The Tavistock and Portman NHS
NHS Foundation Trust

Information Communication Technology Backup and Failure Contingency Procedure

Version:	1.2
Bodies consulted:	--
Approved by:	PASC
Date Approved:	17.06.2016
Lead Manager:	ICT Manager
Responsible Director:	Director of IM&T
Date issued:	June 2016
Review date:	May 2018

Contents

Information Communication Technology Backup and Failure Contingency Procedure

1 Introduction

The Trust operates a Microsoft Windows network comprising over 100 servers and more than 700 PCs and laptops. With this complex set up the Trust recognises that even with robust safeguards there is a continual risk of system problems which could result in loss of access to data on a short, medium or permanent basis.

Some key data is held on the Trust's servers; but several key systems (RiO patient database; Electronic Staff Record; Oracle financial system; Library system; and the Trust's website) are web-based systems supplied by NHS or commercial organisations. These systems are covered by the suppliers' contingency plans and by the Trust's plans to maintain access.

2 Purpose

The purpose of this plan is to set out the arrangements in place in the Trust for:

- Minimising risk of loss of access to computer systems in the Trust
- Detailing the action plan to be followed in the event of medium, long term or permanent loss of part or all of the computer network and system.

3 Scope

This plan applies to the management of all Trust computer infrastructure, hardware and software.

The failure plan is applicable to all staff affected by the failure who will be required to follow any instructions for action as directed by the lead person as set out in Appendix 1.

4 Definitions

IT Failure

- An IT failure is an unplanned incident that results in a significant or total loss of telecommunications, data or the IM&T service to one or more of the Trust's sites arising from: damage to, loss or destruction of critical parts of the IM&T infrastructure; non-availability or destruction of information systems resulting from a virus attack or other external threat.
- An IM&T failure can result from any cause including: fire, flood power failure, human error, sabotage of system etc
- Note: Temporary loss of service due to equipment malfunction, cable breaks etc. is not classified as a failure.

5 Policy Statements

The Trust aims to avoid disruption to services by minimising the risk of loss of access to computer systems and data; and by ensuring a prompt recovery from any such loss.

6 Duties and Responsibilities

6.1 Chief Executive

The CEO has ultimate responsibility for ensuring the Trust has in place suitable and sufficient arrangements to respond to any loss of access to computer systems (both temporary and permanent) and that the Trust actively mitigates against such loss happening. The CEO has delegated the day to day responsibility for this function to the Director of Finance.
The CEO may declare an IM and T Failure under this procedure.

6.2 Director of Information Management and Technology.

The director is responsible for the Trust's IT service, and the ICT Manager reports directly to him. The director may declare an IM and T Failure under this procedure.

6.3 Head of Information Communication Technology (ICT)

The ICT Manager manages the Information Technology (IT) team and is responsible for maximising the resilience of the Trust's systems. This includes ensuring that the day to day back up processes (7.1) are carried out and that all relevant members of staff are fully conversant with the procedures as stipulated in the document; virtualisation (7.2), and testing the DR procedures and recording the results of these tests (7.3).

In the event of an IM&T failure, the ICT Manager is responsible for prompt action to restore service, ensuring that the procedures (Appendices 1 and 4) are followed and that there are no delays. The ICT Manager will ensure prompt, clear and regular communication with all users regarding any interruption to service, the action being taken, and the expected time when service will be restored.
The ICT Manager may declare an IM and T Failure under this procedure.

7 Backup Policy

7.1 Backup Policy and Procedures

The Trust owns data located in a number of locations so it is vital to ensure that this data is maintained in a secure manner, that resilient solutions are in place and that the data can be recovered in the event of a disaster.

This policy defines the principles for managing Trust data and backups.

7.2 Scope

The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as a key deliverable and is not therefore designed as a method of archiving material for extended periods of time.

The 'data' backups cover all systems managed by the IM&T department. Data held and managed locally in departments is excluded. All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the network drives

provided, central e-mail services or with appropriate network based applications such as CareNotes.

