**![I:\RMID General\COMMUNICATIONS\[2017-18]\Corporate Projects\2018 Brand\Final assets\UNZIPPED ASSETS\Brandmark\On White\Digital\RGB\PNG\Brandmark_RGB_Colourway 1.png]()**

**Solutions Management Process**

|  |  |
| --- | --- |
| Owner: | Mike Hall (CIO) |
| Reviewed by: | Cyber Working Group |
| Approved by: | Cyber Working Group |
| Review due date: | 3rd Q 2025 |
| Update history: | Cyber Working Group – 3rd Q 2024 |
| Document Type:  | Process |
| Classification: |  |

Table of Content

[1. Introduction 3](#_Toc114646909)

[2. Scope 3](#_Toc114646910)

[3. Prerequisites 4](#_Toc114646911)

[4. Partner or Service Provider Responsibilities 5](#_Toc114646912)

[5. UR Responsibilities and Tasks 7](#_Toc114646913)

[6. Cyber Security Incident Handling 7](#_Toc114646914)

[7. Appendix 8](#_Toc114646915)

[7.1. Link to standard service catalogue 8](#_Toc114646916)

[7.2. Information required for central register 8](#_Toc114646917)

# Introduction

* 1. The Solutions Management Process is documented to ensure, for relevant systems, services and partnership (including critical infrastructure, cloud services, third-party applications, and data-sharing agreements), that there are no gaps in security responsibilities and security configurations are maintained.
	2. This document provides guidance on the following practices:

• Identify and evaluate vendor and partner relationships and contracts, both new and retrospectively, from a cyber security point of view.

• Select vendors.

• Manage relationships and contracts.

• Manage vendor and partnership risk; and

• Monitor vendor performance and compliance.

# Scope

* 1. This process is covering services and partnerships outside the standard IT service offerings of the university (see appendix for link to the current service catalogue).
	2. These can be services and partnerships that are hosted and or provided onsite or offsite the university environment, both physically as well as digitally.

# Prerequisites

* 1. This process ought to follow the steps taken by the relevant internal parties (Service Owner) to make sure a required service or functionality could not be covered to an acceptable degree by existing services available within the service provisions of the university.
	2. A written and approved Business Case must be provided by the prospective service owner detailing specific gaps in current services to justify why an additional partner or vendor relationship or service is required and where current services wouldn’t provide for this functionality.
	3. The Data protection Officer (DPO) and Information Security Officer (ISO) need to be made aware of the proposal early on in the process (e.g., before a proposal is formally submitted or once initial discussions are underway) to allow timely review.
	Either Data protection Officer (DPO) and/or Information Security Officer (ISO) can recommend NOT to progress with the solution if their assessments show that the solution is not fit for purpose from both or either data protection or cyber security perspective.
	4. Additional costs stemming from the procurement or engaging of additional external services/partnerships must be covered as part of the project and lifetime costs throughout the lifetime of the project, service and or partnership

### Costs can include

* Licenses
* Storage costs
* Staff resources

### Costs can be incurred

* before
* during implementation
* during lifetime
* in the process of decommissioning

# Partner or Service Provider Responsibilities

There are a number of responsibilities the “partner” is required to fulfil and information that has to be provided by all relevant parties, which includes the internal requester(s).

#### Incident prevention

* + - **Maintenance and protection**

The partner agrees to pro-active maintenance

* keeps hardware, operating system and all applications involved up to date, maintained and supported
* monitors the relevant vendor security notices and alerts, and any patches provided by the vendor(s) are installed in a compliant and timely manner, i.e. high level security updates must be installed within maximum 10 days *(CVE score of 7 and higher)*
* provides details of the aforementioned activities on request

The partner further agrees to protect both the environment as well as user information and data that forms part of the service. As part of this the partner will implement

* Protection measures, including firewalls, antimalware, …
* backups, both ‘local’ as well as offline/immutable according to SLA’s agreed with the service owner; at minimum this should meet the university’s backup SLA(‘s)
* encryption across all data or data that is covered under PCI, UK GDPR and other relevant data regulations (incl. backups)
	+ - **Vulnerability Management**

Where applicable, the partner consents to vulnerability scans undertaken either by the university’s IT security personnel or security partners and services we engage for these purposes.

Where this is not possible, the partner must scan at agreed intervals and notify us about any issues found, including when these issues will be addressed.
The partner agrees to successfully address any found vulnerability as follows

* + - SLA to fix **“High”** and **“Critical”** issues within max. 7 business days
		*(this is equivalent to CVSS/CVE score of 7 and higher)*
		- SLA for **“Medium”** issues to be done during next maintenance cycle
		*(this is equivalent to CVSS/CVE score of 4 to 6.9)*

The partner will provide evidence of the aforementioned activities on request or as part of service reviews

* + - **Penetration Tests (Pentest)**

If required, the university can

• either initiate or request a pentest OR

• request access to the report given by the Pentester of the partner OR request an audit document which shows that a pentest has taken place and vulnerabilities had been addressed in line with their severity (e.g. “High” or “Critical” are dealt with within maximum 7 business days *[this is equivalent to CVSS/CVE score of 7 and higher]*)

#### Logging

* + - **Ongoing Review**

the partner proactively monitors the relevant logs to identify suspicious activities , such as repeated failed login attempts, unusual access patterns, unauthorized data access, or unexpected changes to system configurations, etc.

