THE TWO COUNTIES TRUST

DISASTER RECOVERY POLICY

Date of issue: 23/10/2020

1. Purpose

The aim of the Two Counties Trust ("the Trust") is to ensure all data and information stored electronically on its systems is recoverable in the event of a disaster incident. This policy defines the mechanisms by which such recovery is made possible and sets out a schedule for testing to ensure that the efficacy of this process is exercised, and the results recorded.

2. Scope

The Trust employs a common technology across all school sites to provide a homogenous backup and recovery solution. Servers on all sites are backed up locally, and copies of these backup images transmitted securely to an off-net cloud storage solution maintained by the technology provider. This policy covers servers and services managed using this technology.

3. Policy Principles

This policy is designed to outline the technology used to protect the Trust's data, and to describe a top-level recovery operation. The technical steps required to actuate the recovery are detailed in a separate work instruction document aimed at technically competent ICT engineers.

A disaster incident may be a physical incident impacting on the ability of the information systems to deliver the services and data on which the Trust relies, it may be a cyber security incident compromising the systems and rendering the services inoperable, or it may be an infrastructure failing which precludes the ability of the systems to deliver the services. The systems and service recover process is the same regardless of the disaster incident type, only the target recovery location of hardware may vary.

Service recovery is defined by, and measured in terms of, recovery times and points. The objective of the Trust ICT Team is to have the Recovery Point Objective (RPO) as low as possible, and as close to real time as is feasible, and the Recovery Time Objective (RTO) as short a period after the disaster event as possible.

3.1 Definitions

Recovery Point Objective (RPO): The recovery point objective is the point to which information used by an activity must be restored to enable the activity to operate on resumption. RPO can also be referred to as 'maximum data loss'.

Recovery Time Objective (RTO): The recovery time objective is the maximum amount of time allowed to resume an activity, recover resources, or provide products and services after a disruptive incident occurs. This target time period must be short enough to ensure that adverse impacts do not become unacceptable.

Source: ISO 22301:2012

4. Policy Elements

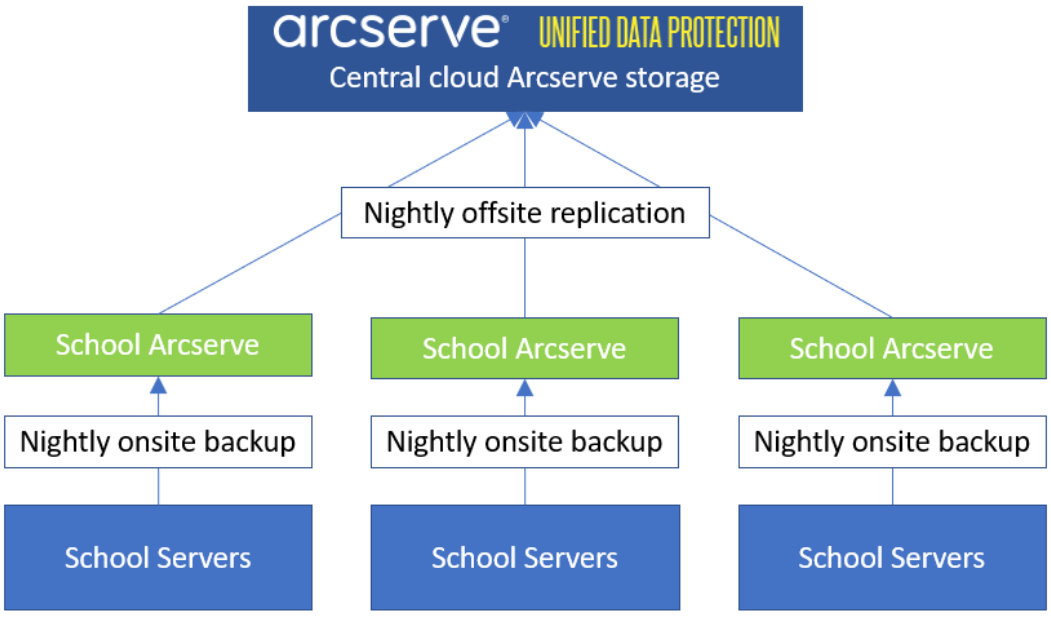

Figure 1: Backup architecture

4.1 Crisis Team

In the event of a disaster recovery scenario, a crisis team should already have been convened through the incident management (IM) process. This team should, throughout an incident, be engaged in disaster recovery activities, and tasks assigned by the crisis lead as required.

For convenience, the ICT crisis team should consist of the network manager(s) for the school(s) concerned, who will co-ordinate the technical recovery, and the Head of ICT, who will maintain strategic oversight, authorise changes as required, and ensure the communications plan is followed.

Key stakeholders for each school have been identified via the impact analysis process and will form the school contingent of the crisis team, along with any nominated other.

Contact details for the ICT team are contained in Appendix I.

4.2 Server Recovery

The virtual nature of most servers within the Trust estate means that the loss of one physical host due to a physical incident such as fire, flood or malicious damage is easily surmounted. The following is the general process necessary to recover a server:

- Log on to the local recovery server, or cloud storage area
- Navigate the resource tree and locate the server(s) required
- Right click and select "Restore" from the context menu

This is illustrated in figure 2 below.