7.3 Backup Policy

Onsite Data

- Full backups of all Trust data are performed weekly. Full backups are retained for 3 months before being overwritten
- Incremental backups of all Trust data are performed daily. Incremental backups are retained for 1 month before being overwritten.
- Where possible backups are run overnight and are completed before 8am on working days.
- Upon completion of backups, data is replicated to cloud based storage.
- Backups are stored in secure locations. A limited number of authorised IM&T personnel have access to the backup application and media copies.

Offsite Data such as CareNotes

- Where Trust data is held offsite as part of a cloud based solution or software as a service there will be a contract or SLA in place stipulating that backup routines will equal or exceed the level defined for onsite data.
- The supplier of offsite services must be contractually obliged to restore TRUST data in the event of a disaster. SLAs should be defined for this activity in accordance with the needs of the commissioning service.

Backup

- The IT Backup systems have been designed to ensure that routine backup operations require no manual intervention.
- The IT department monitor backup operations and the status for backup jobs is checked on a daily basis during the working week.
- Any failed backups identified are re-run immediately the next working day.
- If backups fail more than once the failure will be escalated to the Head of IT and an impact assessment carried out.

Restore

- Data is available for restore within a few minutes of a backup job completing on the daily schedule.

- Data will be available during the retention policy of each backup job – which is currently defined as 3 months.
- Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IT systems at TRUST have been specified to minimise data loss between backup windows by having elements of system redundancy.
- Requests for data recovery should be submitted to the IT Helpdesk.

7.4 Failure Recovery: Data Testing

The IT department undertakes failure recovery testing on a regular basis.

- IT has a dedicated server for this purpose.
- The server is built from scratch; this means everything on the server is deleted and the operating system is reinstalled.
- A backup point is chosen (at random or in sequence) which is then restored onto the new server using either Windows restore or the Veritas software.
- Users are requested to access the server to a) confirm the server can indeed be accessed and b) the data on the server is valid.
- Once this is done the failure recovery/restoration is written up a success and documented.
- Each system will be tested at least once in each calendar year. This will be done by a cycle of testing through the year, with at least one system being tested every three months.
- The resilience of the Trust network (within each main building and between sites) will also be tested at least annually. This will be performed in conjunction with our external partners.
- DR testing will be led by identified members of the IT team. However, the ICT Manager will ensure that all staff have the required skills to carry out a restore if required.
- Details and results of the tests will be recorded (in a central record available for audit) by the performing engineer. Any issues will be escalated to the ICT Manager who will responsible for ensuring appropriate action is taken.
- Recovery testing will establish, among other things, that the back-up records are not corrupted and can be utilised as intended.

8 IT Failure Plan – High Severity Incidents

8.1 IT Failure Procedure

With the increased dependence on IT systems and services for the provision of Trust activity it is essential that clear processes are in place to deal with significant failures.

The following procedure describes the stapes required in the event of a significant IT failure.

Scope
This procedure only applies to severity 1 incidents whereby all or part of an IT system has failed and therefore impacts on Trust services affecting patient care, student training or administrative functions.

Exclusions
Failures of single items such as a PC or telephone would not be included, loss of service for a small number of users where a workaround is available are not included.

Procedure

A. The person who identifies the incident will log a call with the IT Helpdesk.

B. It is the responsibility of all staff to respond to significant incidents in line with this procedure.

C. If the incident occurs outside of regular working hours and the IT Helpdesk is not available an email should be sent to helpdesk@tavi-port.nhs.uk with the following details:

i. Name of person who discovered incident
ii. Description of incident
iii. Description of perceived impact of incident
iv. The asset tag of devices involved in the incident such as "LT1234" for a laptop device
v. Location of equipment currently and when the incident occurred
vi. Contact details for the individual who discovered the incident

D. The person who reported the incident should follow up the email with a phone call once the IT Helpdesk re-opens.

E. When logging an incident with the IT Helpdesk they will capture the above information over the phone.

F. The IT staff member who receives the call (or identified the incident) will escalate to the Head of IT or Director of IM&T (if the Head of IT is absent) if the impact is considered significant. The staff member would add the following:

i. Is the equipment affected business critical?
ii. What is the severity of the potential impact?

iii. Name of system being targeted, along with operating system, IP address, and location.
iv. IP address and any information about the origin of the attack.
v. Any further relevant information they are able to gather through initial investigation.
vi. The Head of IT will lead on assessing the severity of the incident and determining the appropriate response, 2 options exist:
vii. Low impact incident not affecting critical systems or Trust services, or
viii. High impact incident affecting critical systems or Trust services.

