

**Tender**

Wireless and Internet

Student Accommodation

The University of Chichester

**Latest date for Return – 31/05/24 12:00 GMT**

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 LaneChichesterWest SussexPO19 6PE | Telephone:Date:Revision:Email | 01243 81600013/05/20241.0 FinalTenders@chi.ac.uk  |

**Contents**

[0 Introduction 1](#_Toc166485626)

[0.1 Background to this tender 1](#_Toc166485627)

[0.2 High level requirements 1](#_Toc166485628)

[0.3 Further guidance to bidders 1](#_Toc166485629)

[0.4 Seeking clarification 2](#_Toc166485630)

[0.5 Procurement timetable 2](#_Toc166485631)

[0.6 Submission details 2](#_Toc166485632)

[0.7 Assessment criteria 3](#_Toc166485633)

[0.8 Confidentiality and Freedom of Information 3](#_Toc166485634)

[1 Contact Details and Declaration 4](#_Toc166485635)

[2 General Questions 5](#_Toc166485636)

[2.1 General service and cost questions 5](#_Toc166485637)

[2.2 Organisational experience and capability 6](#_Toc166485638)

[2.3 Compliance with the Social Value Model 6](#_Toc166485639)

[3 Costed Proposal 7](#_Toc166485640)

[3.1 Scenario 1: Combined operational fees, (on refresh of technology) 7](#_Toc166485641)

[3.2 Scenario 2: as per Scenario 1, but with pre-investment of IRO £100,000 7](#_Toc166485642)

[3.3 Scenario 3: as per Scenario 1, but with pre-investment of IRO £200,000 7](#_Toc166485643)

[Appendix 1: Supporting Information: Social Value Model: 9](#_Toc166485644)

[Appendix 2: Supporting Information - Minimum Security Standards 12](#_Toc166485645)

[Appendix 3: Supporting Information: Supply Chain Risk Management Strategy 14](#_Toc166485646)

[Appendix 4: Current Service (As-is) 17](#_Toc166485647)

[Appendix 5: Revised Service – Illustration (To-be?) 18](#_Toc166485648)

1. Introduction

The University of Chichester’s student accommodation is situated on its two Campuses, and at the off-campus locations of Stocksbridge and Fishbourne. These comprise of around 1200[[1]](#footnote-2) rooms in purpose built blocks of various sizes. The accommodation is provided with internet access, hard-wired to rooms and communal areas, and with WiFi throughout. The existing provision makes use of the University’s inter-campus dark fibre connection, which with 40GPS, has adequate capacity for the foreseeable future. The incumbent provider has installed fibre to the Chichester Campus and has separate fibre connectivity to the off-site residences.

Over recent years that University has been considering a long term Design, Build, Finance and Operate approach to its accommodation. This could include the provisioning of services, however in the shorter term, the University’s term contracts for internet services are coming to an end, and the University is seeking to renew its provision. Although a technology refresh may be phased, the existing contractual term ends on 30/6/24 and hence the new contracting arrangements and service continuity is essential from 01/07/24. An inventory of the requirement is set out in this document, and this identifies that some of the equipment and services are reaching their end of life, and we anticipate a partial or full technology refresh.

Key criteria (allowing for a range of options) can be considered for the next period of provision, however, please note that the requirement includes that there must be potential to novate part[[2]](#footnote-3) or all of the contract at some future point.

Peak capacity is operating at between 1&2GB, and the expected growth is 20-30% per annum. Halls of Residence are in intensive use, peaking in the evenings. When not in use for Students, the Halls of Residence are used for conference and ‘bed and breakfast’ commercial guests. Consequently, the services required are 24/7/365.

Our vision includes that our provision must be able to cater for the developments we expect (over time) as we invest in localised room management, (monitoring heat/locks/lights) and to enable the increasing range of devices (Gaming consoles, voice based assistants and Internet of Things – IoT).

* 1. Background to this tender

Periodically we are required to market test and ensure the best value. To do this fairly, with the widest competitive approach this tender is published through the tendering site (Contractsfinder[[3]](#footnote-4)). Our aim being to establish a preferred supplier, to enable us to maintain and develop our estate.

The purpose of this tender is to enable suppliers to demonstrate expertise and compliance with the University’s requirements, and to enable the University to assess the most economically advantageous solutions to its requirements, using the prescribed tendering methodology for requirements of this size and nature.

