly committed team to maintain, enhance and constantly improve our Security Operations Centre.

Our infrastructure uses a private dark fibre to connect our two data centres, (one on each of the Chichester and Bognor Regis Campuses) each with a JISC internet connection. The University currently employs two Palo Alto PA-3250 firewalls, with one located on each of its campuses. They leverage Application Filtering, Threat Protection, Cloud based malware protection, SSL decryption and inspection, anti-virus protection, client VPN and user identification to maintain a strong network perimeter for the University’s sensitive data. With a typical average throughput of around 4Gbps, we are looking to expand and futureproof our capacity to better handle peaks in network load, by maintaining the same level of protection on more capable hardware, such as the Palo Alto PA-3410, which offers approximately 3 times the performance of our current PA-3250

Our current service comprises of.

* The supply and commissioning of the Palo Alto hardware and its software,
* Palo Alto subscriptions (which are paid until 31/12/24), and,
* Support Services, including hardware and software maintenance and minor/major updates
  1. Critical Success Factors

The University cannot contemplate business interruption – all systems operate 24/7/365. Any new or altered system(s) must be familiar and proven in the HEI sector and must be capable of seamless implementation.

The University has limited opportunity to disrupt its workflows, as recruitment, retention, and the cycle of the academic year leaves no part of the year when a system can be taken off-line to be replaced, in part or in full.

Although the supplier will initially adopt the existing firewall hardware, we anticipate replacing this early in 2025, with new equipment, to meet our ever growing transactions, and need to retain archival data for safeguarding.

We are objective in terms of hosting arrangements, and are objective in considering the various proprietary solutions, however, we currently believe the existing supported on-premises Palo Alto configuration, with its established system interfaces, offers the most reliable and familiar secure form of delivery.

The University has a Supply Chain Risk Management Strategy (SCRMS), (See [Appendix 5](#Appendix5SCRMS)) which is required to satisfy current and future University partners that we maintain certificated standards, on premises, and throughout the entire supply chain. These include the minimum security standard MSS (see [Appendix 4](#Appendix4MSS)), which is underpinned through the University and its suppliers maintaining accreditations such as ISO27001, Cyber Essentials and where relevant, the Payment Card Industry Data Security Standard (PCIDSS).

Given the specific nature of the firewall as central to our business continuity, we would anticipate that there will be a coherence with the National Cyber Security Centre’s list of approved Cyber Incident Response providers, either directly, or by formal association.

We take pride in safeguarding our students, staff and other stakeholders – this includes protecting their data, but also for the Prevent duty of care, and avoidance of criminality. Key aspects of our evaluation will include the relationship to R;pple, the Home Office Block List, and the classification of, and logging of access to various types of web-site

We draw attention to evaluation criteria in section 1.12, which includes that candidates must be able to demonstrate compliance with for example, the Modern Slavery Act, the Social Values Act ([Appendix 3](#Appendix3SVM)) and must demonstrate evidence of policies and processes for sustainability throughout their operation and supply chain.

* 1. Background to this market testing process

Towards the end of any contract term, the University undertakes market testing to assess the fit, risks and costs of its current and potential alternative solutions. Here, without prejudice, we consider as wide a range of pricing as we can get access to, across the range of options for framework sourcing, tendering or direct negotiated award.

Market testing enables that the University can ensure any procurement decision reflects the up-to-date list price of the solutions presented through the procurement frameworks a university can buy from. However, we recognise that there may be new solutions, solution providers and added value resellers that we are not aware of.

Whilst the supplier community landscape is constantly hanging, we do not find that there are simple, clear providers for our firewall provision, licensing and support requirements available from the various frameworks a university can access. Some companies have some of the requirement on one framework, and there are examples where the same company is registered under a different ‘lot’ on one of the other frameworks.

Consequently, on this occasion tendering appears to be the most competitive and fairest route to engaging with the supplier community, and we use documents such as this and the publication of an outline specification to enable known and unknown solution providers an equal opportunity to identify their capabilities and costs.

In line with current recommended practices, all market testing (and tendering) is published through the tendering site (Contractsfinder / Findatender) as a transparent and suitable method of engaging all potential suppliers, equally, and in accordance with the Public Contracts Regulations 2015 and the guidance available from the Crown Commercial Service. Through this tender, our aim is to assess candidates on a level playing field, and then take the most economically advantageous way forward, taking into account the costs of any solution, and the relative risks of transferring from A to B etc.

* 1. Seeking clarification – Questions and Answers

For all queries about this document and our procurement process please contact us by email [tenders@chi.ac.uk](mailto:tenders@chi.ac.uk).

Please note that you must not otherwise contact University staff directly and you should avoid any related discussion if you happen to be working with us in some other capacity, (as this might be considered canvassing, which could lead to the need to exclude your organisation from the tender process). Equally, we will maintain robust air gaps between any related business as usual, and this procurement process.

