Disaster Recovery Policy

Policy Author(s) | Assistant Director of Informatics: Malcolm Gandy  
| Emergency Preparedness Manager: Jayne Heaney

Accountable Manager(s) | STHK – Director of Informatics: Christine Walters (SIRO)

Ratified by (Committee/Group) | NHS Halton CCG Integrated Governance Committee

Date Ratified | 21/01/2017

Target Audience | All staff, including contractors and volunteers

Review Date | January 2020

This Policy has been developed by St Helens and Knowsley Health Informatics Service (HIS), who act as NHS Halton CCG’s IT Service Provider.

This policy has been approved and adopted by NHS Halton CCG and is applicable to all staff, including contractors and volunteers.

VERSION HISTORY

<table>
<thead>
<tr>
<th>Issue Date</th>
<th>Version No</th>
<th>Brief Description of Change</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2015</td>
<td>5</td>
<td>Updated</td>
<td>STHK</td>
</tr>
<tr>
<td>Jan 2017</td>
<td>6</td>
<td>Updated</td>
<td>STHK</td>
</tr>
</tbody>
</table>
DISASTER RECOVERY POLICY
Version 6.1
Document Summary
This policy details the strategy STHK HIS has put in place, and maintains, to risk assess disaster recovery (DR) requirements and develop, implement and regularly test a tiered DR solution aimed at providing an appropriate response for each service depending on its identified criticality.

<table>
<thead>
<tr>
<th>DOCUMENT NUMBER</th>
<th>STHK0128</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVING COMMITTEE</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>DATE APPROVED</td>
<td>January 2017</td>
</tr>
<tr>
<td>DATE IMPLEMENTED</td>
<td>January 2017</td>
</tr>
<tr>
<td>NEXT REVIEW DATE</td>
<td>Yearly, January 2018</td>
</tr>
<tr>
<td>ACCOUNTABLE DIRECTOR</td>
<td>Senior Information Risk Owner, Director of Informatics: Christine Walters.</td>
</tr>
<tr>
<td>POLICY AUTHOR</td>
<td>Assistant Director of Informatics: Malcolm Gandy, Jayne Heaney: Emergency Preparedness Manager</td>
</tr>
<tr>
<td>TARGET AUDIENCE</td>
<td>Informatics Staff, Emergency Preparedness Manager</td>
</tr>
<tr>
<td>KEY WORDS</td>
<td>Information Security, Confidentiality, Information Governance, Data Protection, Information, Sharing, Consent</td>
</tr>
</tbody>
</table>

Important Note
The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as “uncontrolled” and, as such, may not necessarily contain the latest updates and amendments.
1. SCOPE

St Helens & Knowsley Health Informatics Service (STHK HIS) recognises that Information Media and Technology (IM&T) services are increasingly critical to its Health Economy Customers.

This policy details the strategy STHK HIS has put in place, and maintains, to risk assess Disaster Recovery (DR) requirements and develop, implement and regularly test a tiered DR solution aimed at providing an appropriate response for each service depending on its identified criticality.

This Policy forms the basis for the IT Disaster Recovery Plan and should be read in conjunction with the HIS customers’ Business Continuity Plans.

2. INTRODUCTION

The policy focuses on responses to disaster level outcomes (e.g. loss of one or more services such as Telephones, Electronic Health Records, Active Directory or Carestream PACS for prolonged periods) rather than causes of disaster situations (e.g. fire in a data centre).

The risk assessment mechanisms provided by this DR policy will be applied to all technology directly provided by STHK HIS to deliver services to customers.

DR solutions will be developed, maintained and regularly tested for those STHK HIS provided services deemed to be of a sufficiently critical level.

Specifically this policy applies to services delivered from STHK HIS computer and communication facilities at:

- Whiston Hospital (PABX room)
- Whiston Hospital (SCR room)
- Whiston Hospital (NDR room LG1-2)
- St Helens Hospital
- Nutgrove Villa
- Tower Hill
- Lister Road, Runcorn
- HCRC, Widnes

Services such as the Care Records Service and the e-Referral system are provided by the NHS Digital to the Trust. The disaster recovery of these systems is the responsibility of the NHS Digital and its partners. STHK HIS responsibility for DR provision for these services will be limited to ensuring network resilience to maintain continuous access to these services following a disaster level event affecting the STHK HIS provided computer network locations specified above.

In preparing this policy the following assumptions have been made:

All development work will cease immediately following a disaster. This will free up HIS resources to implement the DR plan. People will be released to enact the
recovery and development computer resources will be available to be reconfigured to replace lost production services.

The policy and plan are expected to cater for only one disaster level event at any one time

3. STATEMENT OF INTENT

DR solutions will be developed, maintained and regularly tested for those STHK HIS provided services deemed to be of a sufficiently critical level.

4. DEFINITIONS

No current definitions required.

5. DUTIES ACCOUNTABILITIES AND RESPONSIBILITIES

The Assistant Director of ICT is responsible for ensuring that appropriate policy, plans and procedures are in place to restore IM&T facilities in the event of a major failure or disaster. In addition he/she is responsible for ensuring that the "out of hours" staff rota is adequately maintained to support the plan outside of normal business hours.

