Dartmoor National Park Authority

Disaster Recovery & Business Continuity Plan for ICT Services

August 2010

Target Audience:
ICT

Contents

Document Control

Organisation	Dartmoor National Park Authority
Title	Disaster Recovery & Business Continuity Plan for ICT Services
Creator	A. Bright
Source	
Approvals	
Distribution	
Filename	ICT Disaster Recovery Plan - Rev 0810-DRAFT.docx
Owner	Head of ICT Service
Subject	Information Security
Protective Marking	None
Review date	August 2011

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
1.0	Ali Bright	Oct 2003	Created
2.0	Ali Bright	Feb 2005	Addition of Document Management System and SQL Server
3.0	Ali Bright	Aug 2010	To reflect move to virtualised server environment

1. Introduction

A Disaster Recovery Plan for ICT Services was first introduced in 2003 following an audit recommendation. It is reviewed biennially, or following any major changes to equipment or systems covered by the plan, to ensure it is always relevant and up to date.

Disasters are, fortunately, are rare but when they do occur they can have devastating consequences. Many services will quickly be brought to a standstill in the event of prolonged computer breakdown. The vulnerability of the Authority's services to the effects of a computer failure have increased markedly in recent years as more and more reliance has been placed on computerised systems to manage services. This is likely to continue in the coming years as ICT systems are increasingly used as a means of generating efficiencies.

2. Definition of Disaster

"For the purposes of this plan a Disaster is defined as loss or damage of part or all of the Authority's ICT Infrastructure, which would have a high, or very high, business impact on the Authority."

Disaster, as outlined in the above definition, includes :

a) Total loss of one site, (ie due to fire damage)
b) Loss or technical failure of one or more network servers
c) Loss or technical failure of network infrastructure i.e. hub/switch/router/comms link
d) Loss or technical failure or Voice Infrastructure, (telephone system)
e) Extended loss of electrical power
f) Failure of a key software system

Key software systems which are specifically referred to in this plan include :

i) FINEST – Financial System
ii) Exchange – Email System
iii) PACS – Planning Application Control System
iv) BLEEP – Electronic Point-of-Sale System

3. How the plan is activated

In the event that a disaster is identified by the Strategic Management Team (SMT), the Head of ICT will be responsible for activating the plan and monitoring the progress of disaster recovery procedures, reporting to SMT and undertaking any further action as necessary.

4. Overview of ICT Infrastructure

The Dartmoor National Park Authority currently has five sites that are connected to its corporate computer and voice network. These sites are 'Parke' at Bovey Tracey, the High Moorland Office (HMO) at Princetown, Postbridge and Haytor Information Centres, and the works depot at Station Yard, Bovey Tracey.

The corporate network at Parke comprises :

- 6 physical servers (3 ESX hosts, an ISA Firewall, ipStor and backup servers)
- 12 virtual servers
- 5 Alcatel Voice Switches (one at each site)
- a mixture of 1Gbps and 100Mbps data switches
- a router connecting Parke to the Devon County Wide Area Network via 2Mbps Megastream
- a router connecting Parke to HMBC via 1Mbps Megastream
- approximately 65 desktop workstations and 40 laptop computers

A detailed network topology diagram shown in appendix B.

Server rooms at both Parke & Princetown are located on the first floor, away from entrances to the buildings from outside to minimise the risk of theft and flood. The room at HMO has no external accesses and the room at Parke only has a small external window. Both rooms have permanent installations which provide air conditioning to maintain air temperatures suitable for the equipment located in them. This was installed in the autumn of 2003 as a result of problems experienced during the heat wave of that summer. Redundant portable air conditioning units are kept available in the event of failure of one of the permanent installations.

The Authority's financial system, 'FINEST', is hosted on a Unix based server at County Hall. Access to the database is provided via the communications link which links Parke and County Hall.

Microsoft Exchange Server is used to provide email services to both sites. It is installed on a virtual server, (DNP3), at the Parke site.

The database system used within the Development Control directorate, 'PACS', has been developed using MS Access and SQL Server by 'exeGesIS SDM Ltd'. It is stored on virtual server (DNP2). It comprises an Access front-end database containing queries, forms and reports, and a SQL 2005 backend database containing data tables.