Please note that dependent upon the nature of the enquiry, and in so much as it does not identify your organisation, the answers to any questions you raise will be responded to by periodic updates in the Q&A section of our tendering website.

* 1. Market Assessment Timetable

The market assessment is working to the following timescale:

|  |  |
| --- | --- |
| Stage | Key Dates |
| Publication of requirements on ContractsFinder | 12/11/24 |
| Closing Date for submission of Expressions of Interest | 30/11/24 12:00 GMT |
| Written Clarifications (Questions and Answers) | Please note we ask for formal questions to be raised at least a week before the submission date. |
| Potential opportunity for 1:1 Q&A session (if required) | Tuesday 10 December – times to be agreed |
| Final close for tender submissions | 12/12/24 17:00 GMT |
| Outcomes notice | 17/12/24 |
| Indicative service live date | 31/12/24 |

* 1. Submitting an Expression of Interest (EOI) – and a request to meet via tenders@chi.ac.uk

We have not set out any format for the submission of an Expression of Intertest, although ideally you will use this document to help shape the reasoning for why we might see you as a viable candidate. The formal submission of the (your) final version of this document will be required if any candidate wishes to be formally assessed.

Please note, simply sending in a ‘we express our interest’ is not necessarily good for you, or us. Please only do so if you genuinely believe you can meet the requirements. We will of course be looking particularly at your company’s visibility in the HEI sector, before considering whether to meet with you.

An EOI identifies to us that you would like to meet with us. Meetings are not in any way compulsory, and you are of course quite at liberty to submit a tender (or not) whether you have met with us or emailed us an EOI. Where we do meet, to retain fairness, we use a scripted process for any such meetings, and we will add any materially relevant questions and their answers to the Q&A section of our tendering website.

Please note however that it would be helpful if you can get in touch with us **as soon as possible**, if you consider that you have a product offer and track record that meets the requirements, with at least some initial evidence that satisfies the evaluation criteria. Please contact us with details via email to [tenders@chi.ac.uk](mailto:tenders@chi.ac.uk) The **final** date for making asking us to arrange a meeting is (**30/11/24 @ 17:00 GMT**).

* 1. Clarifications regarding the Invitation to submit an Expression of Interest

Any modification to the requirements by the University will be notified to participants, no less than 5 working days prior to the deadline. If appropriate, the University will revise the submission deadline to accommodate this.

Participants are expected to examine all instructions, questions, forms, terms and specification, and check they are complete in all respects. We will welcome any notification of any perceived ambiguity, inconsistency or omissions in our documents or the process we have set out and we will communicate corrections through the Q&A on our tendering website.

Participants are responsible for submitting a meaningful proposal, related to the stated requirements and evaluation criteria. This should include indicative pricing, expressed in £Sterling, exclusive of VAT.

Participants may withdraw their Expression of Interest at any time.

The University reserves the right to reject submissions received after that deadline and disqualify any submission that is incomplete or does not provide adequate functional and commercial detail. The University reserves the right to cancel the market evaluation exercise at any point. The University will accept no liability for any losses caused by any cancellation of this procurement exercise.

Participants shall bear their own costs and expenses incurred in the preparation and submission of their Expression of Interest, tender and any applicable site visits or presentations. The University will in no case be responsible or liable for those costs, regardless of the outcome in relation to this procurement project.

* 1. Evaluation of Submissions

The University will evaluate Tender Responses, for technical and commercial merit.

* 1. Evaluation Criteria

|  |  |  |  |
| --- | --- | --- | --- |
| **Tender Evaluation Criteria** |  | **Sub Criteria** | **Weighting** |
| Satisfactory details of the product and proposition for its delivery | A | The information must be accurate and relevant and must address the requirements in context for the University. | Pass/fail |
| Supply Chain Risk Management | B | Clear demonstration of Minimum Security Standards, and throughout the Supply Chain | Pass/fail |
| Partnering Arrangements | C1 | Whether directly as a consortium, all aspects of the service must be offered within a single contracting relationship. (See section 1.13 below) | Pass/fail |
| Business Continuity | D1 | Coherent explanation of implementation of product(s) that achieve the functionality of the Firewall | Pass/fail |
| D2 | Adoption of existing services, and Integration with existing systems | 10% |
| D3 | Migration of current and archive data / operation | 10% |
| Organisational experience and capability | E1 | Industry Knowledge (Standards, and suppliers) | 5% |
| E2 | Identifiable as operating in partnership with other HEIs in similar context | Scale and context may be pass/fail |
| E3 | Is, or has a coherent relationship with a member of the NCSC Cyber Incident Response providers. | Pass/Fail |
| E4 | Adherence to UK Data Protection Legislation and the Minimum Security Standard (see Appendix 2) | Pass/Fail |
| Finance and Commercial | F1 | Availability through a procurement framework that is available to UK HEIs | For information only |
| F2 | Costs and Value for Money (VFM) – EG Banding | 30% |
| F3 | Installation costs |
| F4 | System licensing (e.g. Banding to number of Students) |
| F5 | Hosting requirements and costs |
| F6 | Annuities and support costs / payment scheduling |
| Functional Specification | G1 | Must be a coherent, complete solution that meets the range of functions described in appendices | Pass/fail |
| G2 | Clarity of functions/components | 25% |
| G3 | Clarity of safeguarding functions (e.g. Site filtering) |
| G4 | Component interoperability |
| G5 | Download and patching |
| G6 | Legislative compliance and reporting |
| G7 | Functional and security release management |
| G8 | Interoperability with protective security systems |
| G9 | Management of local and remote access |
| G10 | Ability / process for responding to incidents |
| Environmental Sustainability | H | Demonstrable calculations of CO2e, and Carbon Zero planning in system, and other company activity | 10% |
| Compliance with the Social Value Model | I | See appendix3 for details | 10% |