As part of the Business Continuity Plan (BCP) process, the Assistant Director of ICT, the IT Development Manager and the Managers responsible for each Service must carry out assessments on each Service to measure the realistic impact a failure would have on the health economy, develop the DR plan and procedures to manage this impact and communicate the risks and mitigation steps planned with HIS customers.

The Senior Information Risk Owner and Information Asset Owners will take ownership of the risk of data loss during and DR level event.

The Operations and Development managers are responsible for ensuring that the computer systems including applications and data are backed up as stated in the Backup Policy.

The IT Development Manager is responsible for ensuring that the data network is designed for resilience and maintained with adequate capacity as required in this policy.

A role of Disaster Controller exists within the DR plan and responsibilities are defined within the DR plan. This role will be filled by the most senior HIS manager on-site during normal office hours or initially by the on-call HIS manager outside of normal business hours.
6. PROCESS FOR IMPLEMENTING THIS POLICY DOCUMENT

6.1 Approach

Sufficient capacity will be maintained in the core network and in computer and communications rooms (including air conditioning, power, and floor space) to recover from the loss of one room within target timescales.

Each service provided by the HIS will be classified by business criticality in line with the table below. There will be a four tier classification of services each with a target recovery timescale.

There will be a process to categorize each service by cost and benefit of rapid recovery.

- Tier 1 - recovery within 1 hour
- Tier 2 - recovery within 1 day
- Tier 3 - recovery within 5 days
- Tier 4 - recovery within 14 days

Individual recovery procedures will be developed and maintained to restore each service in line with its required reinstatement time line.

A detailed step by step overall DR plan will be maintained and periodically tested of how recovery will be enacted using the individual recovery procedures including:

- Switching to dedicated fall back equipment where this exists
- The re-assignment and reconfiguration of development systems to support production systems for which resilient hardware does not exist
- Procurement arrangements for equipment, software or contract services to recover less critical systems

6.2 Communication with HIS customers

Sufficient computer hardware will be procured and maintained to deliver recovery of each service according to its priority. For guidance only:

- Tier 1 services will require fully redundant servers and storage with replicated data
- Tier 2 services will require fully redundant servers and storage
- Tier 3 services will require identified servers and storage that can be reconfigured to provide a DR platform
- Tier 4 services may have some identified servers and storage that can be reconfigured to provide a DR platform but additional purchases will be required after a DR level event to recover full service

Capacity planning processes will be run regularly ensure that DR capacity is maintained in line with developments and enhancements on the production environment.
Following a disaster level event this policy assumes that all development, training and other non-live (non-production) work will be suspended.

Testing of the DR solution will be undertaken on a selected subset of STHK HIS provided services at least annually. The selected subset will vary from year to year.

The recovery policy will encompass re-instating services following a disaster at DR locations. Any reinstatement works, such as rebuilding, to allow a return to normal operations is outside the scope of this policy.

6.3 Risk Assessment of Service

A procedure will be applied to each existing service and each new service during development, to assess the following:

How long can the customer afford to be without the service?
What would happen if no pre-disaster preparations are made?
What is the hourly cost of being without the service?

From this assessment a criticality level will be assigned to each service in line with the table in section 6 of this document.

This criticality assignment will then drive investment in pre-disaster preparations for that service and the environment in which it runs (computer room floor space, power and air conditioning) again in line with the guidance in section 6 of this document.

Aligning Business Continuity Plans and DR Plans

It is important to recognise that a Disaster Recovery plan alone is insufficient to guarantee continuity of health economy operations following a DR level event.

The DR plan is one element of a wider Business Continuity Plan (BCP).

To ensure that these different plans remain synchronized regular meetings will be held with Operations leaders from all HIS customers, coordinated by emergency planning managers from each customer.

6.4 Disaster Plan

The Disaster Plan, incorporating communication plan, can be found at:

   \trust2\groups\Development\Disaster Recovery\Disaster Recovery Plan\Disaster Recovery Plan.doc

Designated Disaster Recovery Management Team members must hold an up to date paper copy of this plan at an accessible location away from:

   a) Their usual place of work
   b) The main STHK HIS data centres and communications rooms covered by the disaster plan
7. TRAINING
   • Not Required

8. MONITORING COMPLIANCE WITH THIS DOCUMENT

Key performance Indicators of the Policy

<table>
<thead>
<tr>
<th>Describe Key Performance Indicators (KPIs)</th>
<th>Frequency of Review</th>
<th>Lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duties are carried out as described in the policy</td>
<td>Annually</td>
<td>Assistant Director of Informatics</td>
</tr>
<tr>
<td>Compliance will be monitored via the Information Governance Toolkit</td>
<td>6 monthly</td>
<td>IG Manager</td>
</tr>
<tr>
<td>External Audit Rating to be of an acceptable standard.</td>
<td>Annually – 31st March</td>
<td>IG Manager</td>
</tr>
</tbody>
</table>

