|  |  |
| --- | --- |
| **NHS Digital HSSI Report** | **Ref: XXXXX** |

****

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Incident Created**  **Date / Time** | **NHS Digital**  **Reference** | **Incident Severity** | **Service Desk References** | **Time of Initial Failure** | **Resolution Date / Time** | **Problem**  **Reference** |
| Date of Incident | NHS Digital Reference | Severity | NHS Digital Refs | Time issue occurred | Time issue was resolved | List of all associated Problem References |

|  |
| --- |
| **Incident Description & Investigations** |
| A short summary of the Incident – ie the symptom experienced by the user and the sites affected.  E.g. 1. Users at the SDF reported they were unable to access XXX  E.g. 2. Proactive monitoring detected….  This section should describe how the incident was identified, who was engaged and a full timeline of events during the investigations, including any lines of investigation which turned out not to be related. It should include any key decision points during those investigations, the timings and discussion points of any conference calls, along with detail of when communications were distributed if relevant. |

|  |
| --- |
| **Summary of Impact** |
| A description of the impact in business terms (ie what could not be done? Were users able to carry out required business functions? How were users/patients affected?)   * Number of users/sites affected * Number of extracts affected * Duration of the Incident * Duration of any down time * The business functions that were affected   E.g. 1 All users at, *site* were unable to use *function(s)* in *application name* resulting in a delay to the production of the *XXX* extract.  E.g. 2 All users at *the SDF* were suffering slow response using *functions* in *application name* resulting in *an impact*. Due to the nature of the fault, with agreement from the customer *(Name)* downtime was arranged while the resolution activity was implemented.  E.g. 3. A *back ground process* failed causing the *required item* to be unavailable to the department resulting in *work process* being delayed / unavailable. The *background process* had to be run during the day resulting in poor performance for *users doing functions in application* until it completed.   * 25 users affected * Incident Duration dd/mm/yyyy hh:mm finish dd/mm/yyyy hh:mm * The system was down from dd/mm/yyyy hh:mm until dd/mm/yyyy hh:mm resulting in a hh:mm minute outage. * Poor system performance from dd/mm/yyyy hh:mm until dd/mm/yyyy hh:mm   NB – in the event of Poor Performance an indication of the expected or normal performance and the actual performance during the incident should be included. |

|  |
| --- |
| **Resolving Activity** |
| What was done to resolve the Incident? Was this a permanent fix or a work around?  Describe the permanent Fix if known.  If it is a work around:  Give details of the workaround, the business impact on the users of using the workaround and the business impact of reverting to normal operation.   * Can this be used again? * Is there a knowledge article to be created? * Is it automated or Manual? * How was it implemented? (e.g. a change etc) * What are the implications of maintaining the workaround including the implications of reverting to BAU if the workaround is left in place for a significant length of time? (E.g. Switching to a resilient site).   Included if DR or IT Continuity measures were considered (where applicable):   * Where DR was considered give details of what was considered and the basis on which the decision was taken. * If DR is implemented provide details of timings, business impact of implementing and using the DR procedures and the business impact of reverting BAU service provision   E.g. 1. Agreement was reached with the users to restart the application server at hh:mm. Access was restored at hh:mm and verified with the users at hh:mm.  E.g. 2. As per the documented work around provided by supplier (or from problem record nnnnn) the work around was implemented.  E.g. 3. *Change nnnnnnnn* was raised to implement a *configuration update / patch / activity*. |
| **Root Cause Investigations / Follow Up Activities** |
| Root cause should examine the processes, changes, events and technical failures that caused the problem. These may include volumetric changes, procedural changes, technical changes, hardware failures, user issues etc. This event occurred as soon at the site went live (and possibly during the deployment). Lessons learnt from the process relationship area, did the interactions work or can they be improved? Communications etc should be reviewed as part of the RCA not just the Technical items.  If the technical root cause can be found, ask what caused the technology to be in that state? Human error, process failure, unexpected volumes, hardware fault, bugs, reference supplier knowledge base etc.  Where the cause is “unknown”. If there was resolution action carried out by a specific resolver team then there will be an area of responsibility for that team. Actions to resolve an incident should be taken on the basis of some investigative work and on that basis there should always be an indicator of the cause. If it truly is “unknown”, Provide details of system areas that have been investigated and why these areas have been discounted, give an indication of the suspect areas and the approach the resolver team will be taking to investigate the cause with more action planning in the Actions below. In theory, each symptom should be able to be mapped to a finite set of components and this should be the place to start investigation.  All actions to have timescales and owners.  The owner should always be an individual on the resolver teams Org chart.  Where applicable indicate which process will run the action (eg CSIP, Problem Process etc and quote all reference numbers).  Include references to the suppliers that are involved where applicable.  If a workaround was implemented what is the timetable for providing a full solution?  If SLA targets were breached, indicate any additional actions that are required to ensure targets are not compromised in the future. |