* 1. How the University assesses a tender

All submissions are assessed independently by each of a range of stakeholders from the service areas concerned and from the commercial, IT and legal experts from within the University.

A shorthand of scoring method is used to summarise the confidence each assessor has in each submission’s explanations in relation to the 9 factors (and 28 sub factors in total) set out in section 1.12. This comprises of a marking and assessment check-sheet that is summarised to each of the 28 areas as being:

* Clear, relevant - adds value
* Clear, relevant
* Acceptable
* Limited
* Does not clearly identify
* Does not meet

These factors are calculated using the weightings shown in section 1.12. These are aggregated across assessors, and where there is deviation of 1 (+or-) between assessors, this is reviewed and quality assured.

All assessors are highly experienced and recognise that different or unfamiliar does not mean better or worse, however, it is important to recognise that assessors will only assess what is submitted, they can make no assumptions for information not present, or that is overly novel in its application. Assessors do not follow URLS in documents, do not search company websites and are instructed not to attempt to interpret generic brochure ware.

* 1. Consortia and Subcontracting

We have placed no specific limitation of the composition of any participant, excepting that we anticipate one cohesive, single, supply contract. We do however draw attention to the requirements of seamless operation, the Supply Chain Risk Management Strategy, and the ubiquity of the Minimum Security Standard.

Where a consortium or sub-contracting approach is proposed, information should be provided in your submission in respect of the consortium members who will play a role in the delivery of the requirement. The submissions must enable the University to assess the overall consortia and its net product.

* 1. Confidentiality and Freedom of Information

All market testing and procurement documentation, and any correspondence are treated as strictly confidential. However, the University is subject to UK Data Protection Legislation, and the Freedom of Information Act 2000.

This means that the University can be asked to disclose (for example) procurement and contracting information. Please indicate any areas of your submission that you consider should be exempted from any disclosure requests and identify why they should not be disclosed.

1. Some General Questions

There is no limit or word count for the questions, but please bear in mind the need for clarity etc. Please also pay attention to the assessment criteria set out in Section 1.12, and the notes set out in the appendices. We welcome you sharing your company’s strengths, in our context, but please do recognise our specific aims, and be prepared to explain why a particular technology, or services that you might propose is advantageous for the University.

1. 1. General service and cost questions

|  |  |  |
| --- | --- | --- |
| 1 | Please illustrate the Architecture of your solution | Criteria D1, D2, G(all) |
| e.g. Ideally, please offer us a simple graphic of the solution | | |

|  |  |  |
| --- | --- | --- |
| 2 | Please describe the adoption and evolution of hardware for your solution | Criteria D1, D2, F5, |
| e.g. Please identify how you would adopt the existing PA-3250s and please give an example of the hardware you might expect us to purchase (for example PA-3400 series) – over time.  e.g. Please identify what would be the trigger criteria for the need to invest in updated hardware | | |

|  |  |  |
| --- | --- | --- |
| 3 | Please identify the underlying operating system (E.G. Palo Alto) and how it is accessed – ideally with screen grabs to illustrate core functionality for operational (reporting and alerting). Please identify resilience and support | Criteria E2,D3,G1,G2 |
|  | | |

|  |  |  |
| --- | --- | --- |
| 4 | Please describe the source and maintenance of global threat and block lists | Criteria E3, E4, G6, |
|  | | |

|  |  |  |
| --- | --- | --- |
| 5 | Please describe your safeguarding facilities - i.e. ability to filter, log and alert on user activity at a personal / device level | Criteria E4, G3, |
| e.g. Please identify the data retention and management mechanism – NB, our requirement is to retain 12 months of log data – whether by reporting available to the FW, or off-line data export for archival analysis. | | |

|  |  |  |
| --- | --- | --- |
| 6 | Please describe how you ensure the security of our data | Criteria E4, G8, G9 |
| NB, Please refer to the Minimum Security Standards, and any security accreditations you hold | | |

|  |  |  |
| --- | --- | --- |
| 7 | Please describe how you ensure the integrity of privileged access | Criteria G2, G8, G9 |
| e.g. Please describe how access is managed and monitored for on-site University staff, and for remote access for support. | | |