The electronic point of sale system used within the Information, Education and Communications Service for managing stock and sales from the Authority's Information Centres is 'BLEEP', which is produced by 'Bleep Data Ltd'. It is installed on a physical server at HMO and uses the Borland Pervasive database engine.

5. Risk Assessment and Business Impact Review

Likelihood	Severity	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Rare (1)		Low	Low	Low	Low	Medium
Unlikely (2)		Low	Low	Medium	Medium	High
Possible (3)		Low	Medium	Medium	High	High
Likely (4)		Low	Medium	High	High	Very high
Almost certain (5)		Medium	High	High	Very high	Very high

Physical equipment

Location	Network Element	Type of loss / damage	Likelihood	Severity	Business Impact	Precautions in place
Parke	ESX Servers (ESX1, ESX2 & ESX3)	Fire Theft Water Damage Vandalism Wind Accidental	1	1	Loss of a single ESX server, would result in only a few minutes downtime to the virtual servers hosted on that ESX Server.	VMware High Availability (HA) configured on all ESX hosts. This service monitors the condition of all hosts and if it detects a failure it will automatically restart all the affected Virtual machines (VMs) on a different host. The only operational downtime to the VM would be the amount of time it takes to reboot (typically 1-2 minutes).
		Hard disc failure	3	1	No impact from loss of a single hard disk. The impact of the loss of both disks would be as	Each ESX host has two identical hard drives configured with a RAID1 mirror to introduce redundancy.

					described under Fire/Theft/etc above.	Equipment protected by Dell warranty – same day onsite replacement of failed disks.
		Other failure	3	1	Depending on the type of failure, worse case would be as described under Fire/Theft/etc above.	Equipment protected by Dell warranty – same day onsite repair of any faulty hardware. In the case of a software corruption with the VMware host system, this would be covered under Cristie Silver Level support contract.
		Power failure (Short term)	3	4	Environmental Power Failure would affect all ESX hosts, therefore once the backup power is exhausted all the hosts would need to be shutdown, resulting in complete downtime to the computer network.	UPS installed – approximately 20 minutes backup.
	DNP9 – Backup Server	Fire Theft Water Damage Vandalism Wind Accidental	1	1	Unable to backup data from the network using standard procedure, but no interruptions to service to users.	The system is imaged weekly using Cristie Bare Machine Recovery, (CBMR). In the event of the loss of the machine this image could be restored to a replacement server in around 30 minutes.
		Hard disc failure	3	1	No impact from loss of a single hard disk. The impact of the loss of both disks would be as described under Fire/Theft/etc above.	Two identical hard drives configured with a RAID1 mirror to introduce redundancy. Equipment protected by Dell warranty – same day onsite replacement of failed disks.

		Other failure	3	1	As described under Fire/Theft/etc above.	As described under Fire/Theft/etc above.
		Power failure (Short term)	3	1	Once backup power is exhausted the server would shutdown.	UPS installed – approximately 20 minutes backup.
	DNP11 – ISA Firewall	Fire Theft Water Damage Vandalism Wind Accidental	1	3	Loss of connectivity to the outside world. No access to the Internet, FINEST, delivery of externals emails, etc	The system is imaged weekly using CBMR. In the event of the loss of the machine this image could be restored to a replacement server in around 30 minutes.
		Hard disc failure	3	1	No impact from loss of a single hard disk. The impact of the loss of both disks would be as described under Fire/Theft/etc above.	Two identical hard drives configured with a RAID1 mirror to introduce redundancy. Equipment protected by Dell warranty – same day onsite replacement of failed disks.
		Other failure	3	1	As described under Fire/Theft/etc above.	As described under Fire/Theft/etc above.
		Power failure (Short term)	3	3	Once backup power is exhausted the server would shutdown and the impact would be as described under Fire/Theft/etc above.	UPS installed – approximately 20 minutes backup.
	SAN – Data Storage System	Fire Theft Water Damage Vandalism Wind Accidental	1	5	Loss of the SAN would result in complete downtime to all systems on the computer network until a replacement could be implemented.	All the data on the SAN is backed up regularly according the adopted backup procedure. The hardware is all covered by an onsite maintenance agreement, (next day 8/5)
		Hard disc failure	3	1	No impact from loss of a single hard disk.	The Nexsan disk array contains 14 disks which are configured

