NHS
West Hampshire
Clinical Commissioning Group

IT BACKUP POLICY

Version 3.2

Subject and version number of document:	IT Backup Policy Version 3.2
Serial number:	COR/051/V3.02
Operative date:	1 October 2019
Author:	CSU IT Services
CCG owner:	Senior Information Risk Owner
Links to other policies:	
Review date:	September 2021
For action by:	All Staff
Policy statement:	This policy defines formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster, and allow for an efficient recovery of IT services and data in a timely manner.
Responsibility for dissemination to new staff:	Line managers at induction.
Mechanisms for dissemination:	All new and revised policies are promoted through the staff newsletter and the intranet, and published on the CCG website.
Training implications:	All staff should be made aware of where to find CCG policies at induction.
Resource implications	There are no resource implications in relation to this policy.
Further details and additional copies available from:	Website: https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Equality analysis completed?	South Central & West Commissioning Support Unit (SCW CSU) equality impact assessment framework used to evaluate this policy.
Consultation process	CSU IT Senior Leadership Team CSU IG Steering Group CSU Corporate Governance Assurance Group CCG Policy Sub Group
Approved by:	Policy Sub Group
Date approved:	11 September 2019

Website Upload:

Website	Location in FOI Publication Scheme	https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Keywords:	*Insert helpful keywords (metadata) that will be used to search for this document on the intranet and website*	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	Jan 18	Cover	Review date extended to 25 May 2018 in line with enactment of GDPR.	Jan 18
2	Aug 19		Policy reinstated. Full review. Minor amendments to content to update references to 'CSU' to 'SCW', to reflect current job titles and to include Equality Impact Assessment template. Version control brought in line with that of the CSU.	Aug 19
3				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Reviewer	Ratification Process	Notes
1.01	Sept 16	CSU IT	As detailed above	No amendment to content
3.02	Aug 19	SCW CSU Cyber Security Manager	CSU IT Senior Leadership Team CSU IG Steering Group CSU Corporate Governance Assurance Group CCG Policy Sub Group	See amend 2 above.

IT BACKUP POLICY

As the South, Central & West Commissioning Support Unit (SCW CSU) provides IT networks, equipment and support to West Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services core information security policies, in addition to those of the CCG.

The following policy was developed by the CSU IT Services Team and was adopted for use by the CCG. This has been identified as an IT Core Policy and as such cannot be amended by the CCG.

SUMMARY OF KEY POINTS TO NOTE

This document provides the policies that govern the design and operation of NHS South, Central and West CSU information technology services to ensure adequate business continuity arrangements for the CSU and all customer organisations. The table below provides details of the maximum amount of data that could be lost, together with the time to provide access to the data for end users.

	Recovery Point Objective	**Recovery Time Objective**
Business critical services	24 Hours	24 Hours
Non-Critical Services	48 Hours	48 hours
SCW hosted Email Services	< 1 hour	< 24 hours
Corporate File Shares	< 1 hour	< 24 hours
Network Drive	<12 hours (files created AM can be recovered PM)	Instant recovery from network drive 'previous versions' by end user
Network Drive Email Server, SQL Server, Other Virtual Servers	24 hours	24 hours
	This represents the maximum amount of data that could be lost	This represents the time to provide access to the data for end users

