

**Tender - Specification**

Door locks, and ‘key’ management system

The University of Chichester

**Submissions can be made now, and the final closing date is:**

 **12:00 (Mid-Day - GMT) 31/07/24**

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 81600024/06/20241.0 FinalTenders@chi.ac.uk  |

**Contents**

[0 Introduction 1](#_Toc170128792)

[0.1 The University’s estate 1](#_Toc170128793)

[0.2 Critical success factors 2](#_Toc170128794)

[0.3 Background to this tender 2](#_Toc170128795)

[0.4 High level requirements 2](#_Toc170128796)

[0.5 Further guidance to bidders 2](#_Toc170128797)

[0.6 Seeking clarification – Questions and Answers 3](#_Toc170128798)

[0.7 Procurement timetable 3](#_Toc170128799)

[0.8 Submission details 3](#_Toc170128800)

[0.9 Confidentiality and Freedom of Information 3](#_Toc170128801)

[0.10 Assessment criteria 4](#_Toc170128802)

[1 Contact Details and Declaration 5](#_Toc170128803)

[2 General Questions 6](#_Toc170128804)

[2.1 General service and cost questions 6](#_Toc170128805)

[2.2 Organisational experience and capability 6](#_Toc170128806)

[2.3 Compliance with the Social Value Model 7](#_Toc170128807)

[3 Costed Proposal 8](#_Toc170128808)

[Appendix 1: Supporting Information: Social Value Model: 9](#_Toc170128809)

[Appendix 2: Supporting Information - Minimum Security Standards 12](#_Toc170128810)

[Appendix 3: Supporting Information: Supply Chain Risk Management Strategy 14](#_Toc170128811)

[Appendix 4A: Services to On-Campus Campus Halls of Residence (Onity) 17](#_Toc170128812)

[Appendix 4B: Potential Future Phases - Services to Off-Campus Halls of Residence 18](#_Toc170128813)

[Appendix 5A: Potential Future Phases – Bishop Otter Campus Buildings 19](#_Toc170128814)

[Appendix 5B: Potential Future Phases – Bognor Regis Campus Buildings 21](#_Toc170128815)

1. Introduction

The University of Chichester is a forward looking institution with a rich history that goes back to the 1839. There are around 110 buildings in total, some of which are interconnected or in clusters. Of these, some are modern, but there are also buildings whose construction pre-dates the University.

Most buildings are located on the University’s two campuses (College Lane Chichester and Upper Bognor Road, Bognor Regis), with off campus student residences Stocksbridge (+405 rooms) and Fishbourne (+134 rooms). These buildings are variously used for teaching, student accommodation and administering the University, but also for public access and bookable facilities (sports halls etc) and hosts conferencing, sports, and other events.

Premises are secured with a range of facilities, from hard (physical key) locks, but also (and increasingly) e-locks. These have developed over time, and with different solutions, across locks that enable internal and external facing doors, powered doors, and facilities such as parking barriers.

The ultimate aim is that there will be convergence to integrated (lock) solutions with a long life span, with relevant, convenient and easy to use, standards based methods for current and future generations for staff, students, customers and visitors. This means that we are interested to consider flexible, multiple-token solutions including operation through mobile phones and biometrics (E.G. finger, voice, and eye scan). Ideally this would be with minimised, low maintenance devices and controllers and minimal cabling to infrastructure to each door.

Over time, we aim to bring together the governance and allocation of soft ‘keys’ (tokens/credentials), with ease of allocation, integrity, and of course rapidity and automation for terminating access, in a robust, easy to use and coherent (single) management system.

We do not expect to achieve this overnight and envisage a long term relationship to achieve the aim, in reasonably sized phases (buildings at a time). We expect to prioritise the on-campus student accommodation and the exact shape of the phases / projects may reflect how standards based the solution can be and how this works without adding further complexity to the overall estate. Subsequently, we aim to consider, how we might integrate other campus buildings, and the off-campus student residences.