* + - **Access to logs and records**

the partner provides access to the relevant login, authorization and transaction logs in a manner that allows the university to either

• parse these separate to our logging environment and/or

• ingest these into our central logging solution

#### Incident handling

### Any possible incident must be notified to URs CSIRT at the earliest opportunity

### Investigations

The partner provides

* access to relevant logging and information in a timely manner, either in line with logging requirements mentioned above and/or additional logs as they become necessary
* contact information of their relevant staff, where possible a single point of contact, for the purpose of the investigation and incident handling

# University of Roehampton’s Responsibilities and Tasks

#### Solutions/Service Owner (usually the department utilising the solution /service)

Ensures

* Prerequisites and responsibilities are adhered to
* Guidance provided by DPO and ISO is followed
* Information is provided in a timely manner
* Changes are shared with the relevant parties
* Any changes to this process are observed and supported
* Continued ownership and management of the relationship with the vendor, seeking support as necessary from other UR departments (e.g. IT for technical support where agreed, …)
* Active support of security maintenance of the solution (e.g. maintenance windows to patch/upgrade solutions are agreed to ensure continued compliance)
* if UR user accounts are required as part of a partnership, please see 7.3 for further requirements

#### Business Analysts Team

* reviews the documents provided by the prospective service owner requesting the service(s) in question
* confirms with and engages early in the process with

• DPO / Data Governance Manager

• ISO / Cyber Services

• other parts of IT *(if UR IT plays any part during the lifetime of this service)*

#### Cyber Services ISO together with DPO

* review specific requirements, both UOR and "external"
* provides direction, guidance and recommendations

#### IT Services

* Where agreed, IT will provide support for these areas using the standard ServiceDesk Calls (these requests have to be raised by the service owner or appropriate UR staff). This will also help to track the ongoing support requirement.
* It will also inform the service owner early of any changes to licensing and alike that would have an impact on either services or ongoing costs.

# Cyber Security Incident Handling

The university’s Cyber Security Incident Team (UoR-CSIRT) is tasked to

* Engage and cooperate with the service partner’s CSIRT where the following occurs
* Unauthorized access to their system using an account
	+ that was provided to the service owner, IT, …
	+ that is federated (UoR authenticates this account)
* Data Theft or Data Loss
	+ Due to unauthorized access
	+ Due to hacking, ransomware
* Inform and engage with the service partner’s CSIRT if the incident was either initiated or identified by the university’s CSIRT team

The UoR CSIRT investigators will inform the Chief Information Officer (CIO) and DPO at the earliest opportunity and will follow the university’s processes (e.g. Data Breach process, …)

# Appendix

## Help to record compliance

We have created a form that you can use to assist you in following and recording compliance to this process.


## Link to standard service catalogue

* Please contact IT at the earliest opportunity for more details.

## Information required for central register

**Main Contacts**

 **Partner (Operation, IT, Cyber, …)** : Include role, responsibilities, and contact information.

 **Service owner (Operation, IT, Cyber, …)**: Include role, responsibilities, and contact information.

**Service**

**type (e.g.** hosted website, application, service)

**customers** (Staff, Students, Public, …)

**UR environment integration**

**Type (**Authentication, Data, …)

 **Access** (Incoming, Outgoing (Add firewall rule reference), …)

**Data**

 Data Classification

 Relevant regulations (GDPR, PCI-DSS, …)

 encrypted

 how secured

**Security Information**

 Log Access

 Vulnerability Checks and Report Access

**Backups**

 Frequency

 Offline/Immutable Backup available

 Encrypted

***More information might be required. During engagement of Business Analysts and ISO these details and their importance will be discussed.***

## If Service/Partnership requires UR user accounts

All UR IT policies and requirements are applicable to all account holders (students/trainers), including (not a complete list).:

·         Security requirements and obligations - Password complexity, authentication checks for password resets etc.
Non-compliance with these security requirements may result in account suspension or restricted access until compliance is achieved.

·         Password Self-service & Multi-Factor Authentication (MFA)

o    Users may be required to use Password Self-service to self-manage their access (forgotten passwords, security lockouts etc.), and

o    Where applicable, enrol into MFA and ideally use a smart phone with authenticator app to secure their access.

·         User account lifecycle management - For several reasons relating to security, organisational and legal compliances and licence costs, the life cycle of user accounts must be managed (creation, suspension, deletion etc). This is the responsibility of the UR business unit responsible for the users and must be conducted end-to-end between 1 – 6 months (minimum frequency determines by risk profile), ideally more frequently esp. when large numbers of accounts are being managed, e.g.

o    HR for UR staff, guest lecturers, honoraria etc, Partnership Office and other departments for partnership staff managed by themselves etc,

o    Student Admin for UR students, other departments for partnership students.

**Please Note**

·         Data in the student record system (QL) has been integrated into the user account system, so UR and partner **student** / apprentice accounts held in QL are automatically lifecycle managed according to the student’s status (as managed by Student Admin).

·         Reports can be requested and scheduled to be sent to designated staff to assist in lifecycle management.

·         The ‘manager of the staff (as identified in the HR system - iTrent), or, in the case of non UR staff, someone in UR designated as manager’ will be emailed notifications regarding upcoming account expiries, when an account is deleted etc, so they can address the situation, if necessary, in a timely manner.

·         Some license packages require mandatory Multi-Factor Authentication (MFA) to efficiently mitigate cyber security risks. Where this is the case, it applies to ALL categories of accounts using the package, exemptions, whether for groups of users or specific individuals, are not possible.

·         Accounts can be requested individually or in bulk and great care should be taken to secure data is accurate. Once an account is created, changes, including correcting typos are time-consuming and expensive to implement. They require 3rd line IT involvement and are not quick and will therefore prove disruptive to users.