Maintenance of IT Structure

PURPOSE

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.

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.

RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Administrators	Checking backup status reports, contacting support in cases of hardware failure, restoring service in event of cloud failure

PROCEDURE

Policy

For overall policy see Legal and Governance Policy.

Principles

1. **Monitoring:** Services running in cloud environments rely on the service provider's recommended service for monitoring. For example, in the case of containerised applications, a health check command is executed periodically to verify availability.
2. **Logging:** Where possible, logs are collected and stored centrally using an appropriate service for the given environment.
3. **Back up:** For the protection of data, a backup system appropriate to the environment is employed. Cloud based resources are backed up using the service provider's recommended backup solution at regular intervals.
4. **Anti- Malware Controls:** We deploy and manage a commercial anti-virus package within all of our environments. This is compatible with our on-premises equipment and cloud-based resources.
5. **Clock Synchronisation:** On-premises servers are to synchronise their time with domain controllers using NTP. In our Cloud environments, we rely on the operating system distribution's default configuration.
6. **Change Control:** There is a weekly maintenance period for performing planned changes to IT Infrastructure.

Steps

1. Monitoring of the Infrastructure services is provided in the following categories:
    a. *Availability* - servers are monitored internally and externally.
    b. *Security* - security related events are logged on individual servers.
    c. *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.
    d. *External services* - HIC services available on the public Internet such as websites are monitored remotely in order to collect performance and availability data.
2. For all data and relevant virtual machines residing in all HIC data centres, the following back up procedure is followed:
    a. Data is backed up within a schedule based on the type of data in line with our disaster recovery plan.
    b. Local backups are taken to primary site backup media or disks.
    c. Disaster Recovery (DR) site backups are transferred to DR site media or disks from the primary site backup location.
    d. Data and system configuration in cloud providers is backed up using the appropriate backup service offered by the provider.
    e. 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.
    f. 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.
3. Security Patching
    a. On-Premises Windows servers and desktops: 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.
    b. On-Premises Linux servers: All servers running a supported version of Unix or Linux are patched by an IT Administrator using a manual process.
    c. Cloud Hosted Windows Servers: Windows Updates are applied automatically. These are rebooted during our maintenance window to ensure patches have been applied.
    d. Cloud Hosted Linux Servers: Cloud provisioned Linux servers are configured at first boot to apply unattended upgrades and reboots.
4. Hardware Failure
    a. In the event of hardware failure an IT Administrator will contact the appropriate Supplier to request support.
    b. 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.
    c. For hardware that is not covered by a supplier warranty or support agreement, internal investigation and remediation activities will be undertaken.
    d. 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. Cloud Service Provider Failure
    a. In the event of a failure on a cloud service provider an IT Administrator will attempt to restore the service.
    b. If the service cannot be restored the IT Administrator will open a support ticket with the cloud provider.
    c. 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.
6. Disposal of Assets
    a. 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 (retired media is securely overwritten before formatting). The following configuration details are recorded for each device:
        - The type of device.
        - Encryption type and state.
        - Whether a secure erase was performed.

b. 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.

c. 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.

APPLICABLE REFERENCES

- Data Security
- Data Access Approvals
- Significant Events
- Legal and Governance Policy
- *DATAENTRY Veeam Backup*
- For Definitions see ISMS Glossary

DOCUMENT CONTROLS

Process Manager	Point of Contact
Jenny Johnston	hicbusiness-support@dundee.ac.uk

Revision Number	Revision Date	Revision Made	Revision By	Revision Category	Approved By	Effective Date
1.0	01/01.24	Moved SOP to Confluence from SharePoint and updated into new template	Bruce Miller and Symone Sheane	Superficial	HIC ISMS team member	10/01/24
1.1	04/04/24	Updated Roles and Responsibilities	Bruce Miller	Superficial	HIC ISMS team member	5/04/24
1.2	10/04/24	Formatted document control table and added in revision category	Symone Sheane	Superficial	HIC ISMS team member	10/04/24