University of East Anglia

ICT Contingency Plan

Top Level Plan

Document Control Information

Title:	ICT Contingency Plan: Top Level Plan
Date:	June 2013
Version:	3.0
Authors:	John Redeyoff (NCC) Contents by Neil Dudleston / Bryan Scaife (NCC); Jonathan Colam-French, Raymond Scott, Iain Reeman (UEA)

REVISION	DATE	REVISION DESCRIPTION
0.1		Draft
0.2		Updated draft
0.3	September 2005	Split out from original 'Strawman'
1.0	October 2005	Updated, QA'd and issued
1.1	January 2008	Updated with changes from Jonathan Colam
1.2	February 2008	Some typographical errors corrected
1.3	May 2009	Minor service changes
2.0	June 2010	Updated following review
2.1	June 2010	Updated location of DR DVD
2.2	May 2013	Reviewed and updated with details on location of Service Catalogue and DR Plans
3.0	June 2013	Approved by ISSC

Contents

1	Executive Summary	4
2	Introduction and Overview	5
	2.1 Introduction	5
	2.2 Overview	5
3	Impact Assessment and Incident Management	6
	3.1 Impact Levels	6
	3.2 Levels of Control	7
	3.3 Impact Handling	7
4	Impact Management Procedures	8
	4.1 Calling an Impact Assessment Level	8
	4.2 The Incident Management Process	8
5	Incident Management	10
	5.1 Management of Extreme Impact Incidents	10
	5.2 Management of Significant and Minor Incidents	10
6	Process	12
	6.1 Incident Management Definition	13
	6.2 Operational Team Management	14
	6.3 Crisis Management	15
7	Ownership, Contacts and References	16
	7.1 Ownership	16
	7.2 Internal and External Contacts	16
	7.3 Documentation and References	16
	7.4 DR DVDs	18
8	Testing and Updating the Plan	19
	8.1 Disaster recovery test	19
	8.2 Plan update process	20
	8.3 Update cycles	20
9	Appendix: Recovery Time and Recovery Point	21
	9.1 Recovery Time	21
	9.2 Recovery Point	21
	9.3 RTO and RPO references	21

1 Executive Summary

Information Communications and Technology (ICT) are essential elements in the majority of the University's processes. Reflecting this, it is required that critical ICT resources are able to operate effectively, without excessive interruptions affecting operations.

Contingency planning for ICT supports this requirement by establishing plans and procedures, along with technical measures, that enable critical systems to be effectively recovered in agreed timeframes following a service disruption, outage or disaster. ICT systems are vulnerable to a variety of service disruptions, ranging from severe (e.g. fire) to mild (e.g. short-term power loss). Whilst much vulnerability can be reduced to acceptable limits through technical, administrative and operational controls as part of the University's risk management policy, it is impossible to completely eliminate all risks.

The management team of the University of East Anglia (UEA) is committed to ensuring that the information processing systems that are critical to the university are maintained and protected against relevant threats and that the organisation has the ability to recover systems in a timely and controlled manner. The management process that provides the contingency planning for these systems is described herein.

This document sets out, at a high level, the ICT Contingency Plan for UEA. It is supported by a number of documents which set out, in detail, the procedures to be followed in the case of individual system failures.

See also the supporting documentation listed in the references section (p. 16).

This document describes the management process for contingency planning. The actual work involved in recovering services is described at an individual service level within the DR Plans documentation produced for those services.

The central provision and management of Information Communications and Technology is part of the remit of the Information Services Directorate (ISD). ISD is also responsible for provision of Library Services for which a separate contingency plan (the Library Business Continuity and Disaster Recovery Plan) exists. That plan covers physical resources and services. Should an IT-related incident arise within the Library, the ICT contingency plan will take precedence.

2 Introduction and Overview

2.1 Introduction

The purpose of this document is to provide at a high level a succinct description of the holistic management process and guide for the recovery of the information systems and associated processes immediately following an incident interrupting service. It represents the assertion of control to minimise the impact on University business.

This document only considers restoration of ICT services within the University and as such forms one part of a comprehensive University-wide business continuity plan (BCP).

The scope of this document is specifically fixed at centrally-managed systems. For those systems that are locally managed (e.g. within schools), it is assumed that the local management has put in place appropriate arrangements.