* 1. The University’s estate

The University’s student accommodation comprises of around 1300[[1]](#footnote-2) rooms in purpose built blocks of various sizes. Of these around 800 rooms are on campus and 500 off campus. The layout of our campus accommodation can be seen at <https://www.maps.chi.ac.uk>. Particularly the on-campus accommodation is used for bed-and-breakfast, and for conferencing during the summer, and then intensively for Students from September to June.

There are around 800 rooms/locks in the on-campus student rooms with a legacy (Onity[[2]](#footnote-3)) system of magnetic swipe card entry locks, and an Onity management system, for which support is coming to an end. This uses a simplistic look-up table to identify the Student and manual input for other guests, with a mag-stripe card burner/printer at the Bognor and Chichester accommodation offices. Configuration of a mag card is building/room specific, (allowing for skeleton key entry for authorised personnel), and cards can be rescinded manually.

We have planning approvals and mature planning applications for additional accommodation, and mature plans to refurbish existing buildings. Projects to equip these with e-locks that are consistent with our long term plan for convergence across the whole estate would be a collaborative project with the respective developer(s). For our leased off-campus accommodation, once the on-campus rooms etc have been upgraded, we may consider (in collaboration with its owners) projects to also make these consistent with the rest of the estate.

The University’s learning, teaching and administration buildings are served by 178 Paxton swipe and e-keypad readers. Some of these have NFC capability, and keypad for a PIN, but are typically operated using a MiFare card NFC card. These are served by an up to date NET2Plus (Paxton) management system, with dynamic interfaces to the student, and staff records systems, and a manual interface to create visitor cards. Net2 allows for a range of role-based classifications, and these are configured to enable or disallow access to different buildings etc. The profile on each card can be rescinded automatically (date expiry) and manually.

All accommodation, (on and off campus) and campus buildings are served with power and internet connectivity Each building has a secure communications cabinet that is linked to the University’s private network.

* 1. Critical success factors

Updating the student room’s doors operated with the legacy Onity system is our first priority, and we anticipate transitioning over locks and management (we will maintain the old system as we transition to newer technologies, building by building, and as we remove any old lock controllers that might be in the way).

We are not proposing any specific proprietary technologies, however, usability, future-reproofing, security, any-time any-place and ease of use for operating the management system are key factors. Our general design principles are around, simplification, standardising, low maintenance, security, and supportability and are very much reflective of sustainability in all supply, materials, operation, and longevity.

A popular current feature of the current Students and Staff ID cards is that these are Mifare NFC cards used for door entry, and that they also enable identification for printing, libraries, and our attendance systems. Naturally, it would be advantageous, if Students in our Accommodation did not need to carry 2 cards.

Systems may need to interface with for example the Tribal student ID System and the ITrent Midlands HR system as ‘identity providers’ and with Kinetics Accommodation Management System, (including for conferencing guests etc). We expect privacy be design, and cards, and all systems must actively resist unauthorised access use, card cloning etc. Although we are not anticipating changing any of these systems in the foreseeable future (5-10 years) solutions should be ‘standards based’ and interoperable.

Systems need to work collaboratively with fire and egress systems – for example where a door is an emergency exit, we expect this to be auto-unlocked in relation to an active fire alarm, in that location.

* 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 all tenders are 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 advantageous solutions to its requirements, using the prescribed tendering methodology for requirements of this size and nature.

* 1. High level requirements

Appendices 4 and 5 describes our Residences and Campus locks/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, the Procurement Act 2023 (which comes into effect in October) and the corresponding guidance set out by the Crown Commercial Service[[4]](#footnote-5).

There is some flexibility in how the guidance is expected to be 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. This means we only apply the company checks etc to candidates who meet the criteria. We trust however that it is clear that if you cannot meet the criteria of the 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 – Questions and Answers

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. For fairness to all candidates who may submit their tender earlier rather than later, we will close questions and answers a week before the closing date.

