Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Digital Transformation (IT Operations)

Business Continuity & Disaster Recovery (BCDR) Policy

This procedural document supersedes: CORP/ICT 11 v.4 – Information and Communications Technology (ICT) – Business Continuity Policy (including: Disaster Recovery Plans)

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s)	Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Name and title of author	Roy Underwood – Information Governance Manager David Linacre – IT Ops Security & Continuity Manager
Date revised	June 2022
Approved by (Committee/Group)	Information Governance Group IT Risk Management Group
Date of approval	June 2022
Date issued	October 2022
Next review date	February 2025
Target audience:	Trust-wide

IT Operations - Business Continuity & Disaster Recovery Policy

Amendment Form

Version	Date	Brief Summary of Changes	Author
Version 5	27 June 2022	• Inclusion of reference to the IT Ops Cyber Incident Response Plan	Roy Underwood David Linacre Jerome Boniface
Version 4	10 May 2021	• Change of Policy Title to IT Operations Business Continuity & Disaster Recovery Policy • Addresses (in Section 2) the relationship between this IT Ops Policy and any parallel Polices and/or Processes managed by the Trusts Clinical and Admin functions. • Complete rework of the document to meet the assertions of the Data Security & Protection Toolkit (DSPT) • Update information to Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.	Roy Underwood David Linacre
Version 3	February 2013 May 2012	• Updated for grammar and new style format included. • Updated to meet current systems and priorities and for departmental structure.	S Parsons S Parsons
Version 2	June 2008	• Minor amendments to content around Head of Information & IT Services job roles and references to Disaster Recovery Plans (DRP). • Reformatted to comply with NHSLA and Equality Impact Assessment requirements.	Roy G Underwood
Version 1	July 2006	Implementation	Roy G Underwood

IT Operations - Business Continuity & Disaster Recovery Policy

Contents

Page No.

IT Operations - Business Continuity & Disaster Recovery Policy

1. INTRODUCTION

Planning for the business continuity concerning the Trusts IT Service provision is a complex task. Preparation for, responding to, and recovery from a disaster affecting the IT Service functions of the Trust requires the cooperative efforts of many support organizations, e.g. NHS Digital & the National Cyber Security Centre (NCSC), in partnership with the functional areas supporting the business of the Trust. This document records the Policy that outlines and coordinates these efforts, reflecting the analyses by representatives from relevant departments and by the Trust's Information Governance Lead.

This document addresses the risks and mitigations associated with Digital Transformation's IT Operations business continuity policy and disaster recovery plans.

It should be emphasized that this document applies primarily to the members of the Digital Transformation Team, since they have the responsibility of preparing for, responding to, and recovering from any Operational IT issues that impact on the Trust.

Therefore, any and all Divisions and Directorates who rely on networked or other IT Services provision for their day to day business should have their own business continuity policies and practices in place, and that they will not be described in this policy document.

2. PURPOSE

The Trust increasingly depends on digital information processing and telecommunications. This dependency will continue to grow. The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the Trust and most importantly, patient safety.

The Trust's Information Governance Assurance Framework (IGAF) is an integral component of the Trust's decision to achieve compliance with Cyber Essentials Plus via the Data Security & Protection Toolkit (DSPT). The DSPT ensures that the Trust is always working to the standards defined by the National Data Guardian.

Support

The Trust recognizes that there are usually two distinct levels of support required:

1. There is a high probability in a large Acute Trust of theft or malicious damage to IT facilities. This probability requires Digital Transformation to make plans for a reliable IT Incident Reporting mechanism coupled with a rapid replacement system for 'lost' facilities which does not generally involve any facilities other than the IT service provision itself. Repairs or improvements to physical security measures in vulnerable areas are largely the responsibility of the Trust's Estates Department.

2. There is a lower but still significant probability of severe damage to data processing, network services and telecommunications capabilities that support the Trust. Nevertheless, because of the potential impact, a Policy for reducing the risk of damage from a disaster, however unlikely, is vital. The Trust's Business Continuity & Disaster Recovery is designed to reduce the risk to an acceptable level by ensuring the restoration or continuation of critical Category 1 and essential Category 2 processes.