				The SAN disk array is configured so that it can cope with multiple disk failures without loss of service.	with a mixture of RAID5 and RAID10 to ensure the best protection against loss of data from hard disk failure.
		Failure of the Nexsan SataBoy backplane / controller.	1	5	Loss of a Nexsan disk array would result in complete downtime to all systems on the computer network until a replacement could be implemented.	All the data on the SAN is backed up regularly according the adopted backup procedure. The hardware is all covered by an onsite maintenance agreement, (next day 8/5)
		Power failure (Short term)	3	4	Once the backup power is exhausted the SAN would need to be shutdown, resulting in complete downtime to the computer network.	UPS installed – approximately 20 minutes backup.
	UPSs	Fire Theft Water Damage Vandalism Wind Accidental	1	2	Connected equipment would no longer receive power and would shutdown. Equipment could then be connected directly to the mains supply to restart equipment so downtime in office hours would be limited to 5-10 minutes.	Two UPSs independently supply power to separate redundant PSUs within each ESX host. In the event of failure of either UPS there is no interruption to service. Comms equipment (PABX, routers etc) are only supplied by a single UPS and would need to be connected to the mains in the event of a UPS failure.
		Hardware failure	2	2	As above.	As above.
		Power failure	3	4	Environmental Power Failure would affect all	UPS provides approximately 20 minutes backup power to

					UPSs, therefore once the backup power is exhausted all equipment powered by the UPS will shutdown.	connected devices.
	PABX (Alcatel Omnioffice voice switch)	Fire Theft Water damage Vandalism Wind Accidental	1	4	Loss of all telephones at Parke site, and incoming lines to Princetown and Station Yard (except 890414)	Equipment protected by maintenance agreement with SW Communications Group. All configuration settings backed up to data network quarterly, and after each major change. Backup analogue phone line for use in emergencies.
		Hardware failure	2	4	As above	As above
		Power failure (Short term)	3	3	Once the backup power had been exhausted all telephones at Parke site, and incoming lines to Princetown and Station Yard (except 890414) would go down.	UPS installed – approximately 45 minutes backup power.
	48 Port / 24 Port Data Switches	Fire Theft Water damage Vandalism Wind Accidental	1	2	Loss of access to all PCs and other infrastructure connected via the affected switch	Sufficient spare capacity is maintained so that in the event of failure equipment can be connected via alternate switch.
		Technological failure	2	2	As above	As above
		Power failure (Short term)	3	3	As above	UPS installed – approximately 45 minutes backup power.
HMBC	DNP5	Fire	1	3	Loss of access to the Bleep	Bleep data backed up to

	(AD, DHCP, GIS copy, Bleep)	Theft Water damage Vandalism Wind Accidental			ePOS system and GIS (at HMO only)	external hard drive by MGraves daily, and copies taken offsite weekly. Other data not backed up, as it is only copies of data held at Parke. Hardware covered by Dell onsite warranty.
		Hard disc failure	3	3	As above	No protection against HD failure
		Other failure	3	3	As above	As described under Fire/Theft/etc above.
		Power failure (Short term)	3	3	As above	UPS installed – approximately 45 minutes backup power.
	PABX (Alcatel Omnioffice voice switch)	Fire Theft Water damage Vandalism Wind Accidental	1	3	Loss of all telephones at Princetown site	Equipment protected by maintenance agreement with SW Communications Group. All configuration settings backed up to data network quarterly, and after each major change. Backup analogue phone line for use in emergencies.
		Hardware failure	2	3	As above	As above
		Power failure (Short term)	3	3	As above	UPS installed – approximately 45 minutes backup power.
	24 Port Data Switch	Fire Theft Water damage Vandalism Wind Accidental	1	3	Loss of access to all PCs and other infrastructure connected via the affected switch	Sufficient spare capacity is maintained at Parke, so in the event of a switch failure at Princetown, a replacement could be delivered quickly from Parke.
		Technological failure	1	3	As above	As above

