Shropshire Community Health NHS
NHS Trust

Policies, Procedures, Guidelines and Protocols

Document Details	
Title	**Finance Procedure Y4: Oracle Disaster Recovery Arrangements**
Trust Ref No	954
Local Ref (optional)	
Main points the document covers	Controls in place to ensure business continuity in case of Oracle system failure
Who is the document aimed at?	Finance staff, particularly those in Financial Accounting
Author	David Court Head of Financial Accounting
Approval process	
Approved by (Committee/Director)	Chief Finance Officer
Approval Date	February 2025
Initial Equality Impact Screening	Yes
Full Equality Impact Assessment	No
Lead Director	Sarah Lloyd
Category	Finance
Sub-Category	Finance Procedures
Review date	February 2028
Distribution	
Who the policy will be distributed to	Distributed to senior finance staff as defined by directors
Method	Electronically to senior staff & available to all staff via the Trust website
Document Links	
Required by CQC	
Required by NHLSA	
Other	

Amendments History

No	Date	Amendment
1	November 2012	Amendments relating to re-location of failover server
2	November 2015	Minor wording changes
3	December 2018	Disaster Recovery Testing changed from Annually to Biennial – Because over the last 12 years most issues from failover tests have been identified and resolved. Hence reduced the requirement to once every two years. Amendments relating to URL link in Hardware configuration section.
4	December 2021	Minor wording changes
5	February 2025	Section 2.2 the url for failover has changed to https://rsh-shfc-app-npe.sath.nhs.uk:4444/OA_HTML/AppsLocalLogin.jsp

1 – Background

1.1 The Oracle systems admin team, providing support to the Shropshire Health Finance Consortium (SHFC) run an office hours service (typically 8:30am – 5:00pm), as do most core users. Purchasing operate during similar hours for the creation and despatch of orders.

1.2 The Oracle service is generally viewed as being designed for 24/7 availability, with transaction logging allowing mirroring of the production service to the failover using Oracle DataGuard.

1.3 An automatic fall-back to the failover server is not incorporated as part of the system. Costs to have this 24/7 service would be extremely prohibitive.

2 – Hardware configuration

2.1 Hardware configuration at the production site is a RAID 1 server~~,~~ with DataGuard transaction logging to a second server with a RAID 5 array, housed in a separate building. There is a 20-minute delay between updates to achieve the best balance between data recovery, bandwidth and network traffic.

2.2 The failover server is in permanent standby mode but is locked from access during normal operation. For information for systems leads, failover url is https://rsh-shfc-app-npe.sath.nhs.uk:4444/OA_HTML/AppsLocalLogin.jsp

2.3 Until such point as the reason for a failure to connect to the production service is determined a decision to utilise the failover server should not be taken. Consideration should also be given to the likelihood of a restoration of service and any forecast timescale. Disk failures on the RAID production server are hot swappable. Communications failures due to hardware on the box are on a 4-hour contract so should be resolved rapidly. A UPS is in place on the site to mitigate local small scale power failures, so a decision to fall back to the failover server should only be taken where a major scale incident effecting power or communications at the Production site occurs. For this reason, the decision to drop to failover will rest with the Systems Admin team.

3 – Utilisation of failover service

3.1 Once the Systems Admin team are in possession of all the relevant facts relating to the interruption to the service, a decision will be taken as to the utilisation of the failover service. Anticipated time to fall back to the failover server is between 2 to 4 hours~~.~~ Full functionality will be available on the failover service should this be required for any length of time.

3.2 Users will be notified via an “all mailboxes” e-mail of the loss of the Production service. Additionally, the Trust’s I/T status webpage and Supplies website will be updated to reflect the fact that the Production service is down.

3.3 Once in failover, the Systems Admin team will liaise with Version1, Dell and the local I/T team as to the proposed timetable for restoration of service. Once the Production service is restored to full functionality, Version1 will confirm a date and time for the replication of transactions back to the Production service. This will normally take place “out of hours” and users will once more be notified via e-mail of the return to normal service, and any out of hours downtime whilst this work is completed.

4 – Local reciprocal arrangements

4.1 Where SHFC member organisations suffer “localised” IT failures, such as virus propagation, communications failure or power outages, other consortium members will seek, wherever possible, to accommodate core users at their sites where user cannot work from home. In most cases this will comprise spare desks where staff are absent, unused workstations, scan stations or other PCs used for non-essential tasks, as well as any I/T training venues not being utilised.

4.2 These arrangements have been agreed by systems leads from each consortium member and will continue for the remainder of the Oracle contract.

5 – Disaster recovery testing

5.1 A biennial failover test should be carried out to ensure that the back-up arrangements work as planned. This is managed by the Systems Admin team with testing/support from users. This involves transferring to using the failover server and testing that key processes still work.

References & associated documents

None

Reviewed By ______________________ Date ___________________

Authorised By ______________________ Date ___________________