Disaster Recovery Plan for ADS systems

Version 1.8

Created date:	2006
Last updated:	30 Jan 2018
Review Due:	Jan 2019
Authors:	Tony Austin, Michael Charno and Paul Young
Maintained by:	Paul Young
Previous version:	Version 1.7 (previous online version Version 1.6)

NOTE: THIS IS A REDACTED VERSION FOR PUBLIC CIRCULATION. ALL PERSONAL DETAILS AND SYSTEMS-SENSITIVE INFORMATION HAVE BEEN REMOVED.

Change History

Created 5 Jul 2006 1.0 Tony Austin
Update 2008 1.1 Tony Austin
Update 2009 1.2 Tony Austin
Update 9 Oct 2011 1.3 Tony Austin
Update 27 Feb 2013 1.4 Tony Austin
Update 17 Apr 2014 1.5 Michael Charno
Update 05 Apr 2016 1.6 Paul Young
Update 08 Mar 2017 1.7 Paul Young
Update 30 Jan 2018 1.8 Paul Young

Note: most of the links in this document are internal

Contents

1. Introduction

This plan considers the ADS hardware and software systems.

The ADS has a series of servers located on campus and staff PCs and peripherals located in the ADS Offices. The servers are virtual machines and are maintained by IT Services. In addition, an off-site data store is maintained at the UK Data Archive (UKDA), University of Essex. Locally held original, preservation and dissemination data are regularly synchronised to servers at this remote site. The ADS also makes use of the university Network File System (NFS) and File Storage, both which are maintained by IT Services.

The actions described below are usually the domain of the ADS Systems Administrator or the ADS Administrator.

Generic contact details (see below for specific contacts)

Archaeology Data Service,
Department of Archaeology,
The King's Manor,
York,
YO1 7EP.
Phone: 01904 323954 (internal 3954)
Email: REMOVED
Web: http://archaeologydataservice.ac.uk

IT Services,
The University of York,
Heslington,
York.
YO10 5DD
Phone: REMOVED
Email: REMOVED
Web: http://www.york.ac.uk/it-services/

UK Data Archive,
University of Essex,
Wivenhoe Park,
COLCHESTER,
ESSEX,

CO4 3SQ
Generic Help Desk (if you can't get REMOVED - see contacts below)
Email: REMOVED
Phone: REMOVED
Web: www.data-archive.ac.uk

2. Access to the plan

This plan is located on Google Drive which is managed by the University of York. Access is restricted to ADS staff and associates. Digital and / or paper copies are also maintained off-site, as system or network failure may prevent access to the plan. These are currently held by the:

- ADS Director (off-site)
- ADS Systems Manager (on-site and off-site)
- UK Data Archive

Other important information can be found here:

- **Systems overview** REMOVED
- **Hardware inventory** REMOVED
- **Off-site data storage** REMOVED
- **University File Storage** REMOVED
- **ADS wiki** The ADS wiki contains lots of useful systems information. A digital backup is held in the office on a pen drive and off-site by the Systems Manager (REMOVED). The wiki pages are also backed-up on the NFS drive for 30 days and for 3 months on the tape drive.
- **Usernames / Passwords relevant to ADS systems:** These are stored in REMOVED which is managed by the University of York.
- **ADS and associated organisations domain information** (see REMOVED)
- **Policy and Guide to the Insurances of the University of York** http://www.york.ac.uk/admin/hsas/safetynet/Insurance/insurance_home.htm
- **Current ADS staff list** http://archaeologydataservice.ac.uk/about/contact or http://www.york.ac.uk/archaeology/staff/ads-staff/

3. Production servers

Please see the systems wiki page (link REMOVED) for more information.

3.1 Hardware failure

Please contact IT Services for any ADS systems problems, and the UK Data Archive (UKDA) for any off-site storage problems.

3.2 Hardware damage and theft

This is not relevant as the production servers are maintained by IT Services.

3.3 Data loss

Our important data is backed-up on the NFS for 30 days. This data can be accessed by going to the .snapshot directory on the relevant server. Note that the backups are numbered according to how many days ago the backup was made, e.g. nightly.4 is a backup 4 days in the past. IT Services also maintain backups on tape for a longer period (3+ months) but this data is more difficult to access.