* 1. Procurement timetable

The procurement project is working to the following timescale:

|  |  |
| --- | --- |
| Stage | Key Dates |
| Publication of Tender Notice  | 28/06/24 |
| Closing Date for submission of this Selection Questionnaire | 31/07/24 – 12:00 Mid-Day GMT |
| Clarifications (Questions and Answers) | Please note we will close questions and Answers a week before submission date  |
| 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  | TBC |

* 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 (31/07/2024 @ 12:00 GMT mid-day), to tenders@chi.ac.uk.

Please note you can submit a tender today, and that the above date is the firm closing date and time, your tender will be held securely until after the closing, and then assessed along with those from other candidates.

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. 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. 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 | A | The information must be accurate and relevant | **Pass/fail** |
| Supply Chain Risk Management  | B | Clear demonstration of minimum security standards, and throughout the Supply Chain  | **Pass/fail** |
| Occupants Safety | C | Clear demonstration of the integrity for student safety, anti-intrusion, and insurance  | **Pass/fail** |
| Organisational experience and capability  | D | Industry Knowledge (Standards, and suppliers)  | 10% |
| E | Adherence to UK Data Protection Legislation and the minimum Security Standard (see Appendix 2)  | 10% |
| Financial Position | F | Costs and Value for Money (VFM) | 20% |
| Lock/controller installation costs  |
| System licensing (graduated to number of rooms) |
| Hosting requirements  |
| Locks | G | Coherent model for Hardware (door) system hardware, and system licensing costs  | 20% |
| Minimised hardware for door controller units, with power resilience.  |
| Coherent lock design, that satisfies insurance security standards.  |
| Coherent lock design that allows for simple, and for example powered doors  |
| Coherent design that allows for fire safety – auto unlocks |
| Coherent sign that enables alerts to locks that are out of action, or that have been tampered with.  |
| Core system | H | Experience and long term roadmap. Does the tenderer own the system, or is it a partner.  | 10% |
| I | Usability, and support arrangements (call out and support for system, controllers and locks) and evidence of Customer Satisfaction  | 10% |
| Environmental Sustainability | J | Demonstrable awareness, and clarity of how supplier monitors the environmental damage, in and through its activities.  | 10% |
| Compliance with the Social Value Model | K | 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. 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 0.10, and the inventory set out in the appendices. We have deliberately avoided stipulating any specific manufacturer. It is important however that you can (as set out in the assessment criteria 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  | Criteria G, H, I |
| Please give an example of the hardware for a room, floor (of various numbers of rooms), building (of various numbers of floors) and their power / data connections and cabling.   |

|  |  |  |
| --- | --- | --- |
| 2 | Please describe your door locks and their associated hardware (please add photographs and dimensions etc). Please note maintenance and call-out support)  | Criteria G, I |
| Please identify options for cards/blue-tooth/NFC protocols, biometrics  |

|  |  |  |
| --- | --- | --- |
| 3 | Please describe your proposed operating system and how it is accessed – ideally with screen grabs to illustrate core functionality for operational (reporting and alerting). Please identify resilience and support | Criteria H, I |
| Please advise of your hosting options – whether server(s) are needed on campus etc,  |

|  |  |  |
| --- | --- | --- |
| 4 | Please describe your safeguarding facilities  | Criteria B,C,E,F,G |
| I.e. maintenance alerts, fire, power resilience and any other reporting (locks that are out of action, suspected tampering, unduly wedged open..)  |

|  |  |  |
| --- | --- | --- |
| 5 | Please describe how you ensure the security of our data  | Criteria B, C, H, I |
| Please refer to the Minimum Security Standards, and any security accreditations you hold |

* 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.  | Criteria B, D, J |
| 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. | Criteria B,D |
| Our residences can be in service year round  |

|  |  |  |
| --- | --- | --- |
| 9 | Please describe how you monitor and respond to any service incidents  | Criteria I |
| Ie on-call, emergency and routine maintenance services  |

* 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) | Criteria J,K |
| See criteria in Appendix 1 * Tackling Economic Inequality
* Fighting Climate Change
* Equal Opportunities
* Wellbeing
 |

|  |  |  |
| --- | --- | --- |
| 11 | Skills | Criteria G, I |
| 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.  | Criteria J,K |
|  |

1. Costed Proposal

Please set out your plan, design, and costs assuming transition to enable us to meet our aims over time. Phases might be a block, or several blocks at a time.

