# Scope and Requirements

The scope of this directive is:

**Confidentiality** requirement is high

**Integrity** requirement is high

**Availability** requirement is low

# Approach

Disaster recovery and business continuity requirements is treated proportionately to its availability requirements.

# ROles and Responsibilities

[Unit Head] is accountable for business continuity management within the unit, and is responsible for initiating the the Disaster Recovery and Business Continuity plans into action.

[Senior Officer] is accountable for implementing the plan within the defined timeframe, including carrying out awareness activites and tests as required. [Senior Officer] is also accountable for keeping documentation up to date upon changes to staff, technologies or processes involved in the processes.

[Line Managers] are responsible for reporting incidents from their staff to relevant incident response teams and [Senior Officer], and for informing [Senior Officer] of any changes that affect the business continuity management.

[IT manager] is accountable for implementing the IT disaster recovery plan into action.

**All users** are responsible for using approved procedures for back up and storage of information, and undertaking in related activities as required.

# HOW TO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | **Scenario** | **Initial response** | **Authority** | **Communications method** |
| 1 | **Loss of datasets** | Instruct staff to stop working until data restored | [Unit Head] | Email |
| 2 | **Loss of collaboration environment as well as datasets** | Instruct staff to stop working until data restored | [Unit Head] | Email |
| 3 | **Security incident** | OxCERT and Data Breach teams (if applicable) to be notified, and investigated.  | [Line Manager] | Email to <IT Manager>, Line Manager and oxcert@infosec.ox.ac.uk; data.breach@admin.ox.ac.uk  |

The following scenarios affect the systems, individuals and processes within the scope of the policy. Any scenarios likely to affect more than one system within the [unit] will be accounted for in wider Business Continuity arrangements.

# Scenario 1: Loss of datasets

[Unit Head] initiates the disaster recovery plan, and notifies [Senior Officer].

[Senior Officer] shall call upon IT Manager and request recovery of analysis data, and inform all users affected to temporarily stop activities relating to data until further notice.

[Senior Officer] may call upon an experienced staff member for any questions around data quality and or related checks.

[IT Manager] shall recover dataset from available backups at:

* Hot site:
* Warm site:
* Cool site:

Once complete, [IT Manager] will notify Senior Officer.

[include what you might do if the backups are irretrievable.

[Senior Officer] closes the incident, and notifies staff.

# Scenario 2

[Unit Head] initiates the disaster recovery plan, and notifies [Senior Officer].

[Senior Officer] shall call upon IT Manager and request rebuild of the collaboration environment, and inform all users affected to temporarily to stop activities within the collaboration environment.

Senior Officer may call upon an experienced staff member for any questions around data quality and or related checks.

[IT manager] shall complete the rebuild of the environment from documentations and hardening guides available at:

<LINK>

To recover datasets, follow scenario 1.

Once complete, the [IT Manager] will notify Senior Officer.

[Senior Officer] closes the incident, and notifies staff.

# Scenario 3

[Line Manager] reports any incident to [IT Manager] and OxCERT and Information Compliance team for investigation within 4 working hours of discovery. Use out of office contact if the incident takes place after office hours.

Any breaches involving personal data needs to be reported to the Information Compliance team immediately.

[IT Manager] works with OxCERT as required to isolate affected systems from the network, investigate and mitigate the root cause of incident and then restore accesss once resolved.

Once complete, the [IT Manager] will notify Line Manager.

[Line Manager] closes the incident, and notifies staff.

# REview

This plan must be reviewed and updated annually, and following changes to personnel, organisational strategy, hardware, software, network, applications, data and communication technologies and methods.

# Contacts

**Out of hours contacts for:**

Security Services: 01865 (2)89999

[Unit Head]:

[Senior Officer]:

OxCERT: oxcert@infosec.ox.ac.uk or 01865 (2)83409 (Emergency:7812 215 375)

**During Office hours:**

[Unit head]:

[Senior Officer]:

[IT Manager]:

OxCERT: oxcert@infosec.ox.ac.uk or 01865 (2)82222

Information Compliance team: data.breach@admin.ox.ac.uk

# Baseline Controls

OPS.03 Maintain plans to restore critical services and systems within an acceptable time period following a compromise or loss of availability.

OPS.04 Take appropriate measures to support the implementation of a disaster recovery plan, including the following:

• Maintaining standard build instructions or build images to allow timely system restoration;

• Retaining secured off-site copies of custom software relied upon by the server;

• Retaining secured backups of critical data.

OPS.05 Test service recovery procedures periodically to ensure that systems can be recovered when required.