University College Cork

**External Hosting of UCC Personal Data**

**Questionnaire to be completed by External Service Provider**

**(Appendix 2)**

**Version 2.6**



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 UCC personal data. **This questionnaire will form part of any Data Processing agreement or commercial contract between the service provider and UCC.**

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 Barry Foley, IT Security Officer, IT Services, UCC at +353 (0)21 4903968 or email: b.foley@ucc.ie

**Hosting Service Provider**

**Company Name:**

**Reference URL:**

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

**Questionnaire:**

1. Are you certified to industry accepted IT Security standards, typically ISO 27001? Please provide copies of certification.
2. Do you have an Information Security Policy?
3. Do you have a data privacy policy?
4. Do these policies align with any industry accepted standards framework? If so, which one(s)?
5. Do you notify tenants when you make any material changes to your information and data policies?
6. Are your staff properly educated on their legal and regulatory responsibilities with regard to security and data integrity?
7. Are regular IT security audits conducted by external independent auditors?
8. Are the results of these audits available to tenants at their request?
9. Please confirm that you provide tenants with a ‘right to audit’?
10. Do you have a certificate of PCI compliance?
11. Is your service hosted at a single site? If not, describe your hosting model.
12. In what countries will UCC data be stored?
13. Do you outsource/subcontract the hosting of applications or data storage to any third parties? If so, please provide the names of all entities that will be hosting data and/or applications and:
	1. state which, if any, of these entities are certified to industry accepted IT Security standards, typically ISO 27001 and provide copies of certification, and
	2. describe in detail how data protection and confidentiality is ensured.
14. Will UCC data ever be transported outside the EU? If so, to where?
15. As part of your, or your sub-contractors, data management processes, will the data be routed outside or be accessible from outside the EU?
16. Please confirm that, if requested, you agree to sign the EU Model Contract (standard contractual clauses) for the transfer of personal data to processors in third countries which do not ensure an adequate level of data protection.
17. Do you provide an option to host on the UCC Azure Tenancy or the UCC AWS VPC?
18. Please confirm that you acknowledge and agree you will be required to obtain the prior written consent of UCC if you wish to change the location and/or the entity hosting UCC data (to any location or entity not specified above).
19. Please confirm that you, and any outsourcing partners, will access UCC data only for service maintenance purposes and that if access is required for any other purposes UCC’s prior permission will be sought?
20. Do you have policies and procedures for:
	1. Incident management
	2. Disaster recovery and business continuity planning
	3. Change control (logging and auditing)
	4. Software patches and upgrades
	5. Anti-malware control
	6. System administration
	7. System development
	8. Controlling privileged system access
21. Please confirm that you have a documented process for reporting security incidents (including data protection breaches) to tenants and, if appropriate, to regulatory and law enforcement agencies?
22. Describe measures taken to ensure the physical security of data centre(s) where UCC data will be hosted, addressing access control, environmental control, fire suppression, backup power source, etc.
23. In particular, describe how you ensure system availability consistent with a 24/7 objective.
24. Will UCC data reside only in the production environment? If not, describe the other environments and the protections in place. In particular, mention where UCC data resides in any backup or contingency arrangements.
25. Will UCC data be encrypted when stored in any of these environments? If not, is it possible to encrypt specific fields of personal data?
26. Is UCC data encrypted during any network transfer?
27. If you are hosting data for multiple tenants, describe how UCC data will be logically segmented to ensure that it cannot inadvertently, or otherwise, be accessed by other tenants.
28. Do you have procedures in place to enforce tenant data retention policies?
29. Please confirm that UCC data will be disposed and/or returned of at termination of contract. Describe how this process will be completed.
30. Describe how users of your service can be authenticated by UCC systems (LDAP or Shibboleth enabled).
31. Do you have a standard SLA with response times, etc.?