2.2 Overview

The basis of such contingency planning is:

(a) the identification that an incident has occurred and the classification of the incident in terms of its impact,

(b) asserting the appropriate level of control over the incident to be able to recover the systems effectively,

(c) ensuring that following an incident steps are taken to minimise potential for reoccurrence.

2.2.1 Impact Levels

Any given incident is assessed in terms of its impact. An incident can be considered **Extreme, Significant or Minor.** Section 3.1 sets out the three levels of impact.

2.2.2 Levels of Control

There are four levels of control which are brought into play in the event of an incident. These are: **Strategic**; **Tactical**; **Operational**; **and Local**. Section 3.2 sets out the four levels of control.

3 Impact Assessment and Incident Management

3.1 Impact Levels

Information Systems Contingency Planning can be associated with the loss of any critical system or network, or part thereof that may deny access to systems or significantly hinder the effective operations of the University in providing student, academic, administrative or external information services.

The impact of the loss can be graded as Extreme, Significant or Minor with the following broad definitions:

Impact	Description
Extreme	The most serious impact where the entire network is unavailable or a large percentage of schools/faculties have lost communications to central systems or central systems have failed or there has been an incident that affects the campus as a whole (i.e. evacuation or data centre fire); or The effect, whilst originally Significant, has been in play for such a period of time that it has been escalated to 'extreme'.
Significant	The effect on the University system is significant and affects multiple user groups, or multiple schools/faculties. Key university systems are affected and/or significant parts of the network are unavailable; or The effect, whilst originally minor, has been in play for such a period of time that it has been escalated to 'significant'.
Minor	The effect on the University systems or network is minimal. Minor inconvenience to a specific group of users. Note that 'minor' incidents are, by definition, limited in their impact to a particular unit of operation rather than being University-wide. Therefore: (a) If a 'minor' inconvenience is felt University-wide, then it will be considered significant; and (b) If a 'significant' incident is limited in its scope to a small group of users, it can in some cases be regarded as 'minor' at the University level.

Note that the concept of escalation exists, in that an incident can be escalated from *minor* to *significant* and even to the point of *extreme.*

3.2 Levels of Control

Level	Description
Strategic	This refers to senior university managers who make strategic decisions about the priorities of the University. In an extreme incident such as an evacuation of the campus this team would control the communications channels and communicate strategic decisions directly to the tactical team.[1]
Tactical	A senior management team of subject matter experts within the University. They are responsible for coordinating and directing the operational resources of the University to ensure that the contingency plans are being properly executed.[2]
Operational	Provided by the technical staff who have the detailed knowledge and capability to reconstitute systems with a clear understanding of what needs to be done and how.[3]
Local	The management of incidents in relation to systems that are 'local', i.e. are not supported by ISD.

Not all incidents will require strategic or even tactical control; however this is entirely dependent upon the incident and the severity of the impact upon the effective running of the University. In the majority of ICT related incidents, tactical control will suffice.

3.3 Impact Handling

Impact	Handling Arrangements
Extreme	Managed at a Strategic Control level, with the Strategic Control team relaying instructions and priorities to the appropriate staff.
Significant	Managed at Tactical Control level with the Tactical Control team relaying instructions to the appropriate staff and coordinating information and reporting to the Strategic Control team as appropriate.
Minor	Routinely handled by Operational Control staff.

[1] Strategic control is often referred to as 'Gold Command' in crisis management terminology.
[2] Tactical control is often referred to as 'Silver Command' in crisis management terminology.
[3] Operational control is often referred to as 'Bronze Command' in crisis management terminology.

4 Impact Management Procedures

4.1 Calling an Impact Assessment Level

4.1.1 Minor Incidents

Minor incidents will be identified, addressed and logged routinely by operations staff and would not require the intervention of a tactical team. For example, the loss of a server or network router may require a routine reset of the machine and this may resolve the incident. In the case the operations staff will make the call, resolve the incident and this would not be reported to higher levels of control.

In the case that an incident is not considered to be minor, either by virtue of its impact or due to what is estimated to be a prolonged recovery time, it will be escalated to significant level or, in extreme circumstances, to extreme level.

4.1.2 Significant Incidents

A significant incident is called by the Director responsible for managing the systems/network affected. This may be a direct call (due to the obvious severity of the incident) or as a result of the incident having been escalated by the operations staff.