* 1. Organisational experience and capability

|  |  |  |
| --- | --- | --- |
| 8 | Please describe any similar organisations to the University, that you are involved with, and aspects of your service you feel are particularly advantageous. | Criteria E1, E2 |
| e.g. Ideally, we’d like you to identify Universities that are reference sites for your company | | |

|  |  |  |
| --- | --- | --- |
| 9 | Please describe how you have transitioned a customer’s service from an incumbent supplier, whilst maintaining services. | Criteria D3, F3, |
|  | | |

|  |  |  |
| --- | --- | --- |
| 10 | Please describe how you monitor and respond to any service incidents | Criteria G9, G10 |
| e.g. on-call, emergency and routine maintenance services | | |

|  |  |  |
| --- | --- | --- |
| 11 | Please describe how you can avoid and respond to any breach of the firewall (Zero day events for example) | Criteria E3, G10, |
| e.g. on-call, emergency // NCSC etc and routine maintenance services | | |

* 1. Compliance with the Social Value Model

|  |  |  |
| --- | --- | --- |
| 11 | Please tell us something about you and your organisation, for example in relation to themes of the Social Value Act. (please also see the 17 UN Sustainable Development Goals) | Criteria I |
| See criteria in Appendix 1   * Tackling Economic Inequality * Fighting Climate Change * Equal Opportunities * Wellbeing | | |

|  |  |  |
| --- | --- | --- |
| 12 | The University is committed to sustainability – please tell us what your company / solution is doing to identify and minimise environmental impact. | Criteria H |
|  | | |

|  |  |  |
| --- | --- | --- |
| 13 | Skills | Criteria I |
| e.g. Ideally, we’d like to hear about your commitment and successes in training, apprenticeships and staff development. For example, is there potential for you to collaborate in our Engineering or Computing offer | | |

|  |  |  |
| --- | --- | --- |
| 14 | Please use this section to describe any other add-ons or add-value services which can be provided and sets you apart from other providers. | Criteria I |
|  | | |

1. Costed Proposal

Please set out your plan, design, and costs assuming transition to enable us to meet our aims.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Your proposal – 3 years   |  |  |  |  | | --- | --- | --- | --- | |  | Year 1 | Year 2 | Year 3 | | Equipment update |  |  |  | | Licensing / subscriptions |  |  |  | | Support |  |  |  | | Any other fees |  |  |  |   Notes  Please include a copy of your standard Ts and Cs, |

Alternatives

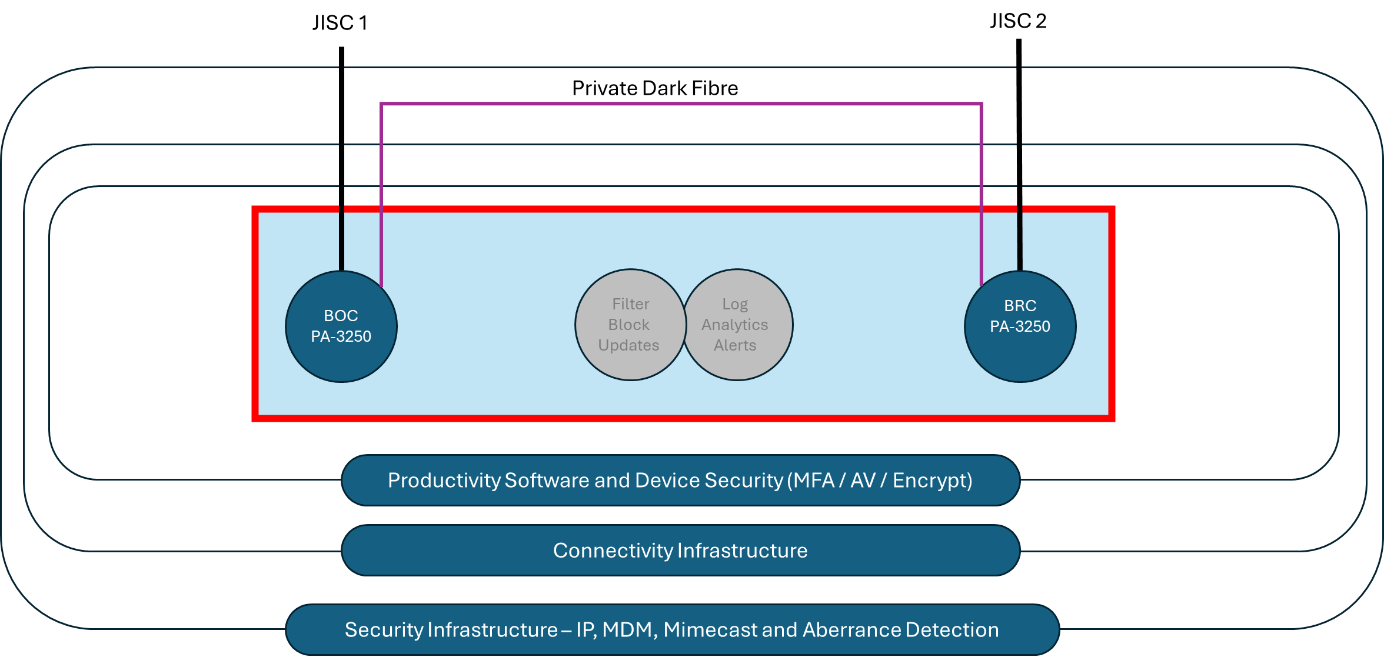
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Your proposal – 5 years   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | | Equipment update |  |  |  |  |  | | Licensing / Subscriptions |  |  |  |  |  | | Support |  |  |  |  |  | | Any other fees |  |  |  |  |  |   Notes  Please include a copy of your standard Ts and Cs, |