Please also set out the banding of the core system based on room numbers – or any other criteria.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7  | Total |
| Locks @ Each |  |  |  |  |  |  |  |  |
| Relative System fees |  |  |  |  |  |  |  |  |
| Any other fees |  |  |  |  |  |  |  |  |

NotesPlease include a copy of your standard Ts and Cs,  |

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 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 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 4A: Services to On-Campus Campus Halls of Residence (Onity)

Internal student room numbers per building are set out below (NB entry/exit doors are additional.

|  |  |  |  |
| --- | --- | --- | --- |
| **Bishop Otter** |  |  |  |
| Amberley  |  |  | 41 |
| Chilgrove |  |  | 47 |
| Harting |  |  | 36 |
| Arundel |  |  | 11 |
| Duncton |  |  | 12 |
| Ifold |  |  | 18 |
| Loxwood |  |  | 24 |
| Midhurst |  |  | 17 |
| Petworth |  |  | 18 |
| Ashling 1 |  |  | 10 |
| Ashling 2 |  |  | 10 |
| Springfield 1 |  |  | 12 |
| Springfield 2 |  |  | 12 |
| Springfield 3 |  |  | 12 |
| Springfield 4 |  |  | 12 |
| Springfield 5 |  |  | 10 |
| Springfield 6 |  |  | 10 |
| Hammond 1 |  |  | 10 |
| Hammond 2 |  |  | 12 |
| Havenstoke Close |  |  | 40 |
|   |   |   | **374** |
|  |  |  |  |
| **Bognor Regis** |  |  |  |
| Barbara Smith Halls 01 (B01)  | 8 |
| Barbara Smith Halls 02 (B02)  | 24 |
| Barbara Smith Halls 03 (B03)  | 24 |
| Barbara Smith Halls 04 (B04)  | 24 |
| Barbara Smith Halls 05 (B05)  | 8 |
| Barbara Smith Halls 06 (B06)  | 8 |
| Barbara Smith Halls 07 (B07)  | 8 |
| Barbara Smith Halls 08 (B08)  | 18 |
| Barbara Smith Halls 09 (B09)  | 12 |
| Barbara Smith Halls 10 (B10)  | 18 |
| Barbara Smith Halls 11 (B11)  | 8 |
| Longbrook (B12)  |  | 52 |
| Charlotte House (B13)  | 7 |
|   |   |   | 219 |
|  |  |  |  |
|  |  |  |  |
| **Total** |  |  | **593** |

Appendix 4B: Potential Future Phases - Services to Off-Campus Halls of Residence

Internal student room numbers per building are set out below (NB entry/exit doors are additional).

|  |  |  |  |
| --- | --- | --- | --- |
| **Stocksbridge**  |  |  |  |
|   |   |   | **405** |
|  |  |  |  |
| **Fishbourne** |  |  |  |
|   |   |   | 134 |
|  |  |  |  |