		Power failure (Short term)	3	3	As above	UPS installed – approximately 45 minutes backup power.
Postbridge Haytor Depot	PABX (Alcatel Omnioffice voice switch)	Fire Theft Water damage Vandalism Wind Accidental	1	2	Loss of all digital telephones at relevant site (Postbridge, Haytor or Station Yard Depot)	Equipment protected by maintenance agreement with SW Communications Group. All configuration settings backed up to data network quarterly, and after each major change. Backup analogue phone line for use in emergencies.
		Hardware failure	2	2	As above	As above
		Power failure (Short term)	3	2	As above	UPS installed – approximately 45 minutes backup power.
County Hall	FINEST system	Protected as part of the Devon County Council Disaster Recovery Plan				

6. Disaster Recovery Plan

There are two distinct elements to this Plan. Disaster could consist of failure of a particular element of the ICT infrastructure, for example, a server or voice switch. Additionally a major disaster such as Fire or Flood could knock out an entire site, large part of a site which contains key systems.

The first table below details steps to be taken in the event of loss of any individual key system. The second table then outlines procedures to be followed in the event of loss of an entire site or a large part of a site which contains key systems.

a) Table showing procedures for recovery of individual network elements

Location	Network Element	Type of Loss / Damage	Recovery Procedures
Parke	ESX Servers (ESX1, ESX2 & ESX3)	Total loss of a single ESX server	Purchase replacement server from Dell. Contact Cristie Data Ltd and request engineer for system rebuild under the silver support contract (01453 847003) Re-distribute VMs across all three hosts
		Hard disc failure	Identify failed hard drive – indicator on RAID controller Contact Dell to arrange shipment of replacement drive (0870 9080500) DNP ICT staff to hot swap hard drive on arrival
		Other hardware failure	Contact Dell to arrange for hardware engineer to attend – same day (0870 9080500) Dell engineer to replace faulty part Restart system
		Software failure	Contact Cristie Data Ltd and request engineer for system rebuild under the silver support contract (01453 847003) Re-distribute VMs across all three hosts
		Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown server and await power restore When power is restored, restart server Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900)
	DNP9	Total loss	Purchase replacement server from Dell.

(Backup server)		Use Cristie CBMR to restore the most recent image to disk Restart system
	Hard disc failure	Identify failed hard drive – indicator on RAID controller Contact Dell to arrange shipment of replacement drive (0870 9080500) DNP ICT staff to hot swap hard drive on arrival
	Other hardware failure	Contact Dell to arrange for hardware engineer to attend – same day (0870 9080500) Dell engineer to replace faulty part Restart system
	Software failure	Use Cristie CBMR to restore the most recent image to disk Restart system
	Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown server and await power restore When power is restored, restart server Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900)
DNP11 (ISA Firewall)	Total loss	Purchase replacement server from Dell. Use Cristie CBMR to restore the most recent image to disk Restart system
	Hard disc failure	Identify failed hard drive – indicator on RAID controller Contact Dell to arrange shipment of replacement drive (0870 9080500) DNP ICT staff to hot swap hard drive on arrival
	Other hardware failure	Contact Dell to arrange for hardware engineer to attend – same day (0870 9080500) Dell engineer to replace faulty part Restart system
	Software failure	Use Cristie CBMR to restore the most recent image to disk Restart system
	Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown server and await power restore When power is restored, restart server Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900)
PABX	Total loss	British Telecom to re-route main switchboard number (01626 832093) to

