|  |  |
| --- | --- |
| **SECTION 1: Information Classification** | **Y/N** |
| **Has the data to be processed been classified according to MMU’s Information Classification Policy?**  If so, please confirm the classification: |  |
| **Have an information asset owner and manager been identified and engaged?** |  |
| **Does the project involve Personal data?**  This means data which relate to a living individual who can be identified   1. from those data 2. from those data and other information which is in the possession of, or is likely to come into the possession of, the university   and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.  (An ICO-published flowchart for helping to identify personal data can be found [here](https://ico.org.uk/media/1549/determining_what_is_personal_data_quick_reference_guide.pdf)) |  |
| **Does the project involve Sensitive personal data?**  This means personal data consisting of information as to   1. the racial or ethnic origin of the data subject 2. the data subject’s political opinions 3. the data subject’s religious beliefs or other beliefs of a similar nature 4. whether the data subject is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992) 5. the data subject’s physical or mental health or condition 6. the data subject’s sexual life 7. the commission or alleged commission by the data subject of any offence 8. any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings |  |
| **Does the project involve other SENSITIVE data?**  This means data meeting the criteria for classification as SENSITIVE according to the MMU Information Classification Policy (found [here](http://www2.mmu.ac.uk/isds/information-security/policies/info-classification/)).  If any sensitive data types are confirmed, explain why the involvement of this data is essential to the system/service to be delivered by the project |  |
| **Has a Privacy Impact Assessment been completed?**  This will confirm the sensitivity of the data being processed, and help in the selection of controls. Please refer to the [PIA Screening Questionnaire](http://www2.mmu.ac.uk/media/mmuacuk/content/documents/data-protection/PIA-SCREENING-QUESTIONNAIRE.pdf) to determine whether a PIA is required. If you answer yes to any of the questions then a PIA must be undertaken.  Please contact Legal Services for advice on the completion of a PIA: [legal@mmu.ac.uk](mailto:legal@mmu.ac.uk).  (A copy of the PIA template can be accessed on the [University’s Data Protection website](http://www2.mmu.ac.uk/data-protection/)). |  |

|  |  |
| --- | --- |
| **SECTION 2: Information Storage, Processing, and Disposal** | **Y/N** |
| **Where will production and test data likely be stored? *(check all that apply)***   1. On server(s) managed by MMU IT Services (ITS) 2. On server(s) managed by another MMU department 3. On server(s) managed by a third party   Please summarise:  **Has consideration been given to the security requirements for hosting?**  Please summarise:  Significant assurance can be taken from the presence of current and suitably-scoped certifications: ISO 27001 for information security management; ISO 22301 for business continuity management; ISO 27017 for cloud security; Cyber Essentials (mainly for HMG departments or providers of services to HMG). The Information Security Manager will be able to offer advice on the suitability of or necessity for certifications. |  |
| **Has retention and disposal of the data being processed been considered?**  Please summarise:  **Does the project involve the migration of data from one system to another?**  Please summarise:  Migration offers a unique opportunity to apply retention and disposal principles, and mitigate information risk by reducing the amount of data migrated. |  |
| **Will data need to be encrypted at rest?**  If yes, please summarise:  This can be required depending on the sensitivity of the data. Consideration needs to be given to the best method – whether full disk, database, file etc. |  |
| **What data entry method(s) will be used? *(check all that apply)***   1. End user input via Web interface 2. End user input via client application 3. File(s) transferred from other system(s) 4. Other – please specify: |  |
| **Will copies of data be transmitted out of the technology or service?**  **If so, what transmission method(s) will likely be used? *(check all that apply)***   1. Electronic file transfers to other information systems within MMU 2. Electronic file transfers to entities external to MMU 3. Output to spreadsheets/databases created by users of the IT product or service 4. Other – please specify:   For each method checked, briefly describe the purpose of the data transmission: |  |
| **Will data be encrypted in transit?**  If yes, please summarise:  Encryption for data in transit can range from password protecting an email attachment, utilising existing secure connection channels such as remote access, to a dedicated site-to-site VPN. It is important that the technology used to secure the data makes use of strong, modern cyphers, and that key lengths are appropriate. The Information Security Manager will be able to offer further advice. |  |

|  |
| --- |
| **SECTION 3: User Access Methods** |
| **What organisational units and user groups will have access to the technology or service?**  Please detail below, considering all likely scenarios; e.g. normal use, support, compliance activity. |
| **What groups or individuals external to the University will have access to the technology or service?**  Please detail below, considering all likely scenarios; e.g. normal use, support, compliance activity. |
| **What remote access is required?**  Please detail the business requirement below. |
| **How will users be authenticated to the system**?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | Users authorised to access only their own data | Users authorised to access data of other individuals | MMU IT staff authorised to administer the system | Third parties authorised to administer the system | | Link to AD accounts |  |  |  |  | | User ID and Password |  |  |  |  | | Software Token |  |  |  |  | | Hardware Token |  |  |  |  | | Other\* |  |  |  |  |   \* If Other, describe here: |
| **How will users be authorised to access the system?**  Please summarise: |
| **How will user activity be monitored?**  Please summarise: |
| **Has access control – authentication, authorization and auditing – been included in testing?**  Please summarise: |
| **Have default account details been changed?** |
| **How will user changes (joiners, movers, leavers) be handled?**  Please summarise: |
| **Has secure operation of the system been included in user training and guidance as necessary?**  Please summarise: |

|  |  |
| --- | --- |
| **SECTION 4: Third Party Services** | **Y/N** |
| **Will the project use third party services (for example, development, business analysis, project management, HR, other consultancy)?**  Please summarise:  Third party services must meet MMU security standards. Where they reference certifications or accreditations, these should be checked. Consideration should be given to ongoing audit of security. |  |
| **What is the contractual route being taken?**   1. Adoption of third party contractual terms 2. Mandating of MM contractual terms   Please summarise: |  |
| **Will the deployed system use third party services for hosting?**  Please summarise, referencing any standards claimed or required, availability SLAs required, geographical location of the data centre: |  |
| **Will the deployed system use third party services for data processing?**  Please summarise, referencing any standards adhered to: |  |
| **Will the deployed system use third party services for support?**  Please summarise, referencing any standards adhered to, SLAs required:    **Does this require a dedicated remote access solution, or access to MMU monitoring systems?**  Please summarise: |  |
| **Has the third party agreed to adhere to MMU security policies?**  Please summarise:  **If not, have the third party’s own policies and certification been checked for compliance with MMU’s policies?**  Please summarise: |  |
| **Is vetting of third party staff required?**  Please summarise:  Vetting may be required if third party data is involved and the third party has a requirement for vetting. Common levels of vetting are BPSS and SC, both generally mandated for access to HMG material at given classifications. MMU do not by default require more than basic ID and right to work checks for staff. Where data is being processed in a different legal jurisdiction, this may change. |  |

|  |  |
| --- | --- |
| **SECTION 5: Information System Development and Deployment** | **Y/N** |
| **Where in-house or third-party development of a technical solution is required, have information security considerations been included in the specification, development and testing plans?**  Please summarise, including any standards adhered to: |  |
| **Does the system require specific firewall changes?**  Please summarise:  **Have these been documented?** |  |
| **Are test and development environments segregated and adequately secured?**  Please summarise: |  |
| **Does the proposed system require independent penetration testing?**  Please summarise: |  |
| **Has the proposed system been included in vulnerability scanning routines?**  Please summarise: |  |
| **Has the proposed system been included in backup routines?**  Please summarise: |  |
| **Has the proposed system been included in patching routines?**  Please summarise: |  |