***Technology Project Plan***

*(Report only on Technology elements of project)*

|  |  |  |  |
| --- | --- | --- | --- |
| **1. General Project Details** | | | |
| **Project Name:** |  | | |
| **Technology Project Manager:** |  | **Date Prepared:** |  |
| **Project Sponsor:** |  | **Quality Reviewers:** |  |

|  |
| --- |
| **2. Outline of Technology Project Plan** |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **3. Cost and Resources Impact of the Project** | | | | |
| **Resources** | | **Cost** | | |
| *What are the resourcing requirements? What other projects are affected by drawing down these resources? Will these cause delays to other projects?* | | *Estimated cost of project staff time. Cost of external supports. Cost of Capital expenditure. Misc (specify)* | | |
|  | |  | | |
| **4. Deliverables** | | | | |
| *A deliverable is a product or service that is given to your client. A deliverable usually has a due date and is tangible, measurable and specific. A deliverable can be given to either an external or internal customer and satisfies a due date that is created and produced in the project plan. A deliverable can be a software product, a design document, a training program or other asset that is required by the project plan.* | | | | |
| **Deliverables** | | | **Planned Start Date** | **Planned Delivery Date** |
| **Deliverable 1:** |  | |  |  |
| **Deliverable 2:** |  | |  |  |
| **Deliverable 3:** |  | |  |  |
| **Deliverable 4:** |  | |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **5. Risk Analysis – Conduct risk assessment of (a) unauthorised access to the development environment (b) unauthorised changes to the development environment (c) technical vulnerabilities of the Technology systems used in the organisation (d) the risk a new technology might bring if used in the organisation** | | | | |
| **Risk Details** | **Mitigations / Controls / Management Actions**  **(Transfer, Terminate, Treat or Tolerate)** | **Risk Ranking** | | |
| *Itemise risks that may cause the project to fail to achieve its stated business objectives or cause major disruption (e.g. Planned legislative changes, business function may be out-sourced)* | *Briefly state what has been done to minimise the risk (if anything) and recommend actions should the risk eventuate. In many instances this will result in the production of a contingency plan. Don’t prepare a contingency plan for every scenario – only when high impact risk has increased in probability.* | Likelihood  L-M-H | Consequence / Impact  L-M-H | Control Effectiveness  L-M-H |
|  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **6. Data Protection** | | | | | | | | | | |
| *Data protection by design, and data protection by default are required under the General Data Protection Regulation (GDPR) May 2018. Where personal data will be collected/processed/retained/transferred/disclosed as part of the project, the protection of this data must be considered right from the planning phase and throughout the whole project.* | | | | | | | | | | |
| **Purpose**  *Briefly state the purpose for which the personal data is being collected, used, retained, transferred, disclosed.* | **Data Category**  *Tick relevant category(ies)* | | | | | | **CSO Data Classification** | **Data Controller**  *Who determines the purpose for, and the manner in which personal data is processed?* | **Data Safeguards**  *Outline the security measures being considered to protect personal data in all it’s states i.e. data at rest, data in motion and data in use.* | **Test Data Retention**  *How long will personal data used in developing and testing need to be held?* |
| **Statistical** | | | **Administrative** | | |
| **Personal** | **Non-personal** | **Both** | **Personal** | **Non-personal** | **Both** |
|  |  |  |  |  |  |  |  |  |  |  |

|  |
| --- |
| **7. Procurement** |
| *Is there any Procurement? Describe plans.* |
|  |

|  |  |  |
| --- | --- | --- |
| **8. Technology Security – Requirements (a) description of authentication systems to be used (b) description of how confidentiality & integrity of information is to be ensured (c) description of non-repudiation of actions will be ensured (d) how misrouting will be prevented (e) how incomplete data transmission will be prevented (f) how unauthorised message alteration will be prevented (g) how unauthorised message duplication will be prevented (h) how unauthorised data disclosure will be prevented** | | |
| *Are there Technology Security issues? Give details.* | | |
|  | | |
| **9. Sign Off Authority** | | |
|  | **Head of Division – Technology Division** | **Project Manager – Technology Division** |
| **Sign Off:** |  |  |
| **Date:** |  |  |