* 1. High level requirements

Appendices 4 & 5 give a list of equipment that is distributed across our estate.

* 1. Further guidance to bidders

Although primarily funded by student subscriptions, the University is classified as a Public Service. Consequently, all procurement must meet the conditions of the Public Contracts Act 2015, and the corresponding guidance set out by the Crown Commercial Service[[4]](#footnote-5).

There is some flexibility in how this is applied, and the University has chosen to defer the rigors of the ‘Standard Selection Questionnaire’[[5]](#footnote-6) (SSQ) to the later pre-contracting stage of the procurement process, and to only apply this to candidates we have progressed from their initial tender. It is of course clear that if you cannot meet the criteria of SSQ then it will ultimately lead to your tender being rejected. It is helpful if you therefore familiarise yourself with what this might entail.

We draw your attention to the expectation that you must demonstrate support for the Modern Slavery Act, the Social Values Act, and that you have robust policies and processes in relation to sustainability throughout your operation and its supply chain.

The University has a Supply Chain Risk Management Strategy (SCRMS), (See Appendix 3) which is required to satisfy current and future clients that we maintain clearly defined standards. Recently, this has focused on cyber risks, and the need for the entire supply chain to meet the Minimum Security Standard (see Appendix 2). The MSS is ideally underpinned through key partners maintaining accreditations such as ISO27001, Cyber Essentials and where relevant, the Payment Card Industry Data Security Standard (PCIDSS)

Please note, it is important in helping us understand fairly, your capabilities and service strengths alongside those of others. We have set out a questionnaire (section 2) and asked for costed scenarios (Section 3) that we ask that you use to enable this. Ordinarily, we would be unlikely to sift through brochures, or follow links to web pages etc.

* 1. Seeking clarification

For all queries, please contact us by email tenders@chi.ac.uk. Please note that during the tender period you must not contact University staff directly and avoid any related discussion if you happen to be working with us in some other capacity, as this might be considered canvassing, and in which case the University might need to exclude your organisation from the tender 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 may be circulated through our tendering web page.

* 1. Procurement timetable

The procurement project is working to the following timescale:

|  |  |
| --- | --- |
| Stage | Key Dates |
| Publication of Tender Notice  | 13/05/2024 |
| Closing Date for submission of this Selection Questionnaire | 31/05/2024 |
| Clarifications  | Up to 10 days from publication  |
| Confirmation of Outcome to this Selection Questionnaire | c20 days from the closing date  |
| Pre contracting due diligence and appointment notice  | c10 days from the award notice  |
| Award Notice (via Contractsfinder) |  Appointment Notice +10 Days |
| Service live date  | 01/07/24 |

* 1. Submission details

There is no need to notify the University with your ‘Expression of Interest’ as all tender documents, Questions and Answers are open to all bidders. But please do send your completed submission, including contact details in Section 1, and signature to Section 4, to the University by the closing date (31/05/24 @ 12:00 GMT mid day), to tenders@chi.ac.uk.

Please note, we **do not** accept submissions via file transfer sites. Tenders@chi.ac.uk accepts emails and attachments of up to 35MB and it is acceptable to submit in more than one email.

* 1. Assessment criteria

The objective of the questionnaire attached is to identify suitable suppliers. All submitted tenders are assessed by a panel, whose evaluation will be quality assured. The University intends to award any contract based on the most advantageous offer.

|  |  |  |
| --- | --- | --- |
| **Tender Evaluation Criteria** | **Sub Criteria** | **Weighting** |
| Satisfactory completion of the Questionnaire | The information must be accurate and relevant | **Pass/fail** |
| Ability to meet timescales  | Service continuity from 01/07/24 | **Pass/fail** |
| Allow for evolution in the contracting body  | Supportive of a potential to novate the contract, to the University’s Accommodation Management Partners if/when required. | **Pass/fail** |
| Organisational experience and capability  | Industry Knowledge | 10% |
| Ability to support Prevent and Safeguarding | 10% |
| Adherence to UK Data Protection Legislation | 10% |
| Financial Position | Costs and Value for Money (VFM) | 20% |
|  | Coherent offer of a capital absorption to amortise renewal costs as revenue cost.  | 10% |
| Technical and Professional capability | Provision of relevant case studies, CVs of key support and liaison staff and demonstration of skills to deliver the service required | 10% |
|  | Demonstrable Customer Satisfaction – backed by end user satisfaction  | 10% |
| Environmental Sustainability | Demonstrable awareness, and clarity of how supplier monitors the environmental damage, in and through its activities.  | 10% |
| Compliance with the Social Value Model | See Section 2, and appendix 1 for details  | 10% |

