STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	PL-DR-001	**Revision Number:** 1
Document Type:	Enterprise Policy	**Page:** 1 of 8
Policy Title:	Data Backup & Retention Policy	

Synopsis:	This policy defines the State of Delaware's established protocol for Backup, Recovery and Retention of electronically stored information for operational and regulatory compliance needs.		
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"		
Applicability:	This Policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, 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 access and continued use of these resources.		
Effective Date:	01/31/2017	**Expiration Date:**	None
POC for Changes:	Jason Clarke, Chief Operating Officer		
Approval By:	James Collins, Chief Information Officer		
Approved On:	03/29/2016		

TABLE OF CONTENTS

Section		Page
I.	**Policy**	2
II.	**Definitions**	5
III.	**Development and Revision History**	8
IV.	**Approval Signature Block**	8
V.	**Listing of Appendices**	8

I. Policy

PURPOSE

The objective of this policy 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 policy 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.

POLICY STATEMENT

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

2. A backup of the organization's data files and the ability to recover such data is a top priority. Organizations' local management must 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 must correlate to the RPO/RTO.

3. The archiving of electronic data files must 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 must 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

4. Data backups on removable media 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.

5. IT management must 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.

6. The vendor(s) providing offsite backup storage for State data must have appropriate clearances for the highest level of data classification stored. Physical access controls implemented at offsite backup storage locations must 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.

7. 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.

8. Backup media must 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 System Architecture Standard, unless other DTI approved mitigating factors are put in place to protect the State's data.

9. A process must 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:
    - Backups are incomplete.
    - Backup software was wrongly configured.
    - Encryption has caused a lockout (unknown password).
    - Backup is only readable by an earlier version of your software.
    - Backup cannot perform the restore from backup media which is several months old.
    - Dormant backup software bugs now plague your newly upgraded operating system.
    - The tape breaks during backup process.

- Unexplained reboots could have caused a system crash and tape rewind during the backup process.

10. 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.

11. Procedures between organization and the offsite backup storage vendor(s) are reviewed at least annually.

12. Backup tapes and/or containers must be identified by labels and/or a bar-coding system.

13. Regulations often include the retention period required for certain types of data.

14. 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.

IMPLEMENTATION RESPONSIBILITY

DTI and/or the organization's technical staff will implement this policy during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

ENFORCEMENT and WAIVER

DTI will enforce this policy 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. This policy may also be enforced by others during the course of their normal business activities, including audits and design reviews.

If there is ambiguity or confusion regarding any part of this policy, contact the point of contact defined in the header of this policy.

II. Definitions

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.

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.

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.

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.

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.

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.

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.

Encryption – The process by which data is temporarily rearranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.

IT Systems – The hardware and software used to store, retrieve, and manipulate information.

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.

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.

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.

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.

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.

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.

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

III. Development and Revision History

Initial version established on 03/29/2016 with effective date of 01/31/2017.

Amended to clarify usage of approved vaulting service and backup media storage requirements 10/06/2016.

IV. Approval Signature Block

Name & Title: James Collins State Chief Information Officer	**Date** 10//06/2016