The Policy:

a. Identifies the critical IT functions of the Trust and the resources required to support them

b. Provides guidelines for ensuring that the necessary personnel and resources are available for both disaster preparation and response, and that the proper steps will be carried out to afford the Trust timely restoration of services.

c. Specifies the responsibilities of individual roles, whose mission is to establish Trust level procedures to ensure the continuity of the Trust's business functions. In the event of a disaster affecting any of the functional areas, IT Operations – through the IT Service Desk – liaise with the functional area(s) affected and other Trust divisions and departments. These services include the support provided by IT, Estates, Fire and Security Services, and public information dissemination handled by the Trust's Communication's & Engagement Office, among others.

d. Understands that The Chief Operating Officer (COO) and the Emergency Planning Lead (EP Lead) are responsible for all arrangements relating to how the Trust Clinical and Admin functions react to and manage their own Business Continuity policies and processes in parallel with the IT BC & DR Policy.

2.1 The Main Threats

The Policy is predicated on the validity of the following threats to IT service provision:

- **Threat 1** – Loss of Power

- **Threat 2** – Serious environmental damage to Computer and /or Telephony Rooms/s (explosion, fire, flood etc)

- **Threat 3** – Denial of Service Attack by:
  - Serious software/system malfunction
  - Serious Virus, Trojan Code or Worm
  - Other malicious means

- **Threat 4** – Serious loss of staff (e.g. sickness/strike) or loss of physical access to Computer / Telephony Rooms (e.g. terrorist activity)

The Trust's IT Operations Leads and the Information Governance Lead/Data Protection Officer (DPO), are responsible for developing the Trust's IT Business Continuity & Disaster Recovery Policy.

However, individual Divisional & Corporate areas across the trust who are reliant on an IT Service provision, are responsible for their own immediate reaction to a loss of some or all IT facilities, and for planning for recovery from same. Central to the Policy and indeed the business continuity and recovery processes is a Executive 'single point of contact' between IT Services and the users of the services they provide.

2.2 IT Incident Management

Ensuring that the Policy reflects ongoing changes to resources is crucial. This task includes updating the Policy and revising this document to reflect updates; testing the updated Policy; and training personnel.

Testing this policy against the Trust's Clinical and Admin support Business Continuity Policies and Plans is an essential element of preparedness. Partial tests of individual components and recovery policies specifically related to an IT Service provision will be carried out on a regular basis and in line with relevant DSP Toolkit Assertions.

3. SCOPE OF THE DIGITAL TRANSFORMATION – IT OPERATIONS - BUSINESS CONTINUITY & DISASTER RECOVERY POLICY

The scope of this Policy gives guidance on the restoration of Critical and Essential systems in the aftermath of a disaster that disables any functional area and/or essential equipment supporting the systems or functions in that area. The risk assessment of the computer applications should assign appropriate categorization. This risk-based process identifies applications that have the highest priority and must be restored within the timescale of the disaster recovery matrix. Specifically, each function of these systems is evaluated and allocated a place in one of four risk categories, as described below.

