Standard ID:	PL-DR-002
Title:	**Backup, Recovery and Retention Guidelines**
Revision Number:	1
Domain:	Information
Discipline:	Backup
Effective:	01/13/2023
Reviewed:	06/27/2023
Approved By:	Chief Operating Officer
Sponsor:	Chief Operating Officer

I. Authority, Applicability and Purpose

A. Authority: Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"

B. Applicability: Applies to all State of Delaware communications and computing resources. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of funding, access and continued use of these resources.

C. Purpose: The objective of this guideline is to define the minimum procedures and guidelines for backup, recovery, and retention of the State of Delaware electronically stored information. Information stored and processed on Information Technology (IT) systems is vulnerable to accidental degradation, intentional corruption or deletion, hardware/software failures, and natural or man-made disasters. A backup and restore guideline is essential to ensuring recovery of information and the ability to continue IT support of critical State business functions. System backups also are an essential component of contingency planning strategies. Backups enable IT support personnel to quickly and reliably recover essential data and software in case of events such as natural or environmental disasters, system or application failures, sabotage, data/system integrity errors and/or system operations errors. In addition, to define when data should be archived for retention purposed to comply with state or federal regulations.

II. Scope

A. Areas Covered: Any location such as on-premise, cloud, etc.

B. Environments: Production environments

III. Process

A. Adoption: These guidelines have been adopted by DTI through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. Revision: Technology is constantly evolving; therefore the guidelines will need to be regularly reviewed. It is the intent of the TASC to review this guideline annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors: Contractors or other third parties are required to comply with these guidelines when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection of the proposed technology solution. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. Implementation responsibility: DTI and/or the organization's technical staff will implement these guidelines during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement: DTI will enforce these guidelines during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These guidelines may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us: Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Definitions/Declarations

A. Definitions

1. Backup

   i. Backup – The saving of electronic information onto magnetic tape or other offline mass storage media for a limited time for the purpose of preventing loss of data in the event of equipment failure, destruction, accidental loss, or corruption. While most backups are on magnetic tape-based media today, the term "Backup" or "Backup Media" may also reference other backup media technology including but not limited to, Optical (CD, DVD, etc), virtual tape systems, USB drives, and other removable media.

   ii. Backup Plan – The schedule of which files should be saved and when. A Backup Plan defines how many backup cycles are to be kept and how media is reused.

2. Recovery
    i. Recovery Point Objective (RPO) – The recovery point objective (RPO) is an important consideration in disaster recovery planning. It represents the age of files that is recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a failure.
    ii. Recovery Time Objective (RTO) – The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application is down after a failure or disaster occurs.
    iii. Restore – The process of bringing ESI back from off-line media and putting it on an online storage system when the data on the online storage system is lost or corrupted.
    iv. Disaster Recovery – The policies, process, and procedures related to preparing for recovery or continuation of technology infrastructure critical to the State of Delaware after a disaster. Disaster recovery focuses on the restoration of IT or technology systems that support business functions that fail in the event of a disaster.
3. Retention
    i. Archives –
        1. The records created or received and accumulated by a person or organization in the course of the conduct of affairs, and preserved because of their historical or continuing value
        2. The agency responsible for selecting, preserving, and making available records determined to have permanent or continuing value.
        3. The building in which an archival repository is located. See also Delaware Public Archives.
    ii. Archival Value – The enduring worth of documentary materials for continued preservation in an archival repository. May also be referred to as historical, continuing, or enduring value.
    iii. Data Archiving – Data archiving is the process of moving data that is no longer actively used to a separate data storage device for long-term retention. Data archives consist of older data that is no longer changing or shouldn't be changing, is still important and necessary for future reference, as well as data that must be retained for regulatory compliance. Data archives are indexed and have search capabilities so that files and parts of files can be easily located and retrieved.

iv. Public Records – Any document, book, photographic image, electronic data recording, paper, sound recording or other material regardless of physical form or characteristics, including electronic records created or maintained in electronic information systems, made, used, produced, composed, drafted or otherwise compiled or collected or received in connection with the transaction of public business or in any way related to public purposes by any officer or employee of this state or any political subdivision thereof.

v. Retention Instructions – Specific instructions directing the minimum retention for each record series. Remarks indicate length of time that the record should be retained by the agency and the events or time periods that need to occur before disposition of the record series can be effected. Exceptions to the retention instructions are noted.

vi. Retention Schedule – A list of record series which describes an agency's records; establishes a minimum period for their retention by the agency and provides mandatory instructions on what to do with them when they are no longer needed for current business. Also called records disposition schedule, records control schedule, records retention schedule, records retention and disposition schedule, or schedule.

vii. Retention Time – The amount of time in which a given set of data will remain available in compliance with state or federal regulations.

4. Electronically Stored Information (ESI) – General term for any electronic information stored in any medium (i.e., hard drives, back-up tapes, CDs, DVDs, jump drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
5. Encryption – The process by which data is temporarily rearranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.
6. IT Systems – The hardware and software used to store, retrieve, and manipulate information.

.

B. Declarations

1. This guideline applies to all State of Delaware electronically stored information, whether stored on premise or in the cloud.
    - An agency should create a backup plan that provides a minimum of four or more weeks of restoration for all production IT systems.
    - Non-production environments are not required to be backed up unless there is a specific business need.
    - Database and file storage servers should be backed up on a daily basis.
    - Web and application servers can be backed up less often depending upon the frequency of changes to the server.

2. Backups should be frequent to match stated RPO for the application. A daily database backup does not meet RTO of anything less than 1 day.
3. The recommended philosophy for backups is the 3-2-1 strategy. There should be 3 copies of the data (production, backup, offsite backup). The copies should be stored on at least 2 types of media (tape or different storage). Finally, one offsite copy for disaster recovery is recommended.

V. Guidelines

A. Backup

1. A backup of the organization's data files and the ability to recover such data is a top priority. Organizations' local management should assess the business process by the supported data and/or systems and assign a Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The backup of the associated media should correlate to the RPO/RTO. In addition to RPO and RTO, recovery objects need to account for time to restore or make operational the backup system. If there are multiple systems with same or similar RPO, there should be priority of recovery. In addition, the backup methods must support the RPO and RTO.
2. Data backups must be encrypted for State of Delaware confidential, secret and top secret data. Furthermore, State of Delaware confidential, secret and top secret data must only reside at rest on State owned or DTI approved systems or devices.
3. The vendor(s) providing offsite backup storage for State data should have appropriate clearances for the highest level of data classification stored. Physical access controls implemented at offsite backup storage locations should meet or exceed the physical access controls of the source systems. Additionally, backup media is protected in accordance with the highest State sensitivity levels for information stored.
4. Storage media protection and authentication controls at the storage system and media levels should be implemented to provide strong barriers against unauthorized stored data disclosure, theft, and corruption.
5. Backup media should be stored in a locked, fireproof container (UL-rated for media protection) during transport and while being retained at a pre-determined offsite location unless an approved offsite vaulting service is used (e.g. Iron Mountain, VRI, etc.). Backup media must be stored according to the application's Disaster Recovery Criticality and Level, as specified in the Delaware Information Security Policy, unless other DTI approved mitigating factors are put in place to protect the State's data.

B. Recovery

1. IT management should ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files, especially where such files may replace more recent files.

2. A process should be implemented to verify the success of the electronic information backup. Backups are periodically tested to ensure that they are recoverable within the expected timeframe. Testing helps to identify if:
   - **a)** Backups are incomplete.
   - **b)** Backup software was wrongly configured.
   - **c)** Encryption has caused a lockout (unknown password).
   - **d)** Backup is only readable by an earlier version of your software.
   - **e)** Backup cannot perform the restore from backup media which is several months old.
   - **f)** Dormant backup software bugs now plague your newly upgraded operating system.
   - **g)** The tape breaks during backup process.
   - **h)** Unexplained reboots could have caused a system crash and tape rewind during the backup process.
3. Signing Authorities held by the offsite backup storage vendor(s) for access to State backup media is reviewed annually or when an authorized individual leaves or changes job responsibilities.
4. Procedures between organization and the offsite backup storage vendor(s) are reviewed at least annually.
5. Backup tapes and/or containers should be identified by labels and/or a bar-coding system.

C. Retention

1. The retention of electronic data files should reflect the business needs of an agency, as well as any legal and regulatory requirements for records retention, such as Delaware Public Records Law (29 Delaware Code §501-526) and the Delaware Freedom of Information Act (29 Delaware Code Ch. 100 et seq.). The storage media used for the archiving of information should be appropriate to its expected longevity. The format in which the data is stored is carefully considered, especially where proprietary formats are involved. The archiving of electronic data is to be retained in a manner consistent with the Delaware Public Records Law requirements as provided in the Agency's Specific Retention Schedules and the State General Retention Schedules and by using the procedures of the Delaware Public Archives (DPA) for authorizing records disposition:
   - **a)** Model Guidelines for Electronic Records
   - **b)** State of Delaware retention schedules are located here
2. Regulations often include the retention period that is required for certain types of data.

D. To maximize efficiency, reduce costs, and minimize risks agencies should manage data and information effectively to lower the storage footprint. Through active storage management, storing key information in shared repositories appropriate to its classification, avoiding storing duplicates, utilizing deduplication, and routinely reviewing retention schedules agencies should be able to contain and lower storage growth.

VI. Development and Revision History

Date	Revision
1/13/2023	Rev 0 – Initial version based on a prior policy
6/27/2023	Rev 1 – Clarifying the backup vs recovery vs retention guidance.