G. If the incident is low impact, such as a localized PC failure and workarounds are available, the incident will be managed through normal IT incident processes.
H. If the incident is high impact then the ICT Manager will complete an incident form and escalate to the Director of IM&T, the SIRO, Head of Informatics and the Information Governance Manager (these 5 individuals will make up the ICT Incident Management Team (ICTIMT)).
I. The ICTIMT will grade the incident based on the action cards in appendix 4 and appoint the appropriate incident lead.
J. Depending on the nature of the incident the ICTIMT will determine whether Trust wide communications should be made and whether other staff should be informed or escalated to.
K. The Head of IT will organize a meeting of the ICTIMT to discuss the situation over the telephone or face to face and determine a response strategy.
    i. Is the incident real or perceived?
    ii. Is the incident still in progress?
    iii. What data or property is threatened and how critical is it?
    iv. What is the impact on the business?
    v. What system or systems are affected, where are they located physically and on the network?
    vi. Is the incident inside the trusted network?
    vii. Is the response urgent?
    viii. Can the incident be quickly resolved?
    ix. What immediate steps should be taken to resolve the incident and mitigate risk? This should include both technical, social and communication measures.
L. It is expected that key members of the IM&T Department will stop other work and prioritize resolution of the major incident even if this means performing duties that are not normally within their remit. For example Informatics could assist in answering the phones on the Helpdesk if demand increases.

M. Team members will recommend changes to resolve the incident and possibly prevent the occurrence from happening again.
N. Upon management approval, the changes will be implemented.
O. Relevant communication should take place with affected users before and after implementing the change to resolve the incident.
P. Systems will be tested to ensure they are functioning normally. Basic connectivity testing will be performed by IT but system functionality testing will need to be conducted by the end users. It will co-ordinate this process.
Q. The incident will only be closed once the ICTIMT has been assured that the systems and services are performing normally once more and the threat/issue has been dealt with.
R. Documentation—the following shall be documented in an incident report and processed as per the Trust incident reporting procedure:
    i. How the incident was discovered.
    ii. The category of the incident.
    iii. What the root cause of the incident was.
    iv. What the response plan was.
    v. What was done in response?
    vi. Whether the response was effective.
    vii. Lessons learned.
S. Notify proper external agencies as appropriate.
T. The incident report and lessons learned/action plan shall be shared with the ICTIMT for review and approval.

9 Training Requirements

All IT staff must be fully aware of this plan and of their role in it: see Appendix 3.

The plan and the back-up procedures must be included in the local induction of new IT staff.

IT staff with specific responsibilities for any of the procedures set out in section 7 (see Appendix 3) must have appropriate training to enable them to carry out these duties.

10 Process for Monitoring Compliance with this Policy

The IT Manager will review the backup and testing records regularly, will take action if any gaps are identified, and will report on his findings and on any concerns to the Information Governance workstream.

This procedure will be subject to an annual review and report to the Management Committee.

The backup and testing records will be reviewed by Internal Audit and reported to the Audit Committee. This will be part of the overall internal audit cycle, and will not necessarily be included in each year's work programme.

11 References

BHS Information Management & Technology Security Manual.

12 Associated documents

- Risk Strategy and Policy
- Serious Incident Procedures
- Incident Reporting Procedure
- Risk Assessment Procedure
- ICT Security Policy and Procedure
- Remote Access Procedure
- Laptop Procedure
- Security of Premises and Assets Policy

Appendix A: Equality Impact Assessment

Completed by	**Jonathan McKee**
Position	**Governance Manager**
Date	**12.5.16**

The following questions determine whether analysis is needed	**Yes**	**No**
Does the policy affect service users, employees or the wider community? The relevance of a policy to equality depends not just on the number of those affected but on the significance of the effect on them.	X	
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?	X	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		X

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then undertake the following analysis:

	Yes	No	Comment
Do policy outcomes and service take-up differ between people with different protected characteristics?		X	
What are the key findings of any engagement you have undertaken?			N/a
If there is a greater effect on one group, is that consistent with the policy aims?			N/a
If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?			N/a
Will the policy deliver practical benefits for certain groups?		X	
Does the policy miss opportunities to advance equality of opportunity and foster good relations?		X	
Do other policies need to change to enable this policy to be effective?		X	
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 –seek advice from Human Resources.