Category 1 - Critical Functions

Category 2 - Essential Functions

Category 3 - Necessary Functions

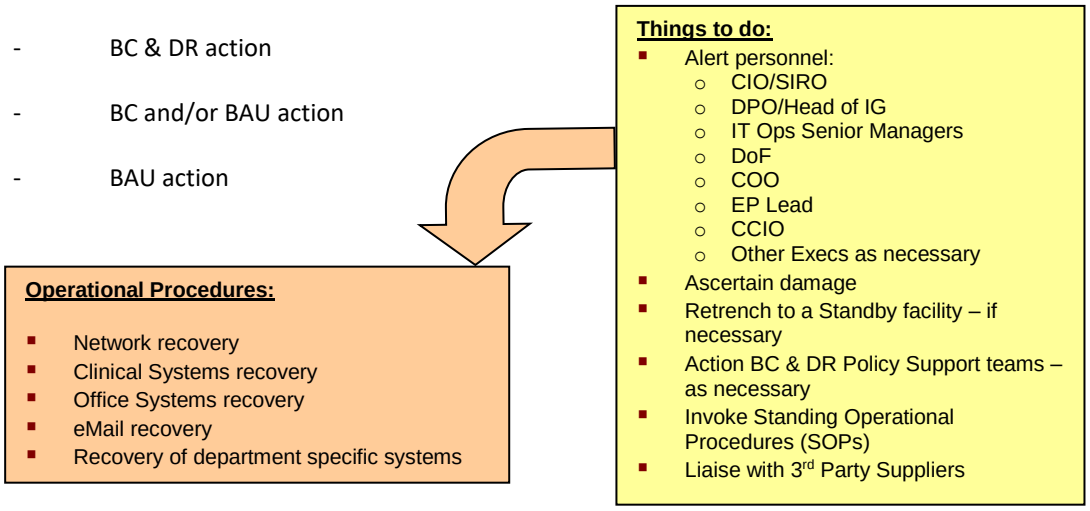
Category 4 - Desirable Functions

Note: Category 4 functions are important to the Trust administrative processing, but due to their nature and other factors, they may be suspended for the duration of the emergency.

The systems in Categories 1 - 3 are those that provide Trust wide services i.e. Patient Systems, Internet and eMail, Medical Records, Office and Finance systems[1]. There are many departmental and laboratory systems as well as non-information processing systems that are also either essential for the Trust or the local area(s) they support i.e. Rotherham, Doncaster and South Humber (RDASH) NHS Foundation Trust, and the Doncaster & Bassetlaw Clinical Commissioning Groups (CCGs). Recovery for these systems too must be based upon Service Level Agreements, including an assessment of the impact of their loss and the cost of their recovery.

The helpdesk will decide – based on information available at the time of the incident – on the seriousness of the incident:

- Major - BC & DR action
- Medium - BC and/or BAU action
- Minor - BAU action



3.1 Disaster Recovery Plan (DCP)

This section describes the required responses to a disaster, or to a problem that could evolve into a disaster:

- Detect and determine a disaster condition
- Notify persons responsible for recovery
- Initiate the Trust's IT Business Continuity & Disaster Recovery Policy
- Ensure that the Trust COO and EP Lead are made aware and are therefore ready to initiation the Clinical and Admin Support Business Continuity Policies and Procedures – as necessary
- Activate a designated hot site (control centre) - if necessary
- Disseminate Public Information
- Provide support services to aid recovery

Each subsection below identifies the organization(s) and/or position(s) responsible for each of these six responses.

[1] For an up-to-date categorisation list, see appendix 1

3.2 Detection and Determination

The detection of an event which could result in a disaster affecting information processing systems at the Trust is the responsibility of IT Services, or whoever first discovers or receives information about an emergency situation anywhere across the Trust.

3.3 Notification

The Duty 'bleep holder' will either:

- notify the IT Services help desk, or;
- use the Trusts Business Continuity Callout Lists,

and then monitor the evolving situation.

3.4 Initiation of the Trust's IT Business Continuity & Disaster Recovery Policy

When a situation occurs that could result in interruption of processing of major information processing systems, the following people must be notified, where possible:

- Chief Information Officer CIO/SIRO
- Director of Finance
- IT Security and Continuity Manager
- Information Governance (IG) Lead/Data Protection Officer (DPO)
- Selected Information Asset Owners (IAOs)
- IT Systems and Development Manager
- IT Infrastructure Manager
- IT Programme Manager
- Telecommunications Manager
- Head of Information
- Medical Records Manager(s)

3.5 Activation of a Designated Standby Facility

The responsibility for activating a designated standby facility or back-up resource is delegated to the CIO/SIRO. In their absence responsibility reverts to the nominated deputy and/or IT Support lead. As soon as possible after the occurrence, the CIO/SIRO, or the appointed deputy, determines the prognosis for recovery of the damaged functional area through consultation with the Information Governance and IT Operations Leads and – where appropriate - the Damage Assessment Team, headed by Estates.

3.6 Dissemination of Public Information

The Communications & Engagement Manager is responsible for directing all meetings and discussions with the news media and the public, and in conjunction with the Personnel Department, Trust personnel not actively participating in the recovery operation. In their absence, the responsibility reverts to the Duty Manager on call.

