Market Briefing

Student and Curriculum Management Systems

The University of Chichester

Expressions of interest can be made until

12:00 (Mid-Day - GMT) 27 September 2024

University of Chichester
College Lane
Chichester
West Sussex
PO19 6PE

Telephone:	01243 816000
Date:	27/09/2024 12:00 Midday
Revision:	1.0 Final
Email	Tenders@chi.ac.uk

Contents

1 Market Testing Student Information System Suppliers

1.1 Aims of this document

The purpose of publishing this document is to invite expression of interest from suppliers who have the capability to provide the next iteration of the University's Integrated Student System (ISS). The current contract for the ISS expires in December 2024. Expressions of interest will allow the University to better understand the capacity and appetite of the market to deliver an Integrated Student System in line with our requirements.

1.2 The University

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

Where suitable, the University employs the leading HE systems to enable its information ecosystem. This includes the most suitable, proven systems for finance, payroll, virtual learning environment, student records, timetabling, accommodation and estates management etc, as well as in its learning and teaching and student services.

1.3 The University's Student Information System

Appendix 2, sets out a high level schematic of the current Integrated Student System, and it is these (currently provided by the Tribal systems product set) that we must establish a new contract for, before the end of the year. The Tribal package has interoperability between the functional products, and additional connectivity and interfacing with a range of custom data feeds and integrations with other systems in our IT ecosystem.

A key role of the ISS is as the identity provider for students, which in turn, provides details for Identity Governance and Administration (IGA) system that manages student access to the ISS and other network and student systems.

The ISS operates in a Microsoft / SQL environment, using a VMWare enabled SAN split across two datacentres, (one on each campus, linked by private dark fibre). The ISS also integrates with the University's primarily Microsoft communication and collaboration tools, Teams, One-Drive, MS Exchange, Stream, MS Telephony and MS365 integration. All systems are also protected by secure snapshot and log-file back-ups and are supported with for example Power BI for enabling analytics, including for the verifiable proofs needed, e.g. for UKVI.

All systems including the ISS are protected by (and need to be compliant with) common security technologies and methods, including, for example, Delineated VLANs, Role Based Access, Insider Protection / Firewalling, Multi Factor Authentication, Mobile Device Management and Virtual Private Network for off-site access.

1.4 Critical Success Factors

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

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

Although we are objective in terms of hosting arrangements, we believe the existing supported on-premises configuration, with established system interfaces, offers the most reliable, familiar and secure form of delivery. Changing this would have to recognise the contract date as well as the review of custom interfaces and staff skills.

The University cannot risk fragmenting student records – including regulated retention of awards, and award data. Solutions must address archival, as well as active records.

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

In any subsequent contracting, we will draw attention to the mandatory criteria that suppliers will be asked to demonstrate compliance with for example, the Modern Slavery Act, the Social Values Act (Appendix 3) and to demonstrate evidence of policies and processes for sustainability throughout their operation and supply chain.

As with all Universities that are subject to the public procurement regime, we must take the most economically advantageous way forward. This includes the costs of any solution, but also the costs and risks of transferring from A to B etc. Our solution must represent the best value.

To assess the market fairly, all market testing (and tendering) is published through the tendering site (Contractsfinder / Findatender) as a transparent and suitable method of engaging all potential suppliers, equally, and in accordance with the Public Contracts Regulations 2015.

1.5 Background to this market testing process

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

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

Consequently, we use Market Briefings such as the publication of an outline specification to enable known and unknown solution providers an equal opportunity to identify themselves.

Please note that this process is not a call for competition and does not commit the University to any specific course of action or procurement process in respect of its requirements.

1.6 Seeking clarification – Questions and Answers

For all queries about this document or process please contact us by email tenders@chi.ac.uk. Please note that you must not otherwise contact University staff directly and you should avoid any related discussion if you happen to be working with us in some other capacity, as this might be considered canvassing, (and in which case the University might need to exclude your organisation from any future 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 to other candidates.

1.7 Submitting an Expression of Interest (EOI)

We have not set out any format for a submission. Please note however that it would be helpful if you can get in touch with us **as soon as possible**, if you consider that you have a product offer that can meet the requirements, Please contact us with details via email to tenders@chi.ac.uk. Please note that the **final** date for making an Expression of Interest is (**27/09/24 @ 12:00 GMT mid-day**).

If you consider that you can fulfil our requirements, please set out in your Expression of Interest, (and succinctly at this stage) the product architecture, and components, and how you believe your product can meet the requirements of our Integrated Student System.

At this stage brevity will be welcomed, but please consider very carefully our Critical Success Factors, timelines and the range of function we need to maintain, without disruption (See Appendix 2), and please send details of the solution, and details of universities where this is being used successfully.

The Expression of Interest process is not part of any pre-qualification or selection process. An expression of interest is no indication of a commitment to participate in any future procurement process, nor will it infer any preferential or special status on organisations who express an interest.