4.1.3 Extreme Incidents

An extreme incident is called by the Director of Information Services. This may be a direct call (due to the obvious severity of the incident) or as a result of the incident having been escalated by the operations or tactical management staff.

In cases where the incident is considered to be so serious in its nature that it has a significant impact upon the continuing operation of the University, the Strategic Incident Management team will escalate the incident to the Executive Team where it will be managed under the University-wide Business Continuity Planning process.

4.2 The Incident Management Process

The following table provides an overview of the approach to recovering from a disaster or incident.

Stage	Action	Details
Incident reported	Declaration and impact assessment	▪ Actions to be considered within this phase are contained within the contingency plans. ▪ The plan is invoked immediately following the declaration of an incident.

Stage	Action	Details
Stage 1 Emergency response	Damage assessment and resumption plan	▪ This phase may last for a few minutes or a few hours following the incident reported phase. ▪ During this time the disaster situation has to be assessed and decisions made quickly as to the course of action.
Stage 2 Recovery process	Continuity actions	▪ This phase may last several hours or several months following the incident. ▪ It ends when normal operations can restart. During this phase essential operations will restart and continue in recovery mode. ▪ It will require actions from nominated personnel within the University
Stage 3 Restoration of service	Restoration actions	▪ During this phase conditions at UEA are restored to as near normal as practical. ▪ Planning for this phase may start at the same time as the incident occurred. However, if there was significant physical damage to infrastructure this phase will not occur until a much later date.
Stage 4 Review	Review and service improvements	▪ During this phase the service risk log is reviewed and updated. ▪ The incident is reviewed to identify any actions, changes or investments which can be made to reduce the risk of recurrence of the incident

5 Incident Management

5.1 Management of Extreme Impact Incidents

Extreme impact incidents are managed by the Strategic Management Team.

5.1.1 Strategic Management Team Responsibilities

The team carries out and carries responsibility for the following:

(a) Communication with key stakeholders

(b) Escalation, if necessary, to ET for invocation of UEA Business Continuity Plans

(c) Decision to implement any resolution plans proposed by the tactical management team

(d) Planning of and movement to alternate site if appropriate

(e) Approval of damage assessment and negotiation with insurers

(f) Media contact if required

(g) Provision of management control and strategic direction

(h) Approval of emergency equipment purchases

(i) Securing financial and human resources as required

(j) Approving all actions not pre-planned

(k) Resolving issues of priority to the University

See the document *DR Contacts* which sets out the makeup of the Strategic team.

5.2 Management of Significant and Minor Incidents

Minor incidents are handled routinely by Operations Staff. They will only be escalated to the status of a Significant incident in the case that:

(a) The failure is part of a pattern, leading to multiple incidents; or

(b) It is apparent that the Recovery Time objective or the Recovery Point objective will not be met.

5.2.1 Tactical Management Team Responsibilities

(a) Escalation, if necessary, to Extreme impact and the passing of control to the Strategic Management team. This must always be carried out if it is recognised that any of the activities defined in (a) through (k) in section 5.1.1 above are required.