3.7 Provision of Support Services to Aid Recovery

During and following a disaster, IT Support Teams are responsible for aiding local divisional/departmental managers. They operate under the direction of the Digital Transformation Business Continuity Management Team (BCMT).

3.8 Business Continuity Strategy

The Business Continuity strategy explained below pertains specifically to a disaster disabling the main Computer Rooms at the DRI and Bassetlaw Hospitals. These functional areas provide core network and major server support to the Trust's administrative applications and IP telephony requirements etc. Especially at risk are the 'critical applications', i.e. those designated as Category 1 systems. The IT Support Teams provide for recovering the capacity to support these critical applications at the earliest opportunity. Summarizing the provisions of the Policy, subsections below explain the context in which the Trust's Business Continuity Policy operates. The Business Continuity Policy complements the strategies for restoring the data processing capabilities normally provided by IT Services.

3.9 Disaster Recovery Strategy

This section addresses three phases of disaster recovery:

- Emergency
- Backup
- Recovery

Strategies for accomplishing each of these phases are described below. It should be noted that the subsection describing the emergency phase applies equally to a disaster any building across the Trust affecting a designated 'critical' system.

3.10 Emergency Phase

The emergency phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures direct efforts to protect life and property, the primary goal of initial response. This will necessarily include Patients, the Public and Members of Staff. Security over the area is established as local support services such as the Police and Fire Departments are

enlisted through existing mechanisms. The Duty Manager is alerted by pager and begins to monitor the situation.

If the emergency situation appears to affect one of the main Computer Rooms (or other critical facility or service), either through damage to data processing or support facilities, or if access to the facility is prohibited. The Duty manager will closely monitor the event, notifying relevant personnel as required to assist in damage assessment. Once access to the facility is permitted, an assessment of the damage is made to determine the estimated length of the outage.

If access to the facility is precluded, then the estimate includes the time until the effect of the disaster on the facility can be evaluated.

The Recovery Team remains active until recovery is complete to ensure that the Trust will be ready in the event the situation changes.

3.11 Back-up Phase

The back-up phase begins with the initiation of the appropriate Trust Policies and SOPs[2] for outages caused by a major disaster. In the initial stage of the back-up phase, the goal is to resume processing critical applications. Processing will resume either at the main Computer Room or at the designated standby facility, depending on the results of the assessment of damage to equipment and the physical structure of the building.

In the back-up phase, the initial standby facility must support critical (Category 1) applications and as many Category 2 applications as resources and time permits. During this period, a reduced service resumes, up to the capacity of the standby facility. Within this period, a main Computer Room or alternative facility will be returned to full operational status.

3.12 Recovery Phase

The time required for recovery of the functional area and the eventual restoration of normal services depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with back-up operations at the designated standby facility. The primary goal is to restore normal operations as soon as possible.

[2] All relevant Trust Policies and SOPs declared in the reference section

4. TEAM DESCRIPTIONS AND RESPONSIBILITIES

The Digital Transformation Business Continuity Management Team (BCMT) is composed of Managers. The following is a list of each position on the BCMT, and a brief overview of each member's responsibilities:

- **Chief Information Officer (CIO / SIRO) -** Acts as Chair of the BCMT and as link-person to the Trust Executive Management.

- **DPO / Head of IG & Head of IT Operations** – Act as a Coordinators for the BCMT, with assistance from other Senior IT Managers.

- **IT Security and Continuity Manager** – Act as the co-ordinator for the BCMT, to provide liaison between the Trust's operational and management teams and the IT Support Teams in affected areas. Responsible for purchase of replacement Assets and for maintenance of the Asset register. Provides technical support for ALL Computing Facilities and other distributed IT Services and Networks.

Trust Support Teams:

Under the overall direction of the BCMT, Trust Support Teams provide support to assist a functional area's recovery. These teams, described below, work in conjunction with personnel in the area affected by the problem condition to restore services and provide assistance at the Trust level. In many cases, these support teams have as their normal responsibility the provision of these support services. This support is generally documented in a procedure manual. The Business Continuity Policy is an adjunct to that documentation and highlights, in particular, the interfaces between the Trust level service and the individual divisions and departments operational requirements. In cases where the documentation in this Policy and the divisions and departments documents differ, the divisions' and departments' documentation has precedence. It will be a Trust requirement that divisions and departments have their own Business Continuity and Disaster Recovery Policies and Plans.