The UKDA take a single monthly disaster recovery tape backup of current data, performed once a month, with a three month retention period. This is in addition to three copies of data currently held directly on servers.

4. PCs and peripherals

The ADS supports a number of PCs as detailed in the hardware inventory (link REMOVED) on Google Drive. Peripherals (printing, scanning) are now provided by the University as part of the York Print Plus (YPP) service.

4.1 Hardware failure

Hardware is protected via a limited warranty (usually three years) which is a part of the purchase. Details of warranties are held in the ADS hardware inventory. YPP equipment is maintained centrally. To initiate a warranty claim contact the supplier directly.

Maintenance beyond a standard warranty for PCs is not currently ADS practice. A policy of replacement is in place for major failure outside of warranty.

4.2 Hardware damage and theft

Maintenance contracts do not cover theft and accidental or malicious damage. The University of York has insurance to cover this but clearly recovery in such scenarios could be protracted. The University's insurance is handled by Campus Services which is situated in the Information Centre, Market Square.

In the event of damage to equipment the ADS Systems Manager or his stand-in needs to supply a list of damaged or stolen equipment and its replacement cost to the ADS Administrator who will further any claim.

The UKDA will be responsible for any insurance claims on servers in Essex. To quote, (UKDA, Essex) 'University has a blanket coverage which covers all equipment. Both hardware damage and theft is covered'.

4.3 Data loss

Facilities exist for staff to backup critical data from their PCs on to the M: Drive or File Storage (storage.its.york.ac.uk).

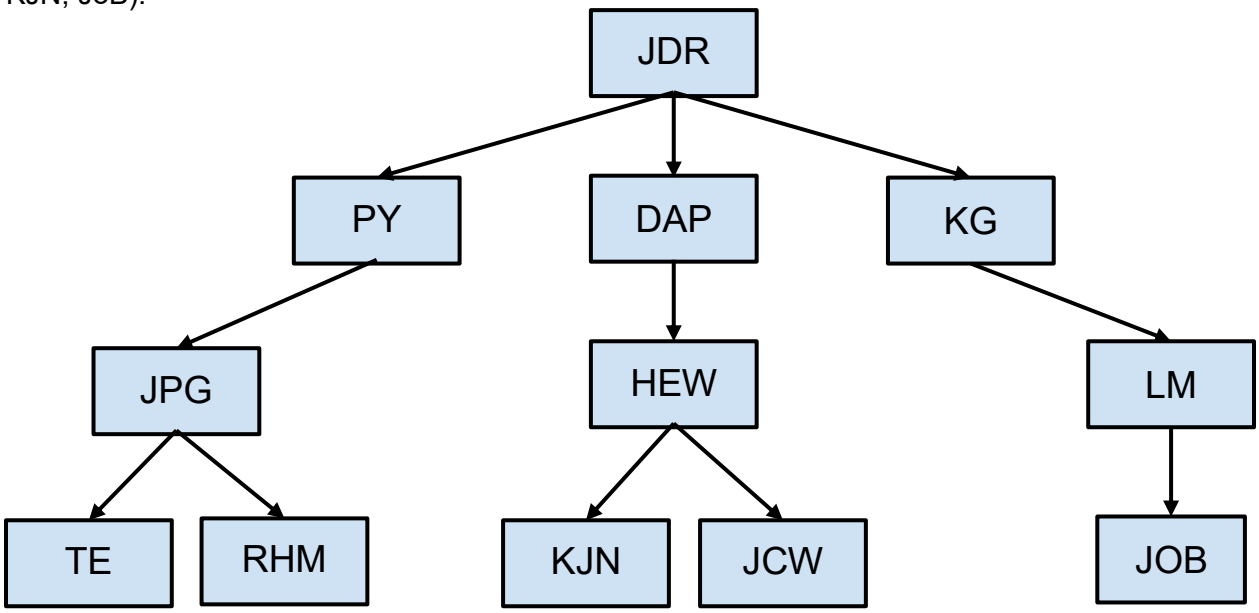
5. Catastrophic Disaster

In the case of catastrophic systems failure the ADS would be reliant on IT Services. However, peripheral services and organisations such as the ADS are likely to have a very low priority in any large-scale failure.