Appendix 5A: Potential Future Phases – Bishop Otter Campus Buildings

|  |
| --- |
| Bishop Otter Campus (BOC)  |
| BOC Barrier to University house car park |
| BOC A-Corridor |
| BOC A206 (IT Office) |
| BOC Academic Building Caretakers Door |
| BOC Academic Equipment Loans |
| BOC Academic Main Door |
| BOC Academic Rear Door |
| BOC Academic Toilet Door |
| BOC B&W Corridor past registry |
| BOC B&W Double entrance door |
| BOC B&W single auto entrance door |
| BOC Business School Office NH Door 1 |
| BOC Business School Office NH Door 2 |
| BOC CELS office door |
| BOC Cloisters glass doors |
| BOC Contemplation Room |
| BOC Cycle North |
| BOC Cycle South |
| BOC Cycle Store |
| BOC Estate Office Main door |
| BOC Gatehouse Finance entrance |
| BOC Gatehouse covered entrance |
| BOC Gatehouse west side front door |
| BOC Gatehouse west side rear door |
| BOC H-corridor (access to gym1 2) |
| BOC Health One ff 1.02 (Classroom) C16-1-02 |
| BOC Health One ff Classroom (next to the PC Room) C16-1-05 |
| BOC Health One ff Office C16-1-22 |
| BOC Health One ff PC Room C16-1-04 |
| BOC Health One ff Simulation Room 3 C-16-1-06 |
| BOC Health One ff Simulation Room 4 C16-1-01 |
| BOC Health One ff Simulation Room Immersive C16-1-14 |
| BOC HealthOne Classroom C16-0-12 |
| BOC HealthOne Front Door |
| BOC HealthOne Side Door |
| BOC HealthOne Simulation Control Centre - C16-0-07 |
| BOC HealthOne Simulation Room 1 - C16-0-05 |
| BOC HealthOne Simulation Room 2 - C16-0-06 |
| BOC HealthOne Sluice Room 1 (Room 0.10) - C16-0-10 |
| BOC HealthOne Sluice Room 2 (Room 0.11) - C16-0-11 |
| BOC HealthOne Treatment Room - C16-0-09 |
| BOC Holts Front |
| BOC Holts Rear |
| BOC LRC Library Office |
| BOC LRC Main front door |
| BOC LRC cafe door |
| BOC LRC staff door |
| BOC MUSIC OLD rear door |
| BOC Media Loans Locker 1 |
| BOC Media Loans Locker 2 |
| BOC Media Loans Locker 3 |
| BOC Music First Floor |
| BOC Music Main |
| BOC New Dance North |
| BOC New Dance Side East |
| BOC New Dance Side West |
| BOC New Hall East |
| BOC New Hall North - careers |
| BOC New Hall North Stu Support |
| BOC New Hall West |
| BOC Oaklands Front |
| BOC Oaklands Side |
| BOC Old Dance Front North |
| BOC Old Dance Rear South |
| BOC Reflection Room (Chapel) |
| BOC SARC First Floor |
| BOC SARC Side Entrance |
| BOC SARC2 ChangingRoom GF |
| BOC SARC2 Emergency Exit West |
| BOC SARC2 reception |
| BOC Science Corridor outside room H142 |
| BOC Southhouse main door |
| BOC Sports Dome |
| BOC Staff Club (Marketing side) |
| BOC Staff Club (Showroom side) |
| BOC UH IT Store |
| BOC UH Post Room |
| BOC Uni House side carpark door |
| BOC\_UH12 |