(b) Communication with key stakeholders

(c) Decision to implement any resolution plans proposed by operational staff

(d) Approval of damage assessment and negotiation with insurers

(e) Provision of management control and tactical direction

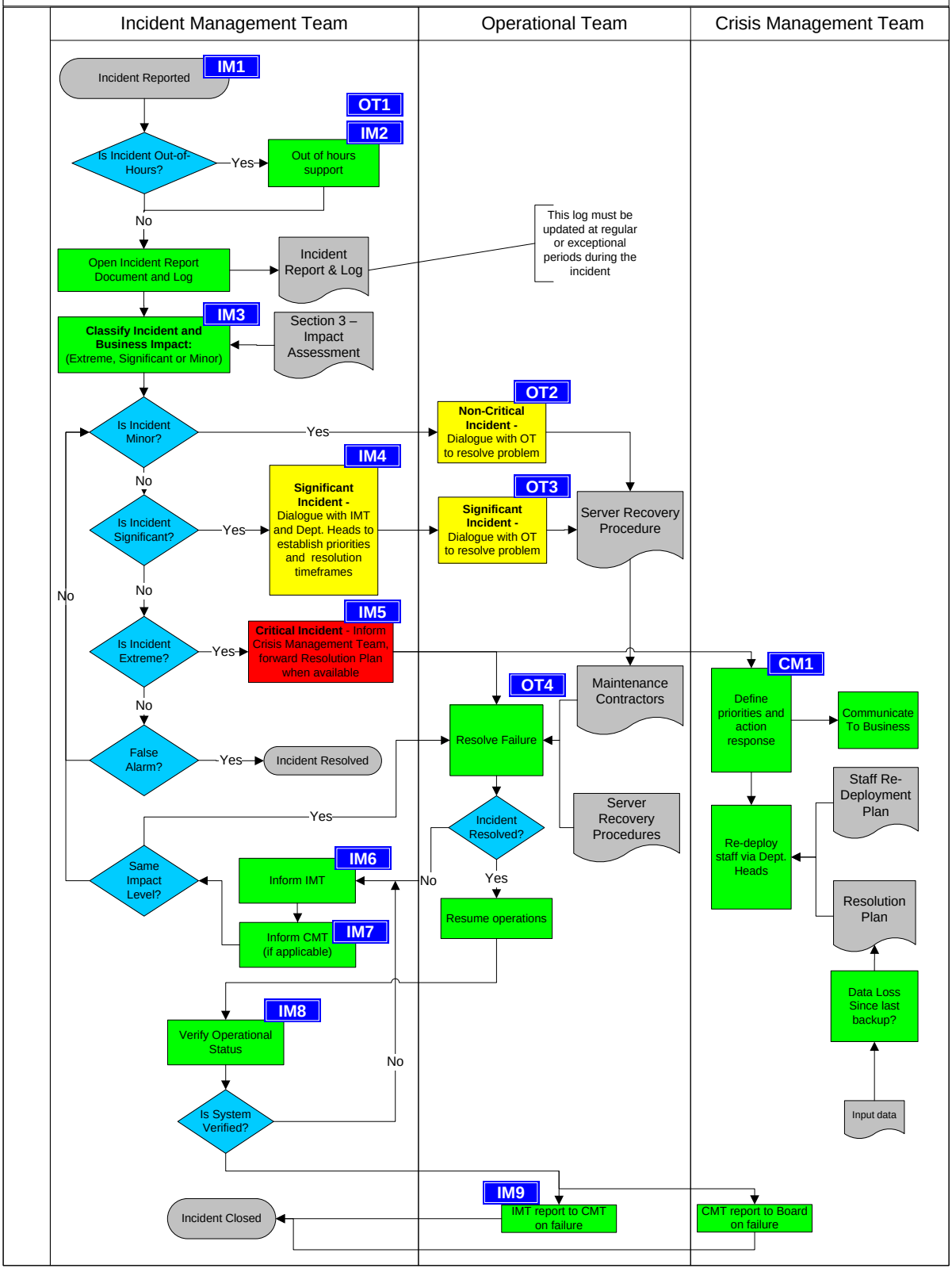
(f) Securing financial and human resources as required

(g) Approving all actions not pre-planned

See the document *DR Contacts* which sets out the makeup of the Tactical team.

6 Process

Internal Server Loss - Loss means entire loss due to mechanical or electrical failure of server units. It is assumed that if the loss occurs due to a major destructive event, then the response to the destructive event will override this procedure.



6.1 Incident Management Definition

Process ID	Owner	Explanation
IM1	All IT staff	The servers are monitored and during supported hours IT would either be notified via the help desk or by monitoring systems. Users would inform the help desk of problems that would lead to IT investigating the cause. The Help Desk shall monitor all calls associated with this procedure. When the incident (of any classification) cannot be resolved within the RTO the Help Desk shall escalate to the IMT. The IMT may reclassify the incident and as a result escalate further to the CMT.
IM2	IMT	There is no out of hours support unless systems are covered in the out of hours scheme[4]. Staff may work overtime as agreed.
IM3	IMT	The IMT shall classify the incident in terms of business impact effect on the University. This then determines the management structure required to coordinate the subsequent events.
IM4	IMT	IMT coordinates dialogue with IMT and Dept. Heads to establish business priorities and tolerable resolution timeframes. The IMT then coordinates this with IT (ID: OT3)
IM5	IMT	This is the most severe incident that renders major services unavailable. The IMT informs the Crisis Management Team who defines the business priorities and delegates coordination to Dept. Heads.
IM6	IMT	IMT will reassess the impact and determine what additional or new actions are required. This may involve escalation to the CMT for special handling.
IM7	IMT	The IMT will inform the CMT, should they have been convened, such that management can reassess business priorities and determine what the short, medium and long term recovery/backlog effects the incident had, such that management can formulate plans for

[4] Details on the ISD OOH Scheme including a list of covered services are in the proposal document in the \Centralvfs-OOH\Private\Admin folder on the DR DVDs.