Appendix 1: Contact Details

Please set out the names / contact details for the people you want to be included in any correspondence from the University. Please note as det out above, that no correspondence from your company in relation to this tender, should be sent elsewhere but to [tenders@chi.ac.uk](mailto:tenders@chi.ac.uk)

|  |  |
| --- | --- |
|  | Response |
| Contact name |  |
| Name of organisation |  |
| Role in organisation |  |
| Phone number |  |
| E-mail address |  |
| Postal address |  |

1. Appendix 2: The Firewall and its broad context
   1. Schematic of components and integrations



* 1. Firewall Services as-is

a) Equipment (current PA-3250) – Potential to upgrade to PA-3410 in 2025

b) Palo Alto Subscriptions

* Core security – Advance Threat Protection
* Advanced URl Filtering
* Advanced Wildfire[[1]](#footnote-2)
* DNS Security
* SD WAN

c) Support Services

* 08:00-18:00 Monday to Friday – Telephone Email and remote access support
* Weekend and Bank-holiday – ticketing
* On-line support portal
* Next day hardware ship
* Software releases (Major and Minor) and updates

Appendix 3: Social Value Model:

|  |  |  |
| --- | --- | --- |
| SVM Theme | SVM Policy Outcome | SVM Model Award Criteria |
| Tackling economic inequality | Create new businesses, new jobs and new skills[[2]](#footnote-3) | Effective measures to deliver any/all of the following benefits through the contract:   * Create opportunities for entrepreneurship and help new organisations to grow, supporting economic growth and business creation. * Create employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas, and for people in industries with known skills shortages or in high growth sectors. * Support educational attainment relevant to the contract, including training schemes that address skills gaps and result in recognised qualifications. |
| Increase supply chain resilience and capacity | Effective measures to deliver any/all of the following benefits through the contract:   * Create a diverse supply chain to deliver the contract including new businesses and entrepreneurs, start-ups, SMEs, VCSEs and mutuals. * Support innovation and disruptive technologies throughout the supply chain to deliver lower cost and/or higher quality goods and services. * Support the development of scalable and future-proofed new methods to modernise delivery and increase productivity. * Demonstrate collaboration throughout the supply chain, and a fair and responsible approach to working with supply chain partners in delivery of the contract. * Demonstrate action to identify and manage cyber security risks in the delivery of the contract including in the supply chain. * Demonstrate how you meet and maintain the Minimum Security Standard * Commitments to informing the University where there are changes in the supply chain, or changes that might affect maintaining security. * Commitments to liaising with the University in the event of a cyber attack |
| Fighting Climate Change | Effective stewardship of the environment | Effective measures to deliver any/all of the following benefits through the contract:   * Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions. * Influence staff, suppliers, customers, and communities through the delivery of the contract to support environmental protection and improvement. |
| Equal opportunity | Reduce the disability employment gap | Effective measures to deliver any/all of the following benefits through the contract:   * Demonstrate action to increase the representation of disabled people in the contract workforce. * Support disabled people in developing new skills relevant to the contract, including through training schemes that result in recognised qualifications. |
| Tackle workforce inequality | Effective measures to deliver any/all of the following benefits through the contract:   * Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce. * Support in-work progression to help people, including those from disadvantaged or minority groups, to move into higher paid work by developing new skills relevant to the contract. * Demonstrate action to identify and manage the risks of modern slavery in the delivery of the contract, including in the supply chain. |
| Wellbeing | Improve health and wellbeing | Effective measures to deliver any/all of the following benefits through the contract:   * Demonstrate action to support health and wellbeing, including physical and mental health, in the contract workforce. * Influence staff, suppliers, customers, and communities through the delivery of the contract to support health and wellbeing, including physical and mental health. |
| Improve community integration | Effective measures to deliver any/all of the following benefits through the contract:   * Demonstrate collaboration with users and communities in the co-design and delivery of the contract to support strong integrated communities. * Influence staff, suppliers, customers, and communities through the delivery of the contract to support strong, integrated communities. |