OFFICIAL

IT Backup Policy
Version 3.2

South, Central and West Commissioning Support Unit

August 2019

DOCUMENT CONTROL

Document Name	Version	Status	Author
Backup and Business Continuity Policy	*3.2*	*Final*	*Associate Director of Technology Management and Architecture*
Document objectives:	*The objective of this policy is to define formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster, and allow for an efficient recovery of IT services and data in a timely manner.*		
Target audience:	*All staff*		
Committee/Group Consulted:	*SCW Information Governance Steering Group*		
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*		
Training/resource implications:	*All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate IT policies pages*		
Approved and ratified by:	*SCW Information Governance Steering Group SCW Corporate Governance Assurance Group*	*Date: 19/08/2019*	
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*	
Date issued:	*19/08/2019*		
Review date:	***July 2021***		
Author:	*Associate Director of Technology Management and Architecture*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
13/01/2013	Matthew Rawles	0.1		Initial Draft version
26/01/2016	Mathew Rawles			Approved by SCW Corporate Governance Assurance Group, subject to review by SCW Corporate Business Manager Chris Jacobs (Business Continuity Lead for the SCW)
03/02/2016	Matthew Rawles	1.0		Updated following comments from by SCW Corporate Business Manager
08/09/2016	Arif Gulzar	1.1		Updated the policy review date
04/10/2016	Arif Gulzar	1.1		Policy signed off by Information Governance Steering Group
29/11/2016	Arif Gulzar	2.0		Version reset after ratification from Corporate Governance Assurance Group
14.12.2017	Arif Gulzar	2.1		Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group
17/05/2018	Arif Gulzar	2.2	All	Updated policy template with corporate branding. Updated the job title of Associate Director of TMA in section 2.4
21/05/2018	Arif Gulzar	2.3		Policy reviewed and approved by IT senior leadership team.
24/07/2018	Arif Gulzar	3.0		Version changed after CGAG ratification
21/06/2019	Arif Gulzar	3.1		Policy reviewed and signed off by IT senior leadership team
12/07/2019	Arif Gulzar	3.2		As per IG steering group sign off feedback, policy name is changed from Backup and Business continuity to IT Backup policy.
19/08/2019	Arif Gulzar	3.2	All	Policy ratified by SCW Corporate Governance & Assurance Group (CGAG)

Reviewers/contributors

Name	Position	Version Reviewed & Date
Simon Sturgeon	Director of IT Services	V3.1 21/06/2019
Andy Ferrari	Associate Director of IT Strategy and Planning	V3.1 21/06/2019
Cathy Jukes	Associate Director of IT Projects and Programmes	V3.1 21/06/2019
Michael Knight	Associate Director of Technology Management and Architecture	V3.1 21/06/2019
David Walch	Head of IT Service Delivery	V3.1 21/06/2019
Stephanie Wilson	Head of Service Development and Support	V3.1 21/06/2019

CONTENTS

1. INTRODUCTION

This document provides the policies that govern the design and operation of NHS South, Central and West Commissioning Support Unit (SCW) information technology services to ensure adequate business continuity arrangements for the SCW and all customer organisations.

1.1. Definitions

The following terms are used in this document;

- **Business critical systems** – As defined by our customers, these are primarily email, business critical databases and file server data
- **Recovery point objective (RPO)** – the acceptable latency of data that will not be recovered
- **Recovery time objective (RTO)** – the acceptable amount of time to restore the function to end users
- **Significant business continuity event** – an event that SCW (in consultation with its customers) determines serious enough to invoke its internal business continuity plans and the associated information systems recovery procedures within this document

2. KEY PRINCIPLES

2.1. Business continuity policy

SCW information technology solutions are designed and operated to meet the following minimum recovery objectives in a significant business continuity event.

Service	Recovery Point Objective	Recovery Time Objective
Business critical services	24 Hours	24 Hours
Non-Critical Services	48 Hours	48 hours

To achieve this objective;

- all business critical services should be replicated to an alternate SCW datacentre location at least once a day
- all non-critical services must have a backup copy in an alternative SCW datacentre, copied once a day
- recovery hardware must be available to restore services from replicas or backup copies

Typically funding for infrastructure for business continuity will not exceed 25% of the total annual infrastructure cost. Performance of systems in a disaster recovery

event are expected to be below normal operational levels, with priority given to critical business services.

Non-critical services may remain unavailable to end users for extended periods to ensure resources are available for critical systems.

Customers requiring high levels of performance in a disaster recovery scenario are required to provide additional funding for dedicated hardware.

IT Services will agree with customers which solutions are business critical and support annual testing of the recovery of these services in a controlled recovery environment.

2.2. Business continuity of high availability solutions

Where practical, solutions will be engineered to exceed these objectives. Typically this is where a technology provides a high availability service that can be located in multiple SCW datacentres.
Depending on the nature of the failure access to these services may not be available for up to 24 hours although data loss is minimised.