From the proposals submitted, if there is no clear organisation whose value needs the criteria better than others, then there is potential for the University to offer an interview process for clarifications. Subsequently the leading organisation will be asked to submit further details to support the contracting element of the procurement.

|  |  |  |
| --- | --- | --- |
| **Pre Contract Evaluation Criteria** | **Sub Criteria** | **Weighting** |
| Satisfactory compliance with the Crown Commercial Service’s (CCS) Standard Selection Questionnaire (SSQ) | The information must be accurate and relevant and must suitably set out how any of the criteria for exclusion does not apply.  | **Pass/fail** |
| Submission of further evidence, for example, satisfactory statements relating to the Modern Slavery Act, and Supply Chain Sustainability.  | The information must be accurate and relevant | **Pass/fail** |

* 1. Confidentiality and Freedom of Information

All tendering documentation and 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 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.

Please note that from October 2024, the University will be required to comply with the Public Procurement Act (2023), which requires routine openness and disclosures about any procurements.

1. Contact Details and Declaration

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

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

1. 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 0.7, and the inventory (as-is) set out in Appendix 4. We have set out an illustration of what we think a ‘to-be’ solution might consist of in Appendix 5 having deliberately avoided stipulating any specific manufacturer. It is important however that you can (as set out in the assessment coterie) show that you a reliable supply chain, and that you can explain why a particular technology that you might propose is right for the University.

* 1. General service and cost questions

|  |  |
| --- | --- |
| 1 | Please describe the Architecture of your solution  |
| The current architecture relies on the University’s intersite (private campus to campus dark fibre) at no additional cost to the provider. Although currently utilising only 1Gbps, this can be increased within the overall capacity of 40Gbps. This allows for the provider to connect their own fibre to just one campus (BOC in the current case). Fishbourne, and Stocksbridge are separate, dedicated fibre connections from the current provider.  |

|  |  |
| --- | --- |
| 2 | Please describe what (if any) infrastructure you require from the University  |
| I.E., continued reliance on the collection of fibre to the campus data centres, and use of the Intersite fibre.  |

|  |  |
| --- | --- |
| 3 | Please describe your approach to additional Services we require - BMS |
| The University may require some access to enable building management and other services such as the payments for laundries, localised environmental monitoring, CCTV lift alarms, electronic door locks etc. We expect to work in partnership on additional room level monitoring, and may therefore seek to enable local monitoring devices, that connect back to centralised facilities.  |

|  |  |
| --- | --- |
| 4 | Please describe your approach to additional services we require – E.g. SSIDs |
| To enable full convenient roaming, we currently enable Eduroam and our Guest service SSIDs across the providers networked (by way of two additional SSIDS’s backhauled) to the University. |

|  |  |
| --- | --- |
| 5 | Please describe your safeguarding facilities  |
| I.e. Under 18s, and for the prevention of extremism  |

|  |  |
| --- | --- |
| 6 | Please describe how you ensure the security of our data  |
|  |

* 1. Organisational experience and capability

|  |  |
| --- | --- |
| 7 | Please describe any similar organisations to the University, that you are involved with, and aspects of your service you feel are particularly advantageous.  |
| Ideally, we’d like you to identify Universities that are reference sites for your company  |

|  |  |
| --- | --- |
| 8 | Please describe how you have transitioned a customer’s service from an incumbent supplier, whilst maintaining services. |
| Our residences can be in service year round  |

|  |  |
| --- | --- |
| 9 | Please describe how you monitor and respond to any service incidents  |
|  |

* 1. Compliance with the Social Value Model

|  |  |
| --- | --- |
| 10 | 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) |
| See criteria in Appendix 1 * Tackling Economic Inequality
* Fighting Climate Change
* Equal Opportunities
* Wellbeing
 |

|  |  |
| --- | --- |
| 11 | Skills |
| 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  |

|  |  |
| --- | --- |
| 12 | Please use this section to describe any other add-ons or add-value which can be provided and sets you apart from other providers.  |
|  |

1. Costed Proposal

Please set out your plan, design and costs for the two scenarios below. Please tells us why as well as what.