Appendix 5B: Potential Future Phases – Bognor Regis Campus Buildings

|  |
| --- |
| BRC Arran House |
| BRC BIC Side Door |
| BRC BIC main door |
| BRC BMITS |
| BRC Cycle Store |
| BRC Dome 05 Ground Floor Computer Suite |
| BRC Dome Ground Floor Main Entrance |
| BRC Dome LHS Stairwell First Floor |
| BRC Dome LHS Stairwell Gnd Flr Rear Fire Exit (north) |
| BRC Dome LHS Stairwell Second Floor |
| BRC Dome Lift |
| BRC Dome Lower Ground Floor - lift lobby |
| BRC Dome RHS Stairwell First Floor |
| BRC Dome RHS Stairwell Gnd Flr Rear Fire Exit (south) |
| BRC Dome RHS Stairwell Second Floor |
| BRC G7 Fire Exit |
| BRC G7 Left Door |
| BRC G7 Right Door |
| BRC John Parry - side door |
| BRC John Parry -Main door |
| BRC MS 1 |
| BRC Mord Front Doors |
| BRC Mordington House basement |
| BRC Mordington Main |
| BRC Mordington side door |
| BRC Prayer Room |
| BRC Reprographics Rear Doors |
| BRC Reprographics main door |
| BRC SIZ Courtyard (large) |
| BRC SIZ Courtyard (small) |
| BRC SIZ Front Door |
| BRC SIZ IT Loans gnd flr |
| BRC SIZ IT teaching room north gnd flr |
| BRC SIZ IT teaching room south gnd flr |
| BRC SIZ Meeting room gnd flr |
| BRC SIZ Office Back door |
| BRC SIZ Office internal door gnd flr |
| BRC SIZ Side fire exit |
| BRC SIZ Staff Room gnd flr |
| BRC SIZ coffee shop door gnd flr |
| BRC SIZ internal corridor gnd flr |
| BRC St Michaels |
| BRC St Michaels LG1 |
| BRC St Michaels main door |
| BRC St Michaels rear side door |
| BRC St Michaels sliding door |
| BRC St Mics S1 |
| BRC St Mics S3 |
| BRC Staff Hub (L) |
| BRC Staff Hub (R) |
| BRC Student Union Office |
| BRC Theatre Front East |
| BRC Theatre Front West |
| BRC Theatre Rear East |
| BRC Theatre Rear West |
| BRC TP - L - B38-4-17 |
| BRC TP - R - B38-4-17 |
| BRC TP 4.12 Postgraduate room |
| BRC TP 4.20 Nursing BRC Simulation room |
| BRC TP Advanced Analysis Lab (L) |
| BRC TP Advanced Analysis Lab (R) |
| BRC TP Animation Studio - B38-4-22 |
| BRC TP Barrier BSH |
| BRC TP Barrier Main In |
| BRC TP Barrier Main Out |
| BRC TP CDIO Active Learning Space - Ground Floor - Main door |
| BRC TP CDIO Active Learning Space - Technician door |
| BRC TP CDIO Mezzanine Engineering Staff Only |
| BRC TP CDIO Mezzanine access |
| BRC TP CDIO back lobby |
| BRC TP CDT Comms Room B38-1-28 |
| BRC TP Edit Suites 1-6 - B38-2-19 |
| BRC TP Editing Suites 7- 9 & Master Suite - B38-2-26 |
| BRC TP Electronics Lab - Left door |
| BRC TP Electronics Lab - Right door |
| BRC TP Estate Management Office - Ground Floor |
| BRC TP Ext - Starbucks External |
| BRC TP Ext - Felpham side - External Door |
| BRC TP Ext - Main Door to Plaza |
| BRC TP Fabrication & Testing - Left door |
| BRC TP Fabrication & Testing - Right door |
| BRC TP Games Design and Development Suite - L - B38-4-27 |
| BRC TP Games Design and Development Suite - R - B38-4-27 |
| BRC TP Gaming Centre NEW - Corner Door - B-38-1-35 |
| BRC TP Gaming Centre NEW - Main door - B38-1-35 |
| BRC TP Lobby to Stage 1 & Stage 2 (Greenscreen) |
| BRC TP Mac Suite - 2nd Floor L B38-2-36 |
| BRC TP Mac Suite - 2nd Floor R B38-2-36 |
| BRC TP Machine shop 1 |
| BRC TP Machine shop 2 |
| BRC TP Materials Prep Lab |
| BRC TP Materials Prep Lab |
| BRC TP Mechanical Engineering Lab 1st Floor - L - B38-1-22 |
| BRC TP Mechanical Engineering Lab 1st Floor - R - B38-1-22 |
| BRC TP Media Store External Door |
| BRC TP Micro-electronics Lab (door 1) |
| BRC TP Micro-electronics Lab (door 2) |
| BRC TP Recording Studio Lobby - B38-3-22 |
| BRC TP Stage 1 Control Room - B38-1-29 |

1. Within extant plans, this may grow to c1450 rooms over the period of this contract. [↑](#footnote-ref-2)
2. There are around 1100 Onity locks in total [↑](#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)