Performance Management of the Policy

<table>
<thead>
<tr>
<th>Aspect of compliance or effectiveness being monitored</th>
<th>Monitoring method</th>
<th>Individual responsible for the monitoring</th>
<th>Frequency of the monitoring activity</th>
<th>Group / committee which will receive the findings / monitoring report</th>
<th>Group / committee / individual responsible for ensuring that the actions are completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be specific as the aspect of compliance being monitored within the policy. refer Key performance indicators KPI's</td>
<td>Reviews</td>
<td>Assistant Director of informatics</td>
<td>Yearly</td>
<td>IG Steering Group</td>
<td>Risk Management Council</td>
</tr>
<tr>
<td>If your ‘policy’ includes Mandatory training then you should cross reference to the Induction Mandatory and risk</td>
<td>IG Toolkit 309-1a</td>
<td>IG Manager</td>
<td>Yearly</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Management
Training Policy
Training needs analysis policy - below is an example of the wording that can be used to monitor this.

9. REFERENCES/ BIBLIOGRAPHY

10. RELATED TRUST POLICY/PROCEDURE

- Network and Information Security Risk Policy
- Information Governance Policy
- Major Incident Business Continuity Plan
- Informatics Business Continuity Plan
APPENDIX 1

Equality Analysis

“St Helens and Knowsley Teaching Hospitals NHS Trust is committed to creating a culture that promotes equality and embraces diversity in all its functions as both an employer and a service provider. Our aim is to provide a safe environment, free from discrimination, and a place where all individuals are valued and are treated fairly. The Trust adheres to legal requirements and seeks to mainstream the principles of equality and diversity through all its policies, procedures and processes.

The Trust takes a zero tolerance approach to all forms of discrimination, harassment and victimisation and will make every effort to ensure that no patient or employee is disadvantaged, either directly or indirectly, on the basis that they possess any of the “protected characteristics” as defined by the Equality Act 2010. The protected characteristics are as follows: - race; disability; sex; religion or belief; sexual orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; and age.

This policy will be implemented with due regard to these commitments.

All authors of policy documents must include a completed equality analysis Stage 1 screening. Policy authors must refer to the Trust Equality and Diversity Policy 2011 and the equality analysis toolkit and associated guidance documents (Stage 1 and Stage 2) available on the intranet.
### Equality Analysis Stage 1 Screening

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td><strong>Title of Policy:</strong> Disaster Recovery</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td><strong>Policy Author(s):</strong> Malcolm Gandy</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td><strong>Lead Executive:</strong> Christine Walters</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td><strong>Policy Sponsor</strong> Phil Corrin</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td><strong>Target Audience</strong> All staff</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td><strong>Document Purpose:</strong></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td><strong>Please state how the policy is relevant to the Trusts general equality duties to:</strong> N/A</td>
</tr>
<tr>
<td></td>
<td>eliminate discrimination</td>
</tr>
<tr>
<td></td>
<td>advance equality of opportunity</td>
</tr>
<tr>
<td></td>
<td>foster good relations</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>List key groups involved or to be involved in policy development (e.g. staff side reps, service users, partner agencies) and how these groups will be engaged</strong> Trust communication tools (Team brief, global emails)</td>
</tr>
</tbody>
</table>

**NB Having read the guidance notes provided when assessing the questions below you must consider,**

- Be very conscious of any indirect or unintentional outcomes of a potentially discriminatory nature
- Will the policy create any problems or barriers to any protected group?
- Will any protected group be excluded because of the policy?
- Will the policy have a negative impact on community relations?

If in any doubt please consult with the Patient and Workforce Equality Lead

**9** Does the policy significantly affect one group less or more favourably than another on the basis of: answer ‘Yes/No’ (please add any qualification or explanation to your answer particularly if you answer yes)

<table>
<thead>
<tr>
<th></th>
<th>Yes/No</th>
<th>Comments/ Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Race/ethnicity</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Disability (includes Learning Disability, physical or mental disability)</td>
<td>N</td>
</tr>
</tbody>
</table>
and sensory impairment)

| Gender | N |
| Religion/belief (including non-belief) | N |
| Sexual orientation | N |
| Age | N |
| Gender reassignment | N |
| Pregnancy and Maternity | N |
| Marriage and Civil partnership | N |
| Carer status | |

1. Will the policy affect the Human Rights of any of the above protected groups? N
2. If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? N
3. If you have identified a negative impact on any of the above protected groups can the impact be avoided or reduced by taking different action? N
4. How will the effect of the policy be reviewed after implementation? N/A

If you have entered yes in any of the above boxes you must contact the Patient and Workforce Equality Lead (ext 7609/ Annette.craghill@sthk.nhs.uk) to discuss the outcome and ascertain whether a Stage 2 Equality Analysis Assessment must be completed.

Name of manager completing assessment: (must one of the authors) Malcolm Gandy

Job Title of Manager completing assessment Assistant Director of Informatics

Date of Completion: December 2016
The Trust has a duty as a public body to publish all completed Equality Analysis Screening and Assessments. Please forward a copy of your completed proforma to Annette.craghill@sthk.nhs.uk

The Patient and Workforce Equality Lead will conduct an audit on all completed Screening and Assessments every six months.