	(Alcatel Omnioffice voice switch)		Princetown Order replacement voice switch from SW Comms (01392 369369) Contact SW Comms and request engineer attend for system rebuild (0844 871 2020) – Same day SW Comms engineer to restore system configuration from latest backup British Telecom to re-route main switchboard number to back to Parke
		Hardware failure	Contact SW Comms and request engineer attend to repair/replace faulty hardware (0844 871 2020) – Same day SW Comms engineer to restore system configuration from latest backup
		Software failure	Contact SW Comms and request engineer attend for system rebuild (0844 871 2020) – Same day SW Comms engineer to restore system configuration from latest backup
		Power failure	Ensure UPS is operating correctly – 45 minute backup Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900) If power outage to exceed ½ day, Western Power Distribution to provide backup generator Plans for connection of external power generator with DNP Contract Works Manager.
	48 Port / 24 Port Data Switches	Total loss	Re-connect devices from affected switch to alternative switches and restart Order replacement switch and install Re-distribute devices across available switches
		Hardware failure	As above
		Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown system and await power restore When power is restored, restart system Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900)
HMBC	DNP5 (AD, DHCP, GIS copy, Bleep)	Total loss	Purchase replacement workstation from Dell. Contact AME Solutions and request engineer for system rebuild (01392 824022). DNP ICT staff to collect server from Princetown for work to be undertaken at Parke AME Solutions engineer to re-install operating system from CD Active Directory, (including User accounts) to be replicated from Domain Controllers at Parke

			Restore data from latest backup, (excluding GIS) Copy GIS from server at Parke Install and test Bleep system.
		Hard disc failure	No redundant hard disk, (machine is a standard workstation not a server) Contact Dell to arrange for replacement hard drive – same day (0870 9080500) Install replacement hard disk and follow procedure for total loss, above.
		Other hardware failure	Contact Dell to arrange for hardware engineer to attend – same day (0870 9080500) Dell engineer to replace faulty part Restart system
		Software failure (other than Bleep)	Procedure as for total loss, above.
		Software failure (Bleep system)	Contact Bleep Computing (0207 7170200) to arrange for repair or reinstallation.
		Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown system and await power restore When power is restored, restart system Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900)
	PABX (Alcatel Omnioffice voice switch)	Total loss	British Telecom to re-route main number (01822 890414) to Parke. ICT Team re-configure switch to present Princetown DDIs locally. Order replacement voice switch from SW Comms (01392 369369) Contact SW Comms and request engineer attend for system rebuild (0844 871 2020) – Same day SW Comms engineer to restore system configuration from latest backup British Telecom to re-route main switchboard number back to Princetown. ICT Team re-configure switch to present Princetown DDIs at Princetown.
		Hardware failure	Contact SW Comms and request engineer attend to repair/replace faulty hardware (0844 871 2020) – Same day SW Comms engineer to restore system configuration from latest backup
		Software failure	Contact SW Comms and request engineer attend for system rebuild (0844 871 2020) – Same day SW Comms engineer to restore system configuration from latest backup
		Power failure	Ensure UPS is operating correctly – 45 minute backup

		Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900) If power outage to exceed ½ day, Western Power Distribution to provide backup generator
24 Port Data Switch	Total loss	Re-connect devices at Parke site to free up spare switch Install switch at Princetown and re-connect devices Order replacement switch Install new switch at Parke and re-distribute devices across available switches
	Hardware failure	As above
	Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown system and await power restore When power is restored, restart system Contact Western Power Distribution to determine reason for power outage, if not planned (0800 365 900)

a) Table showing procedures for recovery in case of loss of entire site or large part of a site which contains key systems.

Location	Type and extent of loss/damage	Recovery procedure	Persons responsible
Parke	Flood / Fire (Entire site)	Key software systems PACS, Exchange to be installed on server at HMBC, and staff re-located to Princetown until suitable accommodation elsewhere can be provided. Access to the Financial System, (FINEST), to be provided at County Hall and staff re-located to Exeter until suitable accommodation elsewhere can be found. British Telecom to re-route main switchboard telephone number (01626 832093) to voice switch at Princetown. Replacement equipment, as per official inventory, to be ordered at the first opportunity for installation as soon as suitable alternative accommodation becomes available. Cristie DataLtd to provide engineers to assist in the restore of ESX hosts and virtual servers new accommodation becomes available. DNP ICT Team to be responsible for setting up replacement PCs. Replacement voice switch to be ordered at the first opportunity for installation as soon as suitable alternative accommodation becomes available. Once installed, British Telecom to re-route main switchboard telephone number and all DDIs to new location.	ICT Team / AME Solutions / Cristie Data Ltd ICT Manager / Devon CC British Telecom ICT Manager Cristie Data Ltd / ICT Team ICT Manager / TTML / British Telecom
	Flood / Fire (Localised to part of building containing server room)	Replacement equipment, as per official inventory, to be ordered at the first opportunity for installation at alternative cabling position. Cristie Data Ltd to provide engineers to assist in the restore of ESX hosts and virtual servers. *The points above will only provide ICT Services to the areas of the building that are*	Head of ICT Chimera CMT / ICT Team

