HIC SERVICES STANDARD OPERATING PROCEDURE

Maintenance of IT Infrastructure

SOP NUMBER:	SOP 11
VERSION NUMBER:	7.1
EFFECTIVE DATE:	
DOCUMENT SECURITY LEVEL:	Open
REVIEW DATE:	This SOP will be reviewed at least every 12 months, or at other times as requested by: HIC Information Governance Committee
AUTHOR:	Matt McGowan
DATE APPROVED BY THE INFORMATION GOVERNANCE COMMITTEE:	15/11/2022
DATE APPROVED BY THE HIC EXECUTIVE COMMITTEE:	__/__/2022
DATE REVIEWED BY HIC OPERATIONS GROUP:	24/10/2022
CONTACT PERSON FOR THIS SOP:	Infrastructure Team Lead

DOCUMENT REVIEW AND REVISION HISTORY:

Version Number:	Edited by (job title):	Effective Date:	Details of editions made:
1.0	Kevin Moran (IT Manager)	01/09/13	New SOP
2.0	Chris Scott (Senior IT Infrastructure Specialist)	01/01/15	Complete review and update
3.0	Matt McGowan (Infrastructure Security Specialist)	01/01/16	Reviewed and updated to reflect network changes
4.0	Chris Hall (Senior Data Analyst) / Guney Hanedan (IT Manager)	01/03/16	Reviewed and updated Backup section 5.2 and Change Control section 5.3.
4.1	Howard Rogers (Snr Infrastructure Specialist)	01/03/18	Removed Mackenzie building reference from section 5.2
5.0	Duncan Heather (HIC Governance Manager)	08/11/18	Update to reflect GDPR
6.0	Kenny Gillen (Senior Infrastructure Specialist)	10/06/19	Clarifications
	Tracey Stewart (Data Entry Team Leader)	24/02/20	Updated cover sheet with new approval process information.
	Rachael Torano (Business Support)	15/05/20	Updated with new and approved Header Changes made to cover page to include Op's review date as agreed at the HIC Information Governance Meeting Document Review and Revision History table header updated As agreed by the HIC Governance Committee signatures have been removed from cover page and Document Review and Revision History table has been updated to include review dates and notes

7.0	Ian Fletcher (Senior Cyber Security Infrastructure Specialist)	10/09/2021	Minor grammatical and punctuation amendments and addition of Cloud services
7.1	Simon Li (Senior Infrastructure Specialist)	15/11/2022	Amended purpose to define cloud and added cloud provider failure section

Draft and Archived/Obsolete revisions are not to be used.
Access current versioning system to verify revision.

Table of Contents

1. PURPOSE

Health Informatics Centre (HIC) is a University Research Support Unit operating within the Tayside Medical Science Centre (TASC) at the University of Dundee, in collaboration with NHS Tayside and NHS Fife. HIC Services provides Data Users with linked, anonymised information derived mostly from large population-based health datasets, owned mainly by the NHS and the University of Dundee. HIC also develops data collection software, provides data entry services, web development services and provides secure access to research data.

This SOP describes the relevant monitoring and data management systems that are being used within HIC Services. These systems may be hosted in on-premise data centre or with a cloud service provider.

2. SCOPE

This SOP covers the IT Infrastructure hardware and software products that are owned or used exclusively by HIC Services. It does not cover products or services owned or provided by the wider University or by NHS Tayside.

3. DEFINITIONS

For overall definitions see HIC Services SOP Appendix B - Definitions.

4. RESPONSIBILITIES

- IT Administrators - Responsible for all IT Infrastructure procedures

5. POLICY

For overall policy see HIC Services SOP Appendix A - Policy.

5.1 Monitoring

Monitoring of the Infrastructure services is provided in the following categories:

i. Availability - servers are monitored internally and externally.
ii. Security - security related events are logged on individual servers.
iii. Forensic - security related events from the last 30 days are collected and stored centrally to assist in the diagnosis of any reported breaches of network security.
iv. External services - HIC services available on the public Internet such as websites are monitored remotely in order to collect performance and availability data.

5.2 Backup

For the protection of data, a backup system appropriate to the environment is employed:

For all data and relevant virtual machines residing in all HIC data centres, the following procedure is followed:

i. Data is backed up within a schedule based on the type of data.
ii. Local backups are taken to primary site backup media or disks.
iii. Disaster Recovery (DR) site backups are transferred to DR site media or disks from the primary site backup location.
iv. Data and system configuration in cloud providers is backed up using the appropriate backup service offered by the provider.
v. Automated reports on the status of the previous night's backups are available and checked by the IT administrator(s) as part of routine monitoring activities.
vi. Details of backup schedules, media used, source and destination storage locations, and data retention periods are reviewed in the Service Description for backup provision for the appropriate HIC data domain.

5.3 Change Control

There is a weekly maintenance period for performing planned changes to IT Infrastructure.

5.4 Security Patching

Windows servers and desktops:

i. All servers running a supported version of Windows are patched using a centrally managed service. Security patches are applied regularly according to a rolling schedule.

Unix and Linux servers:

i. All servers running a supported version of Unix or Linux are patched by an IT Administrator using a manual process.

5.5 Hardware Failure

i. In the event of hardware failure an IT Administrator will contact the appropriate Supplier to request support.
ii. If a site visit is required from a supplier representative, this will be carried out under the supervision of a HIC IT Administrator. At no time will hardware containing data leave the IT Server Room/s.
iii. For hardware that is not covered by a supplier warranty or support agreement, internal investigation and remediation activities will be undertaken.
iv. If the hardware failure has resulted in a service outage, a HIC IT Administrator will report the status and progress of any hardware fault to the relevant stakeholders.

5.6 Cloud Service Provider Failure

i. In the event of a failure on a cloud service provider an IT Administrator will attempt to restore the service
ii. If the service cannot be restored the IT Administrator will open a support ticket with the cloud provider.
iii. If the failure has resulted in a service outage, a HIC IT Administrator will report the status and progress of any resolution to the relevant stakeholders.

5.7 Disposal of Assets

i. All local storage from equipment that is to be decommissioned are removed for destruction using the secure disposal service provided by the University of Dundee unless the local storage has hardware encryption enabled or is securely erased before leaving HIC's control, in which case they may be repurposed. The following configuration details are recorded for each device:
    a. The type of device.
    b. Encryption type and state.
    c. Whether a secure erase was performed.

    For each disposal, the total number of devices is matched with the data available on the receipt from UoD IT or their contracted secure disposal service.
ii. All hardware that has been decommissioned is disposed of using the standard, environmentally friendly, service provided by the University of Dundee. All hardware disposals are recorded in the Asset Register.

6. APPLICABLE REFERENCES

i. HIC Services SOP 01 HIC Data Security
ii. HIC Services SOP 02 Data Access Approvals
iii. HIC Services SOP 03 Handling HIC Significant Events
iv. HIC Services SOP Appendix A Policy
v. HIC Services SOP Appendix B Definitions
vi. HIC Services Service Description 11 - Server Backup Provision for DATAENTRY domain
vii. HIC Services Service Description 16 - Safe Haven Backup Provision