ACCESS
Advancing Education Technologies

Data Backup and Email Retention Policy

1/21/22

ACCESS Backup Procedures

Overview

This document details the procedure in place for daily backup of all ACCESS Apha Server, Windows and Linux systems.

Technology – Alpha Server (deprecated 2022)

ACCESS currently uses *Data Protector* and *TSM* (through the MCOECN) software to backup all data. A copy of all backed up data is stored both locally as well as offsite. Locally stored backups permit instant recovery of data without the necessity of retrieving data from the offsite vault, while still protecting the integrity of data in the event of a catastrophic event. The benefit of the *Data Protector* solution is the limiting of human interaction involved in the backup procedure with the exception of the following:

- Review of daily backup logs
- Adding additional tape media when available media is low
- Sending and receiving tape media to the offsite backup vault
- Manually correcting software issues for hosts that did not back up correctly

Procedure

Alpha Server

The Alpha server is backed up with *Data Protector* and *TSM* client backup software with data sent nightly to the MCOECN DR Site in Columbus, Ohio. Likewise, data is also stored offsite locally for easy retrieval. The daily backup log files are stored in the following location: SYS$COMMON:[ADSM.LOGS]

Windows and Linux Servers

Back-up for Windows and Linux virtual servers occur as follows.

- Virtual devices are backed-up and replicated utilizing *Veeam Backup and Replication* software installed in a virtual environment. The nightly backup occurs on all files. Backups are stored on an Netapp SAN at both the main data center as well as a secondary disaster recovery location.

Backup Retention and Data Availability

The following sections will provide a detailed list of data ACCESS currently has available to its member districts by service area. All files are backed up for a minimum of 30 days with the current backup strategy in place. Any additional data and its associated retention period are available below.

FISCAL (USPS-r & USAS-r)

Daily backups
- ➢ One(1) previous day

Monthly backups
- ➢ 45 days

Yearly backups

- Seven (7) years from current fiscal year are immediately available on the system

Reports

- Ten (10) years

Software Versions

- Dependent on the State Software Development Team’s availability.

EMIS

Every Reporting Period

- Seven (7) years

EMIS Reports

- Seven (7) years

STUDENT

ACCESS Student Information servers are located at our data center.

- A SQL database synchronization runs every 15 minutes to disk local to the DB server.
- A SQL backup (create the BAK files) runs nightly with the entire server being backed up to our off-site disk storage nightly.
- ACCESS retains a 10-day backup of the entire server.

INFOhio

- Servers are all hosted at the Ohio Supercomputer Center (SOCC)
- Solaris backups are retained for 30 days and are stored in AWS

ACCESS Email Retention Policy

ACCESS utilizes an archiver appliance and *Google Vault* as our email archiving solution.

- Retention period for archived material is a minimum of seven (7) years.
- Delegated administration is available for school districts wishing to retrieve read-only historical data.

Archiving by ACCESS does not constitute the retention of records in accordance with Ohio law, but is rather a backup to prevent against a loss of Users email records for a set period of time. ACCESS shall not be responsible or liable for the improper destruction of records by the User under the public records laws of Ohio.