		cabled from the alternative cabling position (approx ½ the building). Cabling contractors to install replacement network cabling for voice and data to affected areas of the building following repair. Re-connect PCs to new cabling in effected areas.	 SEC Ltd ICT Team
HMBC	Flood / Fire (Entire site)	Re-locate staff to temporary accommodation at Parke. Replacement equipment, as per official inventory, to be ordered at the first opportunity for installation at Parke initially and then at suitable alternative accommodation when available. British Telecom to re-route main telephone number (01822 890414) to voice switch at Parke. Voice switch at Parke to be re-configured to present Princetown DDIs locally. AME Solutions to provide engineers to assist in the restore of server once new accommodation becomes available. DNP ICT Team to be responsible for setting up replacement PCs. Replacement voice switch to be ordered for installation as soon as suitable alternative accommodation becomes available. Once installed, British Telecom to re-route main switchboard telephone number and all DDIs to new location.	 Head of ICT British Telecom / ICT Team AME Solutions / ICT Team Head of ICT / SW Comms / British Telecom
	Flood / Fire (Localised to part of building containing server room)	Given the size of the building, number of users and cabling structure at the HMBC site it would not be practicable to relocate equipment else where in the building. Plan for recovery in this case would be as per the first 4 points shown under ‘Entire Site’ above, until equipment can be re-installed at the HMBC site.	 As above

7. Testing the plan

It is essential that each of the various elements of this plan are tested to ensure that in the event of an actual disaster, systems can be recovered in line with this plan with a minimal interruption to users.

It will not be necessary to fully test the plan for all of the virtual servers which currently make-up the DNPA network, because the recovery procedure is the same for each. However, it is considered important that each system which has a different procedure for recovery is tested. Therefore following tests should be carried out :

- Recovery of one or more virtual servers from backup
- Recovery of the ipStor server which controls the SAN data storage
- Recovery of the physical workstation at Princetown which acts as a server, and which runs the Bleep ePOS system.
- Recovery of a PABX voice system
- Recovery of one of the physical servers from its CBMR image
- Full test of all the UPS equipment to ensure correct operation, and sufficient battery life.

Each of these tests will have to be planned in advance in order of priority. Some of these tests will require significant amounts of staff time, and in some cases expenditure with external contractors which will need to be scheduled in work programmes and budget requested through the usual budget bid process.

Wherever possible these tests should be carried out during normal office hours, and not involve any downtime of live servers during core working hours.

In addition to these tests, the following should be carried out regularly :

- Test restores from disk and tape to ensure that backups are reliable
- Tests of UPS systems to ensure they are functioning correctly

It is imperative that backups are checked daily to ensure they are operating correctly. Automated emails will be generated daily detailing success or failure of individual backup jobs.

8. Review – Maintenance of the plan

This plan is to be reviewed annually or shortly after the installation of any new key ICT infrastructure by the Head of ICT Service. When installing any new infrastructure due regard must be given beforehand to any impact that the installation will have on this plan.

Copies of this plan are to be stored in fire-proof safes at both the Parke and Princetown sites along with the backup tapes. A further copy should be kept as an appendix to the Network Managers Handbook. This is to ensure that a copy is readily available and that in the event of a major disaster at least one copy of the plan will remain intact.

9. Appendices

Appendix A : Site location maps
Appendix B : Site floor plans including cable layouts
Appendix C : Network topology diagram
Appendix D : Results of tests carried out to date