1.8 Confidentiality and Freedom of Information

All market testing and procurement 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 for example procurement and contracting information. Please indicate any areas of your submission that you consider should be exempted from any disclosure requests and identify why they should not be disclosed.

Appendix 1A: Contact Details

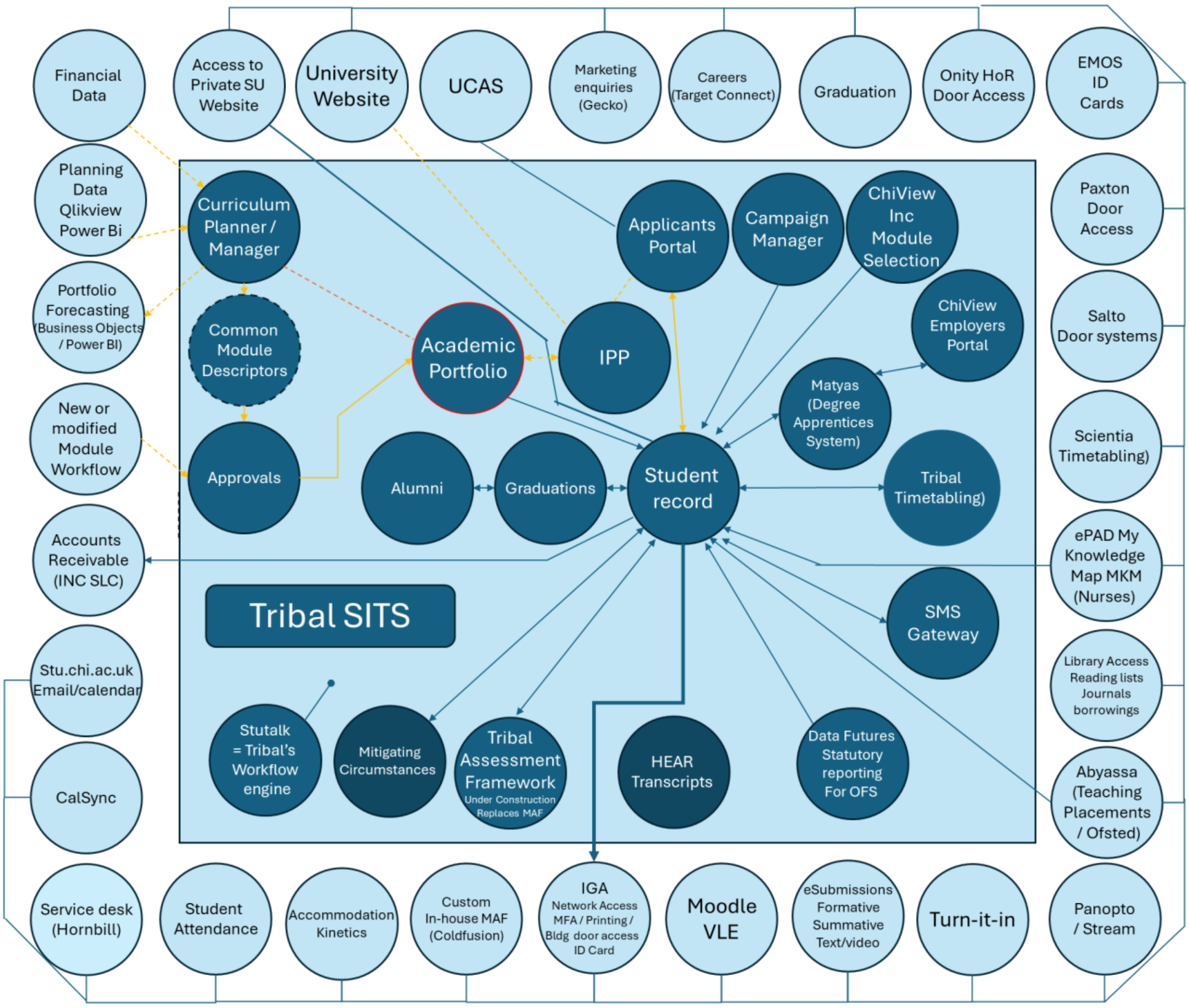
Please set out the names / contact details for the people you want to be included in any correspondence from the University. Please note as det out above, that no correspondence from your company in relation to this tender, should be sent elsewhere but to tenders@chi.ac.uk

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

Appendix 1B: Solution Details

Solution Details
NB please review the individual and linked functions set out in appendix 2 NB it will be helpful if you can indicate any HEI frameworks that your solution can be sourced from, and any pricing tariffs etc