In the event of a national or international disaster, multiple and distributed copies of data will help the chances of survival but cannot guarantee it. Furthermore, it does not guarantee that there will be the will or wherewithal to resurrect and curate such data or indeed even awareness of its survival.

6. Disaster action including avoidance

Swift action may avoid disaster or lessen the effects. For example, the effects of flooding might be lessened by moving stuff to areas that do not flood. In order to act quickly a means to cascade information to staff 'out of hours' is necessary by telephone. This is shown as a pyramid. In an ideal situation information would cascade down from the top. However, the first person who becomes aware of a **catastrophic** situation will initiate a cascade by contacting the top. Some situations would obviously not require a full cascade. For example, if a server or service is down PY should be contacted directly in the first instance. If PY is not available then JPG should be contacted. If neither are available a digital archivist should be contacted (RHM, KJN, JoB).



If someone is unavailable jump to the next person. It may be necessary in some cases to call back the person jumped depending on the situation (see examples).

Initials	Name	Mobile

TE	Tim Evans	REMOVED
JPG	Jo Gilham	REMOVED
KG	Katie Green	REMOVED
RHM	Ray Moore	REMOVED
LM	Louisa Matthews	REMOVED
KJN	Kieron Niven	REMOVED
JOB	Jenny O'Brien	REMOVED
DAP	Donna Page	REMOVED
JDR	Julian Richards	REMOVED
JCW	Judith Winters	REMOVED
HEW	Holly Wright	REMOVED
PY	Paul Young	REMOVED

6.1 Example scenarios

The following describe some possible disaster recovery/avoidance scenarios that may arise.

6.1.1 Water penetration

This is a known problem in ground floor offices; G11 and G12. It is mainly centred on the dividing wall between these offices but does spread along joining walls.

Scenario:

As observed on the local news an unpredicted severe weather warning for the York area develops over the weekend especially for Sunday evening.

KG has a growing concern and phones JDR but receives no answer.

KG now phones LM, who is the next person down in the cascade from JDR.

KG and LM now decide to cascade down the list in order to try and find someone who is able to attend King's Manor. It is probably reasonable to assume that it is easier for people living in York to attend the offices.

LM phones JOB who agrees to go to King's Manor.

JOB attends KM, unplugs the electrical stuff and moves paper documents from areas likely to be affected to a safer location.

6.1.2 Service failure

Scenario:

One evening JDR notices that our main website is down.

JDR phones PY but there is no answer.

JDR phones JPG who logs in remotely and ascertains the problem is Glassfish which she restarts.

6.1.3 Loss of access to offices

This is pure fiction but demonstrates where everyone might need to be contacted using the cascade.

Scenario:

KJN sees on the local evening news that a serious incident has occurred at King's Manor with access to the whole complex likely to be closed off for sometime.

KJN phones JDR in case he isn't aware of the situation. JDR decides that the best option is for people to work from home the following day, where practical, or to seek computer access on campus. Also, staff should check university email for updates during the following day.

JDR phones DAP and PY who in turn cascade the information downwards.

PY phones JPG who does not answer. PY makes a note to retry JPG later on.

PY jumps to the next person in the cascade and phones TE successfully.

All other calls are successful in the cascade.

7. Other contacts

IT Services:
Tel: REMOVED
Email: REMOVED
Url: http://www.york.ac.uk/it-services

If you think your machine has been attacked or other activity of concern is taking place, contact the York CERT (Computer Emergency Response Team).

Email: REMOVED
Phone: REMOVED

Name	Org	Role	Phone (work)	Email
REMOVED	ITS	Linux & Security	REMOVED	REMOVED
REMOVED	ITS	Linux & Security	REMOVED	REMOVED

REMOVED	ITS	Linux & Security	REMOVED	REMOVED
REMOVED	ITS	Linux & Security	REMOVED	REMOVED
REMOVED	ITS	Databases	REMOVED	REMOVED
REMOVED	SoA	Library Catalogue	REMOVED	REMOVED
REMOVED	UoY	Insurance Officer	REMOVED	REMOVED
REMOVED	UKDA	Systems Manager	REMOVED	REMOVED
REMOVED	UKDA	Systems Admin	REMOVED	REMOVED