Appendix 4: Minimum Security Standards

Minimum Security Standards – General Guidance

1. **Introduction**
   1. The University of Chichester (“University”) is committed to high standards of data quality. In addition to its statutory obligations, and standards set by itself and its auditors for value, security, and ethicality etc, the University’s clients set out conditions that the University must demonstrably meet and maintain. These conditions include that the University must assure standards in the entirety of the University’s supply chain.
   2. The University’s policies, and procedures refer to the Supply Chain Risk Management Strategy (SCRMS) that describes the supply chain’s roles and responsibilities in maintaining a secure environment for information. The University’s SCRMS is established in accordance with the international standard ISO27001 (2022).
   3. The SCRMS requires the University to establish, maintain and monitor its contractual relationships using a set of standards that are familiar and auditable by the University’s regulators, and clients.
   4. This document supports the SCRMS by describing the Minimum Security Standard (MSS) and provides guidance for where the MSS will be a factor of procurement, contract forming, contract maintenance, partnerships that share data and for the security of data where a contract or partnership comes to an end.
2. **Minimum Security Standards**
   1. The SCRMS requires that in the context of any procurement and supply that involves information, that Minimum Security Standards (MSS) are established and maintained.
   2. The SCRMS is applied to all new procurements and partnerships, including for a renewal of an existing contract, as well as (where possible) for updating existing contracts that are part way into their term.
   3. The Minimum Security Standard element of the SCRMS is particularly relevant to any systems, services or processes that acquire, create, adapt, or store University information.
   4. The Minimum Security Standard relating to any supplier, system or process is proportional to the risk. Information at the University is in summarised form, classified as:
      1. Public which does not identify people and has no particular intellectual property or copyright value,
      2. Private, which means there is intellectual, commercial, contractually valuable business information that does not contain personal identifiers or other information relating to people,
      3. Confidential, is information relates to people, their personal identifiers, sensitive personal information, and to data that is classified as protected characteristics in the Data Protection Act,
      4. Unauthorised (which is actively monitored for an removed)
   5. Establishing the proportional and appropriate Minimum Security Standard includes reference to the classification of information involved.
   6. The SCRMS requires that the Minimum Security Standard is maintained, relative to the prevailing risks, and the prevailing classification of any information, throughout the whole life of the contact, licensing, or partnership agreement, including throughout where such agreements end.
3. **Demonstration of the Minimum Security Standard (University)** 
   1. The University must be able to demonstrate that it meets the Minimum Security Standard stipulated by its client’s partners, regulators and stakeholders, including in the entirety of the University’s supply chain.
   2. The University achieves this through audited documentation, and compliance with standards, including for example PCIDSS, Cyber Essentials and ISO27001 (2022). The University’s compliance is audited and where possible is supported by external verification and relevant certification.
   3. As part of maintaining the evidence of its overall compliance with the standards, the University must establish and monitor the achievement of the Minimum Security Standard, with all of its suppliers.
4. **Demonstration of the Minimum Security Standard (Suppliers and Partners)** 
   1. Establishing and monitoring that suppliers and partners apply a Minimum Security Standard will occur during the procurement or creation of supply agreements, contracts, and partnership agreements, and through periodic review thereafter.
   2. In procurement, this explanatory note, and the processes for how to communicate, consult and assess the proportionality is built into the University’s procurement processes. These processes reflect the practices and guidance set out by the Crown Commercial Service and complies with the Public Contracts Act 2015.
   3. In partnership forming the same rationale and dialogue relating to Minimum Security Standards is undertaken and is often a two way agreement to meet each other’s respective Minimum Security Standards.
   4. In commodities purchasing (for example software), it may be difficult to persuade a supplier to adopt the University’s Minimum Security Standard, especially where their design and terms are global. However, if after undertaking a Data Protection Impact Assessment, the product, system, or service cannot achieve the Minimum Security Standard, even though additional supplementary processes and oversight, the product system or service will not be used.
   5. If the MSS is not maintained, a contract may be suspended, and in extremis, terminated.
5. **Recognised Standards**
   1. Demonstrating the Minimum Security Standard can be satisfied by evidence of for example where an organisation already has institution wide ISO27001 and PCIDSS (where relevant), If these are certificated, then it can be accepted that this supplier / partners meets the University’s (and the University’s stakeholders) highest requirements.
   2. By proxy, a supplier’s ISO27001, supports the University’s own compliance with ISO27001, and provided these are monitored and maintained, this will (in most cases) satisfy the University’s partners and clients.
   3. The questions and considerations of a proportional Minimum Security Standard may therefore include, that the supplier (or partner) can demonstrate that they have:
      1. ISO27001
      2. PCIDSS
      3. Cyber Essentials, or Cyber Essentials plus in relation to the supplier and its supply chain.
      4. Cyber Essentials, or Cyber Essentials plus in relation to the specifics of the supply
   4. In considering some form of supply or partnership, the University will undertake the Data Protection Impact Assessment (DPIA) screening questions and will consider if a full DPIA is required.
   5. The University will consider the specificity of any electronic / digital connectivity and the respective access and encryption, and aberrance and the infiltration and exfiltration detection controls involved.
   6. It is also essential that SCRMS Standards are maintained, and ant contract or partnership agreement will therefore consist of periodic review, and agreement for if some sort of incident occurs. These agreements and contracts will therefore consist of commitments to:
      1. Consult with the University if any of the Suppliers supply chain changes that affect the security in the supply of goods of services to the University.
      2. Consult with the University if there are any changes to the risks of cyber-attack across the Supplier’s supply chain.
      3. Consult with the University in the event of any suspected cyber-attack in any aspect of the supplier’s supply chain, with adequate notice such that the University can meet its statutory obligations to notify regulatory bodies, its staff, and customers where applicable.
6. **Periodic review**
   1. To ensure that the Minimum Security Standard for the supply/partnership is relevant to current risks, then this will be considered within the periodic contract performance reviews (commonly, annually).