	Recovery Point Objective	**Recovery Time Objective**
SCW hosted Email Services Utilising real-time data availability group replication	< 1 hour	< 24 hours
Corporate File Shares Utilising real-time distributed file system replication (DFSR)	< 1 hour	< 24 hours
	This represents the maximum amount of data that could be lost	This represents the time to provide access to the data for end users

2.3. Backup and restore policy

SCW information technology solutions are designed and operated to minimise the impact of accidental data loss. The table below details theSCW policy on the expected level of backup and recovery of key technology solutions:

Solution (Backup Technology)	**Backup interval**	**Recovery Point Objective**	**Recovery Time Objective**	**Backup Retention**
Network Drive (Volume Shadow Copy)	Twice daily, typically 8am and 12pm	< 12 hours Files created AM can be recovered PM.	Instant recovery from network drive "previous versions" by end user.	32 days, 2 backups a day.
Network Drive Email Server (Server image)	Daily	24 hours	24 hours	30 days of daily backups 12 weeks of weekly backups 13 months of monthly backups
SQL Server (SQL database backup)	Daily	24 hours	24 hours	30 days of daily backups 13 months of monthly backups
Other Virtual Server[1] (Server image)	Daily	24 hours	24 hours	30 days of daily backups

[1] any server supporting a service with no long term file recovery requirement, examples include terminal servers, web servers etc.

Volume Shadow Copy – a Microsoft technology to create "recovery points" within a server, typically a file server supporting a network drive, end users can recover files directly from network drives.

Server Image – a style of backup where the entire server is included in the backup, typically supporting both full sever and individual file recovery, recovery times are slower than volume shadow copy although they can be typically less than the 24 hours stated (depending on the nature and age of the restored data)

SQL database backup – managed within the database application, backups written to a dedicated network area to enable full or partial recovery of specific databases.

2.4. Procedures for business continuity, backup and restore

The SCW will maintain detailed procedures to cover;

- Backup of all services
- Recovery of files and/or services from backup
- Business continuity arrangements
- Testing of backup and business continuity arrangements
- Checklists for operational staff on common recovery processes

The Associate Director of Technology Management & Architecture is responsible for the maintenance of the operation procedures that underpin this policy.

Appendix A - Equality Impact Assessment

For IT Backup Policy

1.	**Title of policy/ programme/ framework being analysed** **IT Backup Policy.**
2.	**Please state the aims and objectives of this work and the intended equality outcomes. How is this proposal linked to the organisation's business plan and strategic equality objectives?** **The objective of the IT Backup Policy is to define formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster, and allow for an efficient recovery of IT services and data in a timely manner.**
3.	**Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers** **Staff.**
4.	**What evidence do you have of the potential impact (positive and negative)?** **None expected.**
4.1	**Disability (Consider attitudinal, physical and social barriers)** **No impact**
4.2	**Sex (Impact on men and women, potential link to carers below)** **No impact**
4.3	**Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences).** **No impact**
4.4	**Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare).** **No impact**
4.5	**Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment)** **No impact**
4.6	**Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people).** **No impact**
4.7	**Religion or belief (Consider impact on people with different religions, beliefs or no belief)** **No impact**
4.8	**Marriage and Civil Partnership** **No impact**
4.9	**Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities).** **No impact**
4.10	**Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation).** **No impact**

4.11 Additional significant evidence (See Guidance Note)

Give details of any evidence on other groups experiencing disadvantage and barriers to access due to:

- **socio-economic status**
- **location (e.g. living in areas of multiple deprivation)**
- **resident status (migrants)**
- **multiple discrimination**
- **homelessness**

No impact

5. **Action planning for improvement (See Guidance Note)**

Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.

Sign off

Name and signature of person who carried out this analysis
Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit

Date analysis completed
23rd July 2018

Name and signature of responsible Director
Simon Sturgeon, Director of IT Services

Date analysis was approved by responsible Director
Director of IT Services
23 July 2018