

**External Data Hosting Questionnaire**

**Version 1.3**

**8th July 2021**

**Revision History**

|  |  |
| --- | --- |
| **Date of this revision:** 08/07/2021 | **Date of next review:** 01/07/2022 |

|  |  |  |
| --- | --- | --- |
| **Version Number/Revision Number**  | **Revision Date**  | **Summary of Changes**  |
| 1.0 | 27/05/2021  |  Initial Draft |
| 1.1 | 18/06/2021  |  Modified questions |
| 1.2 | 24/06/2021  |  Reviewed Questions |
| 1.3 | 08/07/2021  |  Threat questions added |

# Overview

The purpose of this questionnaire is to ensure that third party Data Processors (in terms of the Data Protection Acts, 1988 and 2003) have acceptable IT security and data privacy policies and procedures in place to minimise the risk of loss or exposure of TU Dublin personal data.

Please answer all questions and provide sufficient detail to enable an informed risk assessment. In particular, please provide links to any policies, procedures, etc. as appropriate.

If you wish to discuss any aspect of this questionnaire, please contact the Cloud Service Provider Assessment Group by email: CSPAG@tudublin.ie

**Hosting Service Provider**

**Company Name:**

**Reference URL:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Contacts** | **Name** | **Phone** | **Email Address** |
| **Administrative Representative** |  |  |  |
| **Technical Contact** |  |  |  |

**Questionnaire:**

# Supplier Security

1. Who is responsible for Cybersecurity within the Organization?

|  |
| --- |
|  |

1. Do <Service Provider> have any cyber insurance? If yes, please state below; if possible please issue TU Dublin with a copy of the last certificate of insurance and any relevant supporting documentation

|  |
| --- |
|  |

1. Do <Service Provider> have any security certifications (e.g. **ISO 27001**, **ISO 27701 PCIDSS**, **ISAE**), if yes, please state below, if possible please issue TU Dublin with a copy of the last certificate and any relevant supporting documentation

|  |
| --- |
|  |

1. Do you comply with the GDPR (General Data Protection Regulation)

|  |
| --- |
|  |

# Data Security

1. Will data be hosted within the European Union or a location which complies with EU General Data Protection Regulation? (this includes if data is outsourced to a 3rd party hosting provider), please state location/locations.

|  |
| --- |
|  |

1. Is TUDublin Data encrypted during network transfer?

|  |
| --- |
|  |

1. Is TUDublin Data Encrypted at rest?

|  |
| --- |
|  |

1. Do you have a Data recovery capabilities? If so, please give additional details

|  |
| --- |
|  |

1. Is production data used for testing? Please explain/expand on this area, in particular, where are <Service Provider> testing, will you be using live production TU Dublin data for testing?

|  |
| --- |
|  |

1. Do you have a documented process for reporting security incidents (including data protection breaches) to tenants and, if appropriate, to regulatory and law enforcement agencies?

|  |
| --- |
|  |

1. Please confirm that you, and any outsourcing partners, will access TU Dublin data only for service maintenance purposes and that if access is required for any other purposes TU Dublin’s prior permission will be sought?

|  |
| --- |
|  |

1. Will TU Dublin data reside only in the production environment? If not, describe the other environments and the protections in place. In particular, mention where TU Dublin data resides in any backup or contingency arrangements.

|  |
| --- |
|  |

1. If you are hosting data for multiple tenants, describe how TU Dublin data will be logically segmented to ensure that it cannot inadvertently, or otherwise, be accessed by other tenants.

|  |
| --- |
|  |

1. Please confirm that TU Dublin data will be disposed and/or returned of at termination of contract. Describe how this process will be completed.

|  |
| --- |
|  |

1. Describe the process you have in place to communicate to us security incidents affecting our data

|  |
| --- |
|  |

# Disaster Recovery

1. Does the <service provider> have a disaster recovery plan? If so, can you confirm that the DR plan will maintain services and confirm the maximum tolerable downtime which may elapse before Disaster Recovery is invoked, please explain and please also specify the failover zones/locations that this is restricted to?

|  |
| --- |
|  |

1. If applicable, can <Service Provider> confirm that TU Dublin information hosted in the primary location Data Centre will failover to a secondary location with **at least equivalence in securit**y, meeting the same regulatory and jurisdictional obligations? Please explain your Business Continuity process for TU Dublin’s <Service Provider>:

|  |
| --- |
|  |

1. Can <Service Provider> confirm that there is a defined incident response plan in place to ensure that security incidents are handled in a controlled manner? Please explain your IR processes and any TU Dublin support in place to ensure that the data is protected and any breach is escalated and remediated according to best practices.

|  |
| --- |
|  |

# Governance and Risk

1. Are secure configurations and hardening guidelines followed to secure the existing infrastructure? Please explain how you secure and harden your infrastructure:

|  |
| --- |
|  |

1. Are risk assessments conducted in the organization, covering risks associated with services provided to TU Dublin? Please explain/expand on this area:

|  |
| --- |
|  |

1. Are Information Security policies and procedures in place that include requirements for administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction?Please explain/expand on this area:

|  |
| --- |
|  |

1. Do you have a change control policy. If so, please give details and provide a copy if possible

|  |
| --- |
|  |

1. Are Staff in your organization provided with Cyber security training and regularly assessed?

|  |
| --- |
|  |

1. How do you manage remote access to your corporate network (if applicable)?

|  |
| --- |
|  |

# Access Control

1. Do you have a privileged system access policy?

|  |
| --- |
|  |

1. Are users assigned individual user accounts and passwords? Please explain/expand on this area:

|  |
| --- |
|  |

1. Will the service support SSO with our O365 environment (if relevant)

|  |
| --- |
|  |

# Threat and Vulnerability Management

1. Do you have an anti-malware control policy, if so, please give details below

|  |
| --- |
|  |

1. Is AV in place on all systems hosting or potentially hosting TU Dublin information?

|  |
| --- |
|  |

1. Do you conduct regular external and internal tests to identify vulnerabilities and attack vectors?

Please give details below

|  |
| --- |
|  |

1. Do you have a patch management policy in place? If so, please give details

|  |
| --- |
|  |

1. If relevant, have you conducted a pen test in the last 12 months? If so, can you provide a copy of the results/report (redacted copy will be accepted)

|  |
| --- |
|  |

1. How do you plan and prepare for a cybersecurity incident? What processes do you have in place to respond to an incident? Do you regularly practice those things?

|  |
| --- |
|  |