The ISD Service Catalogue lists all services covered by the OOH scheme.

Process ID	Owner	Explanation
		resumption of normal operations.
IM8	IMT	Following a server failure the IMT will determine which, if any, user data verification is required to ensure that the system has been restored to a business operational status. The functionality of the system shall also be verified as well as interfaces, communications and links to dependent systems.
IM9	IMT	The IMT shall conclude (including the CMT if appropriate) that the incident is resolved and systems have been returned to full operational status. All logs are updated and closed. The log information should be used to determine if events could have been avoided and used to learn from experience of how the incident was handled. IMT prepare report to CMT based on incident log. CMT to summarise report and submit to CMT Director.

6.2 Operational Team Management

Process ID	Owner	Explanation
OT1	OT	There is no out of hours support unless systems are covered in the out of hours scheme[5]. Staff may work overtime as agreed.
OT2	OT	ISG control the incident and perform routine measures to restore services.
OT3	IMT	IMT control the incident and converse with OT on the options for recovery given the tolerable recovery timescales. These details are fed back to the Dept. Heads who can make continued and informed decisions on how best to utilise their affected staff. ISG perform routine or special (as defined by

[5] Details on the ISD OOH Scheme including a list of covered services are in the proposal document in the \Centralvfs-OOH\Private\Admin folder on the DR DVDs.

The ISD Service Catalogue lists all services covered by the OOH scheme.

Process ID	Owner	Explanation
		the IMT and ISG) measures to restore services.
OT4	OT	OT will determine, from a technical standpoint, if the incident has been resolved. If the Incident is not resolved OT will inform the IMT (ID: IM6) who will reassess the impact. OT will continue to resolve the incident but the escalation of management control may result in different action plans. Where the incident cannot be resolved within the RTO then the IMT shall notify, at the earliest opportunity, the CMT who will approve escalation procedures and alternative actions. The CMT may allocate a specific management duty to another staff member to pursue specific corrective actions.

6.3 Crisis Management

Process ID	Owner	Explanation
CM1	CMT	This is the most severe incident that renders a major system unavailable. The IMT has informed the Crisis Management Team who has the responsibility to define the business priorities and delegate coordination of action plans to Dept. Heads. The Dept. Heads will manage their staff accordingly which may include re-deployment or temporary release from duty. The CMT will manage the resolution plan which has been agreed with the IMT and OT team members. The CMT shall provide resources (financial, technical, operational and facilities) commensurate with the agreed plan.

7 Ownership, Contacts and References

7.1 Ownership

A separate document providing a detailed inventory of all systems and lists: renewal date, server name, purchase date, serial number, rack location, owners, service function, and support and disaster recovery arrangements. See *Server Inventory* (DR arrangements appendix1.xls).

Similarly, the networking team maintain an inventory of all networking equipment. All equipment is supplied and maintained by Pervasive Ltd. and Calyx Communications. Contact: Head of Networking or Networking Operations Manager for further details. See *Network Equipment Inventory* (ntwkeqpt.mdb).

