NHS
North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

IT Services - Backup and Business Continuity Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer:	Matthew Rawles, Head of IT Enterprise Architecture & Design
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Review date:	25/05/2018
Target audience:	All NHS South, Central &West CSU staff and Customers

Document Control Sheet

Title	**IT Backup and Business Continuity Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Matthew Rawles – Head of IT Enterprise Architecture & Design
Date Created	13/01/2016
Date Last Updated	14.12.2017

History			
Version	Date	Author(s)	Comments
0.1	13/01/2013	Matthew Rawles	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 CSU)
1.0	03/02/2016	Matthew Rawles	Updated following comments from by SCW Corporate Business Manager
1.1	08/09/2016	Arif Gulzar	Updated the policy review date
1.1	04/10/2016	Arif Gulzar	Policy signed off by Information Governance Steering Group
2.0	29/11/2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14.12.2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	**Title and contact**
Catherine Dampney	CIO
Phil Evans	Associate Director of IT Services

Contents

1 Introduction

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

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

	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 CSU datacentre location at least once a day
- all non-critical services must have a backup copy in an alternative CSU 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 availably service that can be located in multiple CSU 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**
CSU 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

CSU information technology solutions are designed and operated to minimise the impact of accidental data loss. The table below details the CSU 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 CSU 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 Head of Technology Management and Operations is responsible for the maintenance of the operation procedures that underpin this policy.