Appendix B: Process and Action Plan in the event of an IT Failure

An IT failure is defined in section 4 above.

Grades of 'Failure'

Event	Grade of responsiveness	Lead
Temporary loss of service with anticipated recovery of less than ½ day	Green	Head of ICT
Temporary loss of service with anticipated recovery of less than 1 week	Amber	Director of Information Management and Technology
Full loss of service with no anticipated recovery date	Red	Gold Commander (action cards to be followed) (See the Trust's Business Continuity Plan)

The Trust has established a set of action cards that are to be followed in the event of a system failure resulting in data or communication loss. These are shown at Appendix 4.

The IT Incident Management Team will determine the grade of responsiveness and will be kept informed throughout incident resolution.

Appendix C: What Does IT Backup?

The backups have been separated into three jobs on separate tapes and NAS folders. Backup jobs concentrate on the servers; no PCs or laptops are included.

- Main backup. This includes all databases (Lotus Domino, SQL), file servers and Active Directory data. A full backup is taken every Friday with incremental Monday through Thursday. Every last Friday of the month a full backup is run and kept for 12 months.
- Exchange. This backs up the Microsoft Exchange server information store which contains all email, attachments, contacts and calendar items. A full backup is taken on Fridays with incrementals taken Monday through Thursday.
- Archive Manager. This backs up the email archive database server.

Appendix D: Backup and DR Roles

Role		Responsible
Routine backup schedule. Checking backup job logs. Liaising with supplier if required. Rotating tapes.		Deputy IT manager
Restorations from backup.		IT/Network support technician
Restorations from SonicWALL		IT/Network support technician
Virtual server administration, backup, restore		IT Manager or Senior Engineer

Appendix E: IT Action Cards

Please see the Business continuity Plans for overarching plans for the Trust or service line affected.

Activity area	Key Tasks	Lead
Central coordinating team (IT Incident Management Team)	Establish a central coordination team with a Failure Commander to manage failure, and to recruit members appropriate to the nature of the failure, and ensure all key staff have mobile phones. Establish a central control command location for the duration of the failure. Appoint loggist to keep event log. Determine which (if any) external bodies need to be informed and communicate as appropriate. Take decision re extent of clinical services that can be maintained and review decision at regular interviews throughout the failure. The event will be logged as a 'red' incident and subject to full RCA at the conclusion of the failure period	CEO/Director of IM&T /ICT Manager (i.e. person who called the failure)
Assessment of extent of damage and likely recovery time	Assess extent of damage and report to central team: Determine the likelihood and timing for any system restore. Engage help of agreed external expert contractors for support at the direction of the Failure commander. Reassess situation on at 4 hourly intervals during the failure and provide updates to command team. Manage location and set up of any agreed temporary equipment as advised by external	ICT Manager

Activity area	Key Tasks	Lead
	experts.	
Determination of responsibility for IT service	Determine the extent of the responsibilities for responding to IT failure between Trust staff and other providers Make contact with relevant contact or other service provider as appropriate.	ICT Manager
Communications	Set up a communications point and get notification to staff by any means possible (mobile phones, personal laptops etc) Arrange central hot line number for all external inquiries and provide brief to staff answering phones	Normally the responsibility of the ICT Manager. See also the **Trust's Business Continuity Plan:** In the event of a serious disruption to services (levels 2 or 3), the 'Silver Command' is responsible for managing communications via the Comms team.
Relocation	If it is necessary to relocate from main site to the Monroe Centre or any viable Incident Control Room. This decision will be made by the Gold Commander. IT relocation will be directed by the ICT Manager who will direct staff in his own team and other staff are required (refer also to the Trust's Major Incident Plan and Business Continuity Plan)	Gold Commander Silver Command / Coordinator of the activity ICT Manager

Appendix F: Recovery Priorities List

In the event that there is an option as to the order in which recovery is achieved the following schedule of priority will be followed:

1	Integrated D Care Record
2	DET databases
3	Finance system (ESR, SBS)
4	Email
5	File Servers