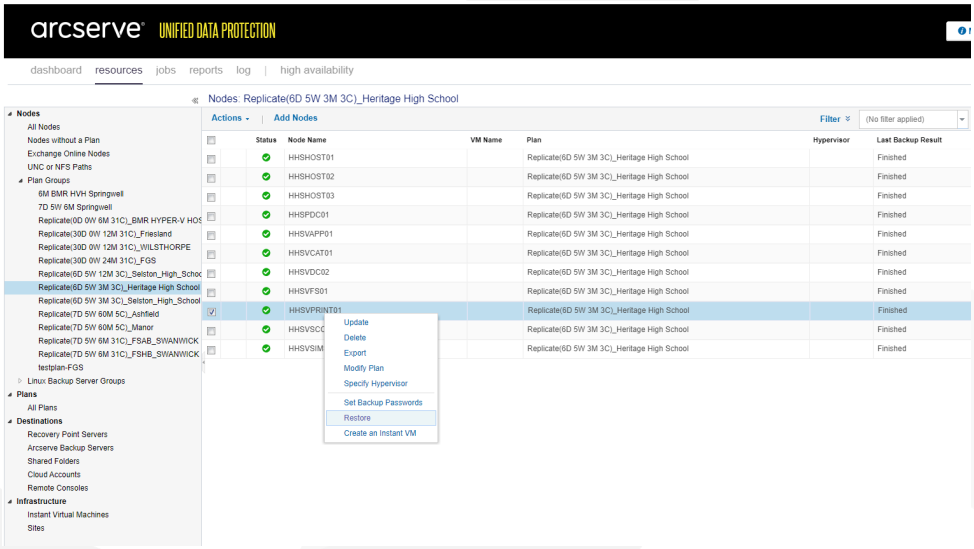

Figure 2: Restore option on management console

Specific per-site work instructions are maintained separately.

4.3 Cybersecurity incident

Recovery from a cybersecurity incident is handled in the same manner as from any other incident, with the caveat that the ICT team must ensure that target hardware is factory reset and / or bare metal installation, to eliminate the risk of any low level firmware rootkit malware.

5. Communications Plan

In the event of a disaster recovery incident, the ICT lead will coordinate the messaging across affected sites. This is a liaison piece which will necessarily involve key stakeholders, and the ICT lead will ensure regular and effective messaging is supplied to keep key parties informed of progress.

6. Scheduling and Exercising

The efficacy and viability of recovering servers and services from backup and DR provision must be validated and recorded via a managed and monitored schedule of tests across the Trust recovery estate. This is a responsibility of the ICT Team, in conjunction with key stakeholders in the school, to arrange and carry out per schedule. Each school must be tested at least annually.

The schedule and results of exercises are maintained in the document:

TTCT_DR_Schedule.xlsx

Limitations of this Policy

This policy defines the overall architecture recovery paradigm of the Trust. Where schools have implemented systems or services outside of the purview of the ICT team, no responsibility is taken for the recoverability of these solutions. All new services and solutions should be implemented with the ICT team and requirements for recoverability captured as part of the project process. These solutions will then be added to the DR testing schedule.

Appendix 1: ICT management team contact details

Name	Responsibility	Email	Phone
Rich Minshaw	Head of ICT	rminshaw@twocountiestrust.co.uk	01623 259 625
Richard Armshaw	Springwell & Heritage	rarmshaw@twocountiestrust.co.uk	01623 259 612
Paul Croot	Ashfield & Selston	pcroot@twocountiestrust.co.uk	
Joe Redmond	Friesland & Wilsthorpe	jredmond@twocountiestrust.co.uk	
Matthew Sutton	Swanwick & FGS	msutton@twocountiestrust.co.uk	TBC
Bradley Wragg	Manor	wraggb@themanor.notts.sch.uk	01623 425 100

Appendix 2: ICT DR testing schedule and record

The figure below shows the content of the testing record, which is maintained separately in the document:

TTCT_DR_Schedule

Two Counties Trust - Disaster Recovery Testing

This schedule and list of results must be maintained by the ICT Team to accurately record dates and results of testing carried out in accordance with the schedule.

Complete the below accurately. Any failures must be documented on the 'Failures' tab, along with follow-on actions and re-testing schedule.

Test ID	Schedule Date	School	Actual Date	Server(s) recovered	Start time	End time	Duration	Technician	Success	Notes / observations
1	18/11/2020	Wilsthorpe								
2	16/12/2020	Heritage								
3	20/01/2021	Selston								
4	17/02/2021	Swanwick								
5	17/03/2021	Friesland								
6	21/04/2021	Springwell								
7	19/05/2021	Ashfield								
8	16/06/2021	Frederick Gent								
9	21/07/2021	Manor								
10	18/08/2021	Wilsthorpe								
11	15/09/2021	Heritage								
12	20/10/2021	Selston								
13	17/11/2021	Swanwick								
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										