Appendix 5: Supply Chain Risk Management Strategy

Supply Chain Risk Management Strategy – General Guidance

1. **Policy Statement**
   1. It is the policy of the University of Chichester (“University”) to maintain a supply chain risk management strategy, that supports related information security policies and procedures that in the round comply with the prevailing published standards designed to ensure security and best value, including for where such standards are integral to working with partners and other agencies.
   2. The purpose of this Supply Chain Risk Management Strategy is to:

* demonstrate the University’s supply chain control processes in the context of ISO27001,
* describe the University’s commitment to the ISO27001 standards based framework, and how this involves the various University suppliers in maintaining information security, and;
* enable regulator and partner insight into the integrity of the University’s policies, procedures, and operation.

1. **Introduction** 
   1. The Supply Chain Risk Management Strategy (SCRMS) sets out how 3rd party suppliers and the University work together, in line with the prevailing published standards to safeguard the security of information.
   2. A Supply Chain Risk Management Strategy (SCRMS) is relevant to the entirety of the operation of the University, across a regularly changing and diverse range of workflows, each in its own lifecycle. The University’s SCRMS is constructed to meet the requirements of the International Standard ISO27001 (2022), whilst also incorporating the guidance set out by the UK’s National Centre for Cyber Security. The University’s SCRMS is therefore designed to be recognisable to regulatory agencies, and to the wide range of organisations the University might work with.
   3. Almost no transactions take place in the University without direct or indirect links to the interconnectedness of modern technology, and hence SCRMS is considered holistically, as well as at a process and supplier level.

**SCRMS: Principle 1 Understand what needs to be protected and why**

The University has a clearly mapped IT ecosystem, using best of breed security throughout. The University maintains a detailed Corporate Systems Database. Any new or altered system that acquires, creates, processes, or stores personal identifiers, or other identifiable information, should be assessed using a Data Protection Impact Assessment (DPIA) screening questions to determine whether a DPIA is required, before being actioned.

**SCRMS: Principle 2: Knowing who our suppliers are and building an understanding of what their security looks like**

The University maintains a Contracts Database and supplier logging in its Financials System. The Supply Chain, and the Corporate Systems Database correspond. The DPIA is ubiquitous, irrespective of whether the information is maintained on or off campus and refers to the mechanisms for accessing information, including through supplier statements and expert assessments of how they meet and maintain the University’s formalised Minimum Security Standard. The University’s contract terms and conditions require all suppliers to notify the University of any supply chain changes or, environmental risks, and expressly in the event of any compromise to their security.

**SCRMS: Principle 3: Understanding the security risks posed by our supply chain**

The IT Ecosystem has in-built security for devices, access, networks, and connections, and a range of aberrance detection and containment mechanisms. The University undertakes a range of security monitoring and establishes in its contract terms and conditions that all suppliers must notify the University of any changed suppliers in their own operation and any changed technologies or risks. Specifically, all suppliers are contractually bound to monitor access, and engage the University should any cyber-attack be suspected. Data integrity, retention and disposal are established, along with the commitment to return data, and, or demonstrate certificated cleansing at the end of any contract.

