

Reference number G050
Approved by Integrated Governance Committee
Date approved 24 January 2008
Last revised 1 September 2007
Review date 24 January 2012
Category General
Contact Director of Finance, Information, Estates and
Procurement
Who should read this All Staff

IT Systems Backup and Restore Policy

Title: **IT Systems Backup and Restore Policy**

Purpose: To allow data essential to the business of the Trust to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems.

Author/Responsibility of: Author: Information Governance Manager;
Responsibility: Trust Boards

Applicable to: All ICT Users working for Herefordshire Primary Care Trust (HPCT) or based at HPCT locations.

All third party contractors working within HPCT.

All third party personnel working within the HPCT.

Scope: Herefordshire Primary Care Trust.

Revision History: 01 August 2005 – First Draft

01 September 2005 – Version 1.0

01 September 2007 – Version 2.0 Amended Contact from Director of Finance, Information and Performance to Director of Finance. Information, Estates and Procurement, amended Information Security Support Officer to Information Governance Manager, amended Head of ICT Services to IT Services Manager.

24 January 2008 – Version 2.0

Approved

Review Date 24 January 2012

Action to be taken in event of breach of policy: For members of staff actions will be taken in accordance with current HPCT Human Resources procedures.

Any actions taken against third party contractors will be inline with the procedures agreed in the contractual agreements or information sharing protocols.

1. Objective

To maintain the integrity and availability of information processing and communication services. Routine procedures should be established for carrying out the agreed back-up strategy, taking backup copies of data and rehearsing their timely restoration.

The objectives of backups are to allow data essential to the business of the Herefordshire Health Community to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems. As

part of the Herefordshire Health Community Information Security Management System (ISMS) this policy aims to reduce the risk of information stored within the server environment being lost.

2. Housekeeping

2.1 Information back-up

Information back-up is one part of Business Continuity (see IT Service Continuity Policy HIS002). All systems should have some sort of backup facility. For large specific applications this will typically be a tape or CD writing backup facility as well as arrangements such as mirrored discs and backup servers to provide additional resilience in the event of component or power failure.

For smaller applications (such as access databases) and data folders, the regular backup of shared network storage drives should suffice.

Users who keep large amounts of information on local hard discs should consider shared storage facilities or other backup facilities such as CD writers.

Each system/area will determine the appropriate backup procedure using the following guides, with advice from the IT department and Information Security Officer:

- Regularity of backup – it makes sense to backup a system every time a change (or set of changes) is made. For multi-user systems (such as PAS), there should be as a minimum, the provision of ‘mirrored discs/raid arrays’ for continual backup and a removable media backup on a daily basis.
- Timing of routine backup – where a system is required on a continual basis at all hours, appropriate timeslots for backups should be determined between the users and the system management/technical staff.
- Size of backup – In conjunction with ‘regularity’, the amount of data backed up should be determined. It is not always possible to backup the entirety of data on a system due to time & capacity constraints. Therefore procedures that take backups of ‘data entered on that day’, which combined with less regular ‘full backups’ can be implemented, so that complete recovery can be achieved (up to the last ‘daily backup’) via a combination of backup tapes/CDs.
- Storage and protection of backup media – Storage should be in a location remote from the main system, but subject to at least the same environmental and physical protection as the main system. All backup media will be store in a fire safe in a different fire zone to the system that it backed up.
- As part of backup procedures regular testing and full restoration of backups to a separate system (see advice on left) should be implemented.

-
- Retention periods for backup information should be determined, with ideally at least 3 complete backup cycles in place prior to disposal.
 - Backup media should be appropriately disposed of following decommissioning.
 - Backup media should be regularly replaced to avoid wear and tear.
 - A Journal file should not be stored on the same disk as the file it is journaling.
 - All electronic mailboxes within Herefordshire Health Community will be backed up to removable media.
 - Backup media will have a minimum 10 day life cycle before being overwritten.
 - All backups will be verified by software on completion.
 - A log of the backup and verification must be automatically generated.
 - Backup software must automatically warn the Service Delivery Manager and Server Manager\Senior Technician of any backup failure.
 - A backup form will be completed for each system and signed by the person who changed the media. These backup forms will be sent to the helpdesk every Friday and will be countersigned by the Head of ICT Services.
 - Training will be available to all staff involved with the backups.
 - Regulatory and legislative requirements will be met.
 - A cleaning tape will be used on all tape drives at least once a month
 - Restoration of any data will be preformed by the system manager responsible for the system on which the data was stored.
 - A recovery test will be performed at least once every six months.
 - The Information Security Manager will randomly audit the backup logs at least twice a month.
 - Backup logs for all systems will be made available to managers of departments that make use of the system being backed up.

When determining the backup requirements of a system, the organisation will calculate the cost of system failure to the organisation, in terms of reduced efficiency (loss of staff productivity), damage and distress.

This combined with the likelihood of failure if sufficient backup is not implemented can give a rough cost of failure to the organisation in a given period. This can then be used in determining the prioritisation of resource allocated to information backup.

2.2 Operator logs

System operational staff (in IT departments typically), will maintain an activity log for each system they are responsible for. This will include:

- System start/finish times, for planned downtime, unplanned downtime and system maintenance routines.
- System error reports & corrective action taken.
- Operator identification for each log entry.

3. Implementation

This policy is supported by the following policies and procedures:

- Protection Against Malicious Software Policy (G047)
- Security Incident Management Policy (G056)
- Email Access Policy (G049)
- Internet Access Policy (G058)

The IT Services Manager is responsible for making sure all backups are complete.

All third party system suppliers must adhere to this policy.

The Information Governance Manager has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation

All system managers are directly responsible for implementing this Policy within their organisational area.

It is the responsibility of each member of staff involved with the backup and restore function to adhere to this policy.

Signature

On behalf of the Herefordshire Primary Care Trust I certify that this document is the IT Systems Backup and Restore Policy for the Herefordshire Primary Care Trust.

Name in Full:

Role:

Signature:

Date: