TERRY E. BRANSTAD, GOVERNOR
KIM REYNOLDS, LT. GOVERNOR

ROBERT VON WOLFFRADT
CHIEF INFORMATION OFFICER

State of Iowa - Data Backup Operational Standard

September 2, 2014

Purpose

To prevent the loss of all operational and historic electronic data in the custody of the State by ensuring timely backup and data restoration capability in case of disaster.

Overview

The State of Iowa is dependent on electronic data to conduct government business. In emergency disaster efforts Iowa's citizens hold State government to the highest standard for data availability, retention and restoration of backup data to operational status in the shortest time possible.

State government is accountable for exercising effective data backup best practices. State of Iowa agencies are responsible for the following: determining the criticality of data, data backup schedules, data backup capability, security of data backup media, data storage requirements, offsite storage requirements, and data restoration schedules based on agency disaster and contingency plans.

Each agency shall incorporate data backup and data restoration into business plans and development plans.

Scope

All State of Iowa participating agencies, and their vendors that host\store state data, shall meet the requirements of this standard. This standard does not apply to cloud based service providers.

This standard applies to all participating agencies as defined by Iowa Code 8A.101 and in support of SF396 passed by the 85th Iowa General Assembly. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Data Backup Standard are defined below:

- **AES 256** - the Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
- **Contingency Plan** – Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
- **Data Backup** – refers to making copies of data that may be used to restore the original data after a data loss event.

Elements

The following are elements of the Enterprise Data Backup Operation Standard:

1. Each agency shall establish backup policies and procedures.
2. Data backup shall be used for the purpose of disaster recovery and file restoration. This standard does not satisfy records management\retention laws or policies.
3. Each agency will establish and follow written procedure for the conduct of data backup addressing the following areas:
   - data backup hardware
   - software configuration
   - technician training
   - technician data backup procedures
   - data identified for back-up
   - data backup schedules
   - vendor support
   - security measures
   - data backup media requirements
   - approved off-site storage facilities
   - restoration plans
   - restoration schedules
   - technician restoration procedures
   - emergency procurement plans.
4. Each agency shall establish metrics for minimum acceptable condition (retentivity, rewrites, and optical longevity) of storage media before committing backup data to storage.
5. Each agency shall test data backup and restoration procedures for hardware and software applications. Data backup recovery plans shall be exercised at least once a year. The restoration exercise must consider risk and not interfere with current operations.
6. Each agency shall encrypt backup confidential (as defined in Iowa Code Chapter 22.7) data in transit and at rest. Media containing backup data shall be encrypted. A minimum of AES 256 shall be used.
7. Each agency conducting data backup for other agencies will establish agreements with each other in accordance with applicable State of Iowa IT standards and requirements:
   - lines of communication
   - security reviews
   - audit log analysis
   - security incident reporting/response
   - contingency plans
   - change management
   - security plan maintenance
   - planned disconnection
   - emergency disconnection
   - restoration of interconnection
   - data restoration
   - data backup systems policy
   - data integrity
   - expected behavior of the data backup service(s).
8. Collaboration between agencies is strongly encouraged to minimize the number of unique systems and implementations to reduce costs for taxpayers.

9. Each agency shall ensure data backup data remains available to support agency requirements.
10. Agencies shall determine criticality of data and systems.

Updates: This document shall be reviewed at least every two years and updated as needed.

Effective Date: This revised standard shall be effective September 2, 2014.

Enforcement: This standard shall be enforced pursuant to Iowa Code 8B.21.

Waiver: A wavier may be submitted to the State's Chief Information Officer as defined in Iowa Code 8B.21.5.