Appendix 2: High Level Schematic of the Integrated Student System


Financial Data
Access to Private SU Website
University Website
UCAS
Marketing enquiries (Gecko)
Careers (Target Connect)
Graduation
Onity HoR Door Access
EMOS ID Cards
Planning Data Qlikview Power Bi
Curriculum Planner / Manager
Applicants Portal
Campaign Manager
ChiView Inc Module Selection
Paxton Door Access
Portfolio Forecasting (Business Objects / Power BI)
Common Module Descriptors
Academic Portfolio
IPP
ChiView Employers Portal
Salto Door systems
New or modified Module Workflow
Matyas (Degree Apprentices System)
Scientia Timetabling)
Approvals
Alumni
Graduations
Student record
Tribal Timetabling)
Accounts Receivable (INC SLC)
ePAD My Knowledge Map MKM (Nurses)
Tribal SITS
SMS Gateway
Stu.chi.ac.uk Email/calendar
Library Access Reading lists Journals borrowings
Stutalk = Tribal's Workflow engine
Mitigating Circumstances
Tribal Assessment Framework Under Construction Replaces MAF
HEAR Transcripts
Data Futures Statutory reporting For OFS
CalSync
Abyassa (Teaching Placements / Ofsted)
Service desk (Hornbill)
Student Attendance
Accommodation Kinetics
Custom In-house MAF (Coldfusion)
IGA Network Access MFA / Printing / Bldg door access ID Card
Moodle VLE
eSubmissions Formative Summative Text/video
Turn-it-in
Panopto / Stream

Appendix 3: Social Value Model:

SVM Theme	SVM Policy Outcome	SVM Model Award Criteria
Tackling economic inequality	Create new businesses, new jobs and new skills[1]	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.

[1] 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.

		▪ Demonstrate how you meet and maintain the Minimum Security Standard ▪ Commitments to informing the University where there are changes in the supply chain, or changes that might affect maintaining security. ▪ Commitments to liaising with the University in the event of a cyber attack
Fighting Climate Change	Effective stewardship of the environment	Effective measures to deliver any/all of the following benefits through the contract: ▪ Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions. ▪ Influence staff, suppliers, customers, and communities through the delivery of the contract to support environmental protection and improvement.
Equal opportunity	Reduce the disability employment gap	Effective measures to deliver any/all of the following benefits through the contract: ▪ Demonstrate action to increase the representation of disabled people in the contract workforce. ▪ Support disabled people in developing new skills relevant to the contract, including through training schemes that result in recognised qualifications.
	Tackle workforce inequality	Effective measures to deliver any/all of the following benefits through the contract: ▪ Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce. ▪ Support in-work progression to help people, including those from disadvantaged or minority groups, to move into higher paid work by developing new skills relevant to the contract. ▪ Demonstrate action to identify and manage the risks of modern slavery in the delivery of the contract, including in the supply chain.
Wellbeing	Improve health and wellbeing	Effective measures to deliver any/all of the following benefits through the contract: ▪ Demonstrate action to support health and wellbeing, including physical and mental health, in the contract workforce. ▪ Influence staff, suppliers, customers, and communities through the delivery of the contract to support health and wellbeing, including physical and mental health.
	Improve community integration	Effective measures to deliver any/all of the following benefits through the contract:

		▪ Demonstrate collaboration with users and communities in the co-design and delivery of the contract to support strong integrated communities. ▪ Influence staff, suppliers, customers, and communities through the delivery of the contract to support strong, integrated communities.

Appendix 4: Minimum Security Standards

Minimum Security Standards – General Guidance

1. Introduction

1.1. 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.

1.2. 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).

1.3. 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.

1.4. 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

2.1. The SCRMS requires that in the context of any procurement and supply that involves information, that Minimum Security Standards (MSS) are established and maintained.

2.2. 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.

2.3. 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.

2.4. 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:

2.4.1. Public which does not identify people and has no particular intellectual property or copyright value,

2.4.2. Private, which means there is intellectual, commercial, contractually valuable business information that does not contain personal identifiers or other information relating to people,

2.4.3. 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,

2.4.4. Unauthorised (which is actively monitored for an removed)

2.5. Establishing the proportional and appropriate Minimum Security Standard includes reference to the classification of information involved.

2.6. 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)

3.1. 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.

3.2. 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.

3.3. 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)

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. If the MSS is not maintained, a contract may be suspended, and in extremis, terminated.

5. Recognised Standards

5.1. 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.

5.2. 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.

5.3. The questions and considerations of a proportional Minimum Security Standard may therefore include, that the supplier (or partner) can demonstrate that they have:

5.3.1. ISO27001

5.3.2. PCIDSS

5.3.3. Cyber Essentials, or Cyber Essentials plus in relation to the supplier and its supply chain.

5.3.4. Cyber Essentials, or Cyber Essentials plus in relation to the specifics of the supply

5.4. 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.

5.5. 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.

5.6. 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:

5.6.1. 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.

5.6.2. Consult with the University if there are any changes to the risks of cyber-attack across the Supplier's supply chain.

5.6.3. 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

6.1. To ensure that the Minimum Security Standard for the supply/partnership is relevant to current risks, then this will be considered within the periodic contract performance reviews (commonly, annually).

Appendix 5: Supply Chain Risk Management Strategy

Supply Chain Risk Management Strategy – General Guidance

1. **Policy Statement**

1.1. 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.

1.2. 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.

2. **Introduction**

2.1. 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.

2.2. 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.

2.3. 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.