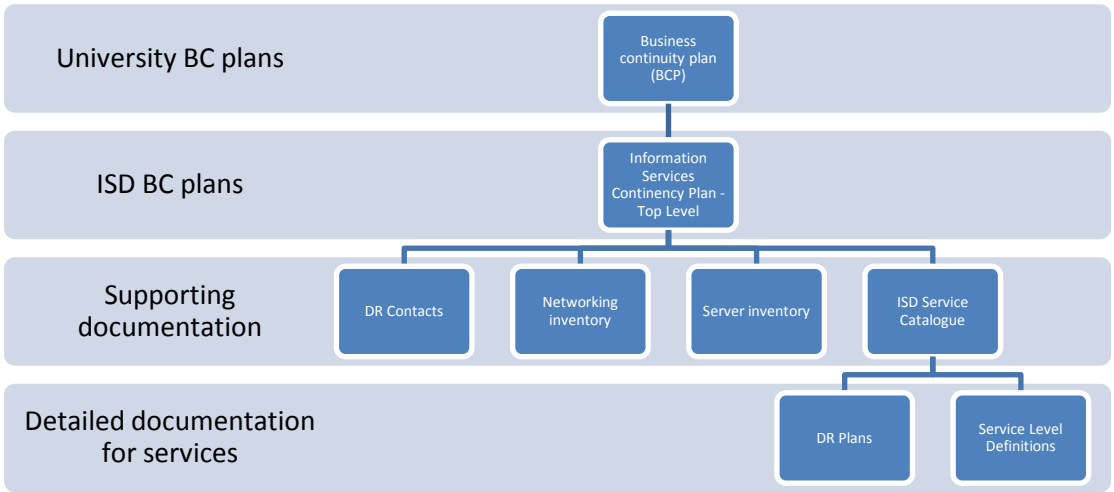
7.2 Internal and External Contacts

A separate document entitled *DR Contacts* sets out a list of all contacts:

- Membership of the strategic, tactical, and operational management teams
- Suppliers for all equipment and information systems

7.3 Documentation and References

7.3.1 Documentation map



The ISD *ICT Contingency Plan – Top Level* joins and forms part of the University's Business Continuity Plan (BCP).

7.3.2 Documentation list

Type	Name	Description	Owner	Filename	Network location of document
DR docs	DR contacts	Lists providing contact details for the strategic, tactical, and operational management teams, as well as support from all suppliers. Key contacts to be involved in the event of an incident and their role	Director of Information Services	DR Contacts.docx	\\Central-vfs\central-div-share1\ISD\DRPlans\TopLevelDRPlans (on Network)
DR docs	DR plans	DR documents for ISD systems including key contacts, maintenance arrangements, risks and usage, RTO and RPO	Service owners	Various	\\Central-vfs\central-div-share1\ISD\Service-Catalogue\Catalogue (on Network)
DR docs	Networking equipment inventory	Database of all networking equipment	Head of Networking	ntwkeqpt.mdb	\\central-vfs\central-div-share1\ISD\Service-Catalogue\Catalogue\S05-48\DR (on Network)
DR docs	Server inventory	List of all servers in the data centres. Provides details identifying the servers, support arrangements, and services delivered.	Data Centre Manager	dr arrangements appendix1.xls	\\Central-vfs\central-div-share1\ISD\ITCS\Computer-Suite\Private\DR & BC\Disaster Recovery (on Network)
OOH docs	Out of Hours Proposal	Details on the out of hours service	ICT Systems Director	Out of hours final proposal.doc	\\Central-vfs\central-div-share1\ISD\ITCS\OOH\Private\Admin (on Network)
Services	ISD Service Catalogue	List of all services offered by ISD with links to related SLDs and DR Plans. List shows which services have OOH cover	Assistant Director SPC	ISD_service_catalogue.xlsx[6]	\\central-vfs\central-div-share1\ISD\Service-Catalogue\Service-Catalogue (on Network)

7.3.3 Local plans

The ISD *ICT Contingency Plan – Top Level* describes the management process for recovering from service failure incidents for centrally-provided services managed by ISD. Services delivered and managed locally within Faculties are subject to their own contingency planning arrangements.

[6] The ISD Service Catalogue is the master repository for all information relevant to the delivery of ISD services (including service DR information).

7.4 DR DVDs

A copy of all ISD DR and BC documentation is copied to DVDs once a month. These are available to be consulted in the event of limited or no access to the network shares where the DR documentation is located. Up to 1 year of DR DVDs will be retained.

The DR DVDs are stored in the firesafe in Data Centre 2.

Key codes to the firesafe are held by ISD duty operators and at Library Reception.

8 Testing and Updating the Plan

The management process described in this ICT Contingency Plan must be reviewed at least every twelve months by the Director of Information Services. This is to ensure that the control process is current with University policy and priorities.

Contact information in the *DR Contacts* document should be updated as changes occur and the document should be subject to bi-annual revision.

New DR Plans and SLD documentation should be created for new services as they are introduced. Existing documentation for existing services are subject to regular review, with frequency determined by the nature of the service and its own review arrangements.