* 1. Scenario 1: Combined operational fees, (on refresh of technology)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Your proposal\*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7  | Total |
| Cost ex VAT |  |  |  |  |  |  |  |  |
| Per bed  |  |  |  |  |  |  |  |  |

Notes |

* 1. Scenario 2: as per Scenario 1, but with pre-investment of IRO £100,000

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Your proposal – with an up-front investment of IRO £100,000

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7  | Total |
| Cost ex VAT |  |  |  |  |  |  |  |  |
| Per bed  |  |  |  |  |  |  |  |  |

Notes |

* 1. Scenario 3: as per Scenario 1, but with pre-investment of IRO £200,000

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Your proposal – with an up-front investment of £200,000

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7  | Total |
| Cost ex VAT |  |  |  |  |  |  |  |  |
| Per bed  |  |  |  |  |  |  |  |  |

Notes |

Appendix 1: Supporting Information: Social Value Model:

|  |  |  |
| --- | --- | --- |
| SVM Theme | SVM Policy Outcome | SVM Model Award Criteria  |
| Tackling economic inequality | Create new businesses, new jobs and new skills[[6]](#footnote-7) | 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 2: Supporting Information - 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 clients 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 a 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 it’s 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 others 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 through 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 suppliers 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 ensue 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 3: Supporting Information: 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.

Appendix 4: Current Service (As-is)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Property Location  | Bed Numbers | Switches  | Wireless APs | Connectivity  | Service Speed  |
| Bishop Otter Campus | 380 | 10/100 wired ports 10/100/1000 APs | 802.11 ACCisco 1702iCorridor Deployment  | 10Gbps to BT Chi Exchange | Up to 100MBS |
| Bognor Regis Campus | 226 | 10/100 wired ports 10/100/1000 APs | 802.11 ACCisco 1702iCorridor Deployment | 1Gbps dedicated VLAN on University link to BOC (can be increased)  | Up to 100MBS |
| Stocksbridge  | 405 | 10/100 wired ports 10/100/1000 APs | 802.11 ACCisco 1702iCorridor Deployment | 1Gbps to BT Chi Exchange | Up to 100MBS |
| Pinewood | 59 | 10/100 wired ports 10/100/1000 APs | 802.11 ACCisco 1702iCorridor Deployment | 1Gbps to University BOC | Up to 100MBS |
| Fishbourne | 134 | 10/100/1000 to all APs and outlets | 802.11 ACCisco 1815W and 1702iIn-Room Deployment  | 1Gbps to BT Chi Exchange | Up to 100MBS |

Appendix 5: Revised Service – Illustration (To-be?)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Property Location  | Bed Numbers | Switches  | Wireless APs | Connectivity  | Service Speed  |
| Bishop Otter Campus | 380 | Refresh to 10/100/1000 | 802.11 AXTBC[[7]](#footnote-8)Room Deployment  | 10Gbps to BT Chi Exchange | Gigabit  |
| Bognor Regis Campus | 226 | Refresh to 10/100/1000 | 802.11 AXTBCRoom Deployment  | 10Gbps dedicated VLAN on University link to BOC (can be increased)  | Gigabit |
| Stocksbridge  | 405 | Refresh to 10/100/1000 | 802.11 AXTBCRoom Deployment  | 1Gbps to BT Chi Exchange | Gigabit |
| Pinewood | 59 | Refresh to 10/100/1000 | 802.11 AXTBCRoom Deployment  | 1Gbps to University BOC | Gigabit |
| Fishbourne | 134 | Refresh to 10/100/1000 | 802.11 AXTBCRoom Deployment  | 10Gbps to BT Chi Exchange | Gigabit |

1. Within extant plans, this may grow to c1450 rooms over the period of this contract. [↑](#footnote-ref-2)
2. Plans are objective to the potentials to split the approach to on and off campus residences. [↑](#footnote-ref-3)
3. <https://www.contractsfinder.service.gov.uk/Search> [↑](#footnote-ref-4)
4. <https://www.crowncommercial.gov.uk/> [↑](#footnote-ref-5)
5. <https://www.gov.uk/government/publications/ppn-0323-standard-selection-questionnaire-sq> [↑](#footnote-ref-6)
6. 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-7)
7. Please specify your preference, and its justification / lifetime etc [↑](#footnote-ref-8)