

Data Backup

Service Description

The Data Backup service backs up application and end user data, and provides restoration of data due to loss or corruption.

1. Data Backup – Standard

- One backup per 24 hour period.
- Data will be retained for a maximum of 30 days. If a longer retention period is required, see Data Backup – Custom.
- Backup data is replicated off-site.

2. Data Backup – Custom

- Data Backup – Custom includes everything contained in Data Backup – Standard, plus any additional direct hardware and/or software costs incurred to meet the customer's unique requirements. Support for system backups that are more frequent than once per 24 hours or support for a system snapshot (i.e., a backup of an entire system at a particular point in time) are examples of Custom Backup requirements.

Service Notes*

- A request for file or system restoration must be made through the DTO Service Desk.
- Requests for a retention period of longer than 30 days will be reviewed on a case-by-case basis.

****See Service Detail for additional important Service Notes and Customer Responsibilities.***

Customer Benefits

- **Retrieval** – Eliminates the need for agencies to maintain local storage in support of backup and restores.
- **Cost-savings** – Customers do not need to procure, maintain or support hardware and/or software for data backups.
- **Experienced, Knowledgeable Staff** – Admin technical support staff is highly experienced with the backup software and in the use of specialized backup and restore hardware devices and appliances.
- **Support** – Service support is provided by Admin staff skilled and experienced in planning, supporting and troubleshooting the service.

Service Rates

Service Offering	Cost
Data Backup – Standard	Contact ARM
Data Backup – Custom	Standard Backup and Restore Price per GB, plus actual costs incurred by Admin for additional hardware/software

Data Backup – Service Detail

This Admin service includes:

1. Data Backup – Standard

Hardware

- Backup hardware technologies and associated connectivity components required for backups (e.g., EMC Avamar, SAN Disk Controllers, SAN Disk Arrays, VTLs, etc.).

Software

- Backup software management tools and technologies as required (e.g., backup software management tools, backup software client agents, etc.).

Installation and Configuration

- Installation and configuration of supported client storage software versions on Admin approved and supported physical and virtual servers at the State Data Center.

Support and Administration

- Incident resolution.
- Monitoring and alerting via email on all supported backup platforms (e.g., failed backup jobs, etc.).
- Monitoring of the backup infrastructure to assure availability and functionality.
- Replication of backup data off-site.
- Upon request, Admin will email a daily backup status report of customer backups. The report will highlight risk areas such as missed or partial backups.

Physical Security and Facilities

- Host all hardware technologies in the secure State Data Center, with appropriate security and environmental controls such as: biometric access control, internal and external security camera coverage, 24/7 armed guard, conditioned power, emergency power, fire detection and suppression, and temperature control.

2. Data Backup – Custom

- Everything listed above for Data Backup – Standard, plus any additional hardware and/or software costs incurred by Admin to support customer requirements that are beyond the standard service. Actual hardware/software costs incurred by Admin will be charged on a pass-through basis to the agency.

Related Services

A Data Backup customer might also be interested in these Admin services which are offered separately:

- Enterprise Storage
- Virtual Servers

- Database Hosting
- Enterprise Content Management (ECM) Hosting

Service Level Objectives

Service Level Targets

TBD

Additional Service Notes

- Planned maintenance (e.g., firmware updates) will occur during non-production hours and will adhere to the enterprise change management process.
- Admin can accommodate litigation holds, which may require retention of data longer than 30 days. The agency should communicate such requirements, and Admin will modify the retention period for the affected data as needed.

Customer vs. Admin Responsibilities

This section identifies in detail the Admin and customer responsibilities for these service offerings.

Responsibilities	Admin	Customer
Monitor the backup infrastructure to assure availability and functionality.	X	
Maintain the backup infrastructure on supported software and hardware.	X	
Notify customers and schedule an appropriate time when backup system maintenance is required (outside of planned maintenance windows).	X	
Provide support and assistance with backup problem resolution.	X	
Assure compliance with all backup requirements.	X	
Provide off-site storage of backup data.	X	
Notify the customer when the backup client software must be upgraded.	X	
Provide the contact person, phone number and an email address to Admin for correspondents regarding back up infrastructure issues.		X
Notify Admin of any federal, state or county compliance requirements. Agency shall attach relevant documentation identifying the deficiency and the requirement for compliance. The document will be kept on file for audit disclosure and a record authorizing the compliance or change.		X

Responsibilities	Admin	Customer
Provide at least one week for backup schedule modifications (add, change or delete) or the removal of any client machine from this service.		X
Client-maintained (unmanaged virtual or physical hosted) server operating system software upgrades should be performed in a timely manner to ensure software support and license compliance with the backup infrastructure.		X
Monitor backup reports and client logs daily for missed or partial backups.		X
Provide tools and procedures to address any corruption that may result from the backing up or restoring of files that were open during a backup.		X
Publish backup schedules.	X	
Identify backup requirements.		X
Publish data retention periods.	X	
Identify retention requirements.		X
Manage offsite backup infrastructure and onsite backup infrastructure.	X	
Publish notifications of backup infrastructure, OS, and backup product compatibility updates and refreshes as needed.	X	
Verify application data backup is successful (as scheduled); troubleshoot all failures to resolution.	X	X
Verify the integrity of the customer data restored from backups.		X
Provide and publish standard maintenance windows and administrator support for infrastructure upgrades (hardware and software), product refreshes and repairs as required.	X	
Provide, upon request, daily backup success/failure reports via email for customer review.	X	
Develop the appropriate startup and shut down scripts for agency applications and or databases as required for proper application backup.		X

All services are delivered in compliance with State of South Carolina Information Security policies, as presented in SCDIS-200.