Tests of DR processes should be undertaken every year to ensure that the process is fit for purpose. Where suggestions for change to the process arise from the simulated disaster recovery test, they should be fed into the update to the plan.

8.1 Disaster recovery test

On an annual basis, one key system or service will be chosen by the ISD Management Team and its DR processes tested.

The tests should be realistic take into account:

- Time of day
- Day of the week
- Whether holiday or working day
- Availability of key staff
- Availability of the network
- Limitations of the test resulting from ensuring the test has no impact on live service

The DR test process will:

- Follow the process described in this plan.
- Follow document references provided in this plan.
- Use DR documentation provided for the system or service, and follow the process described including use of replacement equipment, backup tapes, etc.

A report for each test should be produced for ISSC and describe:

- The nature of the simulated system or service failure
- The steps undertaken to recover the system or service
- Any issues which were observed, and actions arising to eliminate or reduce the risk of the issues occurring again
- The recovery time and recovery points actually achieved, and whether these are within the objectives

8.2 Plan update process

Whenever the top level plan is updated, all copies of the plan as detailed below should be replaced with the updated plan.

1. Review is initiated once a year by the Director of Information Services.
2. The Plan is reviewed against current service delivery and requirements of the University as determined by the VCO and Faculties and in consultation with service owners.
3. The plan is updated.
4. The plan is reviewed by all stakeholders.
5. Once approved internally within ISD, the updated plan is submitted for approval by ISSC.
6. The approved updated plan is distributed to the following areas:
    a. The VCO to be lodged as part of the University's BCP.
    b. The ISD website at the following address http://www.uea.ac.uk/is/itregs/businesscontinuitydisasterrecovery. All Directors of University Services (DUSs) are informed that the documentation has been updated at this location.
    c. On the ISD central fileshare at the following network location \\Central-vfs\central-div-share1\ISD\DRPlans\TopLevelDRPlans. ISD Heads are informed that the documentation has been updated at this location.
7. The approved updated plan will then be added to the next copy of the DR DVDs when they are produced in the monthly cycle.

8.3 Update cycles

Update cycles for this and associated documentation is as follows:

Document	Update Cycle
Top Level Plan (this document)	Annual
DR Plans	Bi-Annual or: ▪ when significant changes in staff ▪ new systems go live ▪ old systems decommissioned
DR Contacts	Bi-Annual or: ▪ when significant changes in staff ▪ new systems go live ▪ old systems decommissioned
Server inventory	Annual or: ▪ when new systems go live ▪ old systems decommissioned ▪ existing systems upgraded
Network equipment inventory	Annual or: ▪ when new systems go live ▪ old systems decommissioned ▪ existing systems upgraded
ISD Service Catalogue	Annual or: ▪ when new services go live ▪ old services are withdrawn

9 Appendix: Recovery Time and Recovery Point

9.1 Recovery Time

The Recovery Time is the number of hours or days required to resume a process or a service back to effective operation. This may not necessarily mean back to the exact state of operation as previous but may require pragmatic solutions to provide service[7].

The Recovery Time objective should take account of the impact on service to the University at different times of the week and the academic year[8], and at times when the University buildings are closed. This varies from service to service. Recovery time objectives are therefore based on hours within business days.

9.2 Recovery Point

The Recovery Point describes the age of the data the University wishes to have the ability to restore to in event of a disaster. For example, if the RP objective is 8 hours, services should be restored in the state they were in no longer than 8 hours ago.

The Recovery Point objective for the University Central Systems is dependent upon, but also influences, the backup regime for each system (typically nightly) but may vary dependent on specific requirements and backup regimes.

A recovery is comprised of re-establishing services within their RT objectives; this includes reinstalling data which has been saved in accordance with required RP objectives as represented by the following diagram.

9.3 RTO and RPO references

RT and RP objectives for ISD systems are listed in the disaster recovery plans (DR Plans)[9] for those services.

[7] For instance, a fire in the data centre may damage several systems. These systems may be rebuilt using other hardware requisitioned from elsewhere on the campus.
[8] For instance, the impact of failure of the accommodation system is different at the start of term from the summer vacation.
[9] Each service has a DR Plan providing technical details on the systems used to run the service including server name, RTO, RPO, and system owner.