- **Damage Assessment/Salvage Team** - Lead by Estates and activated during the initial stage of an emergency, the team reports directly to the BCMT, evaluates the initial status of the damaged functional area, and estimates both the time to reoccupy the facility and the salvageability of the remaining equipment. This team draws members from Estates, IT Services, Fire and Health & Safety Officers, Security Manager, Telecommunications Systems team, local managers of the affected area as well as appropriate vendors supporting the environment.

- **Following the assessment of damage**, the team is responsible for salvaging equipment, data and supplies following a disaster; identifying which resources remain; and determining their future utilization in rebuilding the data centre and recovery from the disaster. The members of the Damage Assessment Team become the Salvage Team.

- **Public Information** - The interface with the media, the general public and patients and staff who are not participating in the recovery process is handled by the Trust's Communications & Engagement Office.

- **The Telecommunications Manager** (with assistance of IT Operations) is responsible for establishing voice and data communications between the affected site and the remainder of the trust sites.

5. MONITORING COMPLIANCE & EFFECTIVENESS

Monitoring the effectiveness of the policy will be achieved through periodic audit with the results going to the Information Governance Group to the Finance & Performance Committee and the Board of Directors.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Review of the current policy and any associated Standard Operational Procedures (SOPs) through desk-top educational scenarios to emulate possible disasters designed to test and improve.	Digital Transformation in conjunction with The Chief Operating Officer, the Emergency Planning Lead, and the Board Secretary	6 monthly	Information Governance Group (IGG) Audit & Risk Committee though IGG Minutes

6. ASSOCIATED TRUST PROCEDURAL DOCUMENTATION

CORP/ICT 2 – IM&T Security Policy

CORP/EMP 4 – Fair Treatment for All Policy

CORP/EMP 27 – Equality Analysis Policy

IT Ops Cyber Incident Response Plan

ISO17799:2005, ISO/ISE 27001

NHSD: Data Security & Protection Toolkit (DSPT)

See also footnote on page 10

7. EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment For All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 2).

8. DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website:
https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

APPENDIX 1 – ASSET FUNCTION CATEGORISATION

Asset Function Categorisation

- Category 1 – Critical Functions
  - Trust LAN/WAN
  - Trust Integration Engine (TIE)
  - CaMIS PAS
  - Radiology (RIS)
  - Zillion
  - Pathology
  - Drug Prescription and Administration (JAC)
  - Order Communications and Results Reporting (ICE)
  - Theatres
  - Symphony ED
  - NHS Network v3
  - Medical Imaging (Picture Archiving & Communications - PACS)
  - Trust eMail
  - Medical Records Tracking (iFIT)
  - IP Telephony Services and Applications
  - Internet (World-wide Web)

- Category 2 – Essential Functions
  - Electronic Staff Record (ESR)
  - Office Systems
  - Trust Intranet

- Category 3 – Necessary Functions
  - Clinic Based systems
  - Audit systems

- Category 4 – Desirable Functions
  - Training systems
  - Car Parking

APPENDIX 2 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Digital Transformation BC and DR Policy: CORP/ICT 11 v.5	Digital Transformation	Jerome Boniface	Existing	June 2022

1) Who is responsible for this policy? Name of Division/Directorate: SIRO/CIO's Office

2) Describe the purpose of the service / function / policy / project/ strategy? Trust-wide Information Governance Policy

3) Are there any associated objectives? Compliance with UK GDPR 2021, the Data Protection Act 2018 and Confidentiality Legislation

4) What factors contribute or detract from achieving intended outcomes?

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage / civil partnership, maternity / pregnancy and religion/belief? No

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) Is there any scope for new measures which would promote equality? No

7) Are any of the following groups adversely affected by the policy?

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: March 2025

Checked by: Roy G Underwood **Date: 23/06/2022**