**SCRMS: Principle 4: Communicating our view of security needs to suppliers**

The University’s Financial Regulations sets out the mandatory approach to procurements, supported by defined processes, and templated documentation. Where there is to be any personal information or identifiers involved in the service provided by the supplier, the documentation sets out how the DPIA, if required, is undertaken, and includes the University’s guidance on, and requirements for maintaining Minimum Security Standards.

**SCRMS: Principle 5: Set and communicate minimum security requirements for our suppliers**

The Minimum Security Standard is a formal document used in procurement and contract forming. This sets out the expectation that suppliers will be able to demonstrate their certified compliance with relevant standards (typically, ISO27001 Cyber Essentials and PCIDSS), or be able to demonstrate equivalent integrity. The Minimum Security Standard can be proportional to the risks involved in the supply or goods or services but is fixed in that supplier must commit to notify and engage with the University if the data, or risks change, and in the event of any compromise such as a cyber-attack.

**SCRMS: Principle 6: In-built security considerations in our contracting processes**

The prevailing, proportional, assessment of risks is established in the University’s Business Case Templates, and subsequently within the procurement templates and supplier assessments (which includes the DPIA, if required) before being formalised in the Contract Terms and Conditions. In addition to the contractual commitment to notify the University of any changes to subcontracting, risks and promptly of any suspected incident, the Contract Terms and Conditions also set out the Contract Performance Review (CPR) Process. This ensures a structured periodic review to assess any prevailing risks, including a review of the DPIA (if undertaken), and the Minimum Security Standard.

**SCRMS: Principle 7: Meeting our own security responsibilities as a supplier and consumer**

The University has been assessed at least annually through internal and external audit, and with further scrutiny through for example insurance and external partner audits undertaken on the University. In addition to the due diligence undertaken on the University by its partners, the University has Cyber Essentials Certification for certain activities, and has PCIDSS in all relevant activities. In 2023, the University has begun the full implementation of ISO27001, and expects to be fully certified in 2024.

**SCRMS: Principle 8: Raising awareness of security within our supply chain**

The University often works within frameworks of supply and subscribes to a wide range of industry and professional bodies monitoring of risks. The University takes seriously its own responsibilities to monitor for, and report risks, and has a range of mechanisms to enable this to happen, both at an IT level, but also at a ‘user’ level. The University’s configuration and risk avoidances incorporate the common professional mechanisms, and the University has mandatory data proception and cyber-risk awareness training, with assessments, and for example testing for resilience to phishing.

All tendering and contracting incorporate the DPIA screening questions and template and the guidance on Minimum Security Standards. This SCRMS document is an additional resource that is made public, as is the University's commitment to the relevant security accreditations and standards.

**SCRMS: Principle 9: Providing support for security incidents**

Like most organisations, the University makes every effort to design out, and avoid information security issues. The University has established automated monitoring, detection and notification processes, well publicised guidance, and regularly communicated requests that all stakeholders will report anything unusual. In addition to the automated process, there is a 24/7 facility to investigate anything that is detected or notified.

Support also consists of written procedures, backed by regular scenario and full disaster testing, and covering all individual and shared assets, all information collections and all connections to clients and other agencies. These are recorded in the University’s Serious Incident Handling Procedures, which also identify supplier, regulatory and any relevant police, civil or other relevant authority, as well as the communication strategy if any event were to occur.

**SCRMS: Principle 10: In-built assurance activities in our supply chain management**

Robust assurances are built in at the point of contracting which includes the commitment to Contract Performance Review. This is underpinned by the University’s commitment to relevant standards, and audit oversight that monitors and reviews that the activities are adequate in design and application.

**SCRMS: Principle 11: Encouraging the continuous improvement of security within the supply chain**

The University maintains audited standards, and these include the review of the mechanisms within, and application of these throughout the acquisition, maintenance and exit of each of the individual supplier contracts and agreements.

The Contract Performance Review Process is a collaborative process to ensure that the prevailing risks are considered in relation to how the suppliers' goods and services are affected by any risks, and any improvements that can be made. Suppliers are committed in contract to notify of any supply chain alteration, and the collaborative nature of the University’s approach to contract performance includes two-way ideas sharing to assess opportunities for continuous improvement.

**SCRMS: Principle 12: Building trust with suppliers**

The University applies a standards-based approach and applies the inwards scrutiny of orthodox methods that are used in Higer Education and more widely. The approach incorporates all legal obligations and is supported by documented processes and guidance. The Minimum Security Standard is applied proportionally to the circumstances, and the University takes pride in being an active partner with its suppliers in achieving mutual goals. In return, The University values an ongoing dialogue, in which there is two-way, up-to-date understanding of the interaction between the supply chain, the University and the University’s customers.

1. https://www.paloaltonetworks.com/network-security/advanced-wildfire [↑](#footnote-ref-2)
2. The University will welcome the opportunity to develop degree apprenticeships, internships and placements, Continuous Professional Development, as well as collaborative programmes and career pathways with suppliers. [↑](#footnote-ref-3)