
Retention of Data Backup Media and Records Management Media - Guideline [1]

Topics:
[backup media](#) [2], [records management](#) [3], [document management](#) [4], [retention schedule](#) [5], [disposal](#) [6],
[legal hold](#) [7], [public record](#) [8], [purge](#) [9]

GM-13-001 Retention of Data Backup Media and Records Management Media

Issue Date: 4/01/2013

Effective Date: 5/15/2013

GUIDELINE

Data Backup refers to the copying and storage of computer data for a limited period for the purpose of being able to restore data back to an original state after a data loss event ([SS-08-046](#) [10]). Backup media refers to the devices upon which data is stored: tape, disk, optical storage, etc. Each agency should create a backup media plan (Backup Plan) that should provide for up to one (1) year of generational backups to support recovery in the event of a data loss ([SS-08-027](#) [11]). Backup Plans should include consideration of the data criticality and should follow a best practice rotation scheme in order to reduce the State's risks from loss of data ([SS-08-046](#) [10]).

Agencies should ensure that media is sanitized (to clear or purge data) according to the frequency defined in the Backup Plans prior to recycling media for subsequent use ([SS-08-034](#) [12], [SS-08-035](#) [13], [SS-08-043](#) [14]). Backup Plans requiring a rotation schedule for media longer than three (3) years must be approved annually by the agency head and the plan shall include the projected annual cost.

An agency's Records Management process may include storing electronic records for legal and operational requirements in consideration of both State and Federal requirements. Records retention periods for specific electronic records are derived from an agency's records retention schedule ([PS-08-007](#) [15], [SS-08-003](#) [16]). Media used for storing these records may include the same types of devices used for Data Backup media, but generally are selected from devices which support longer terms of retention ([SS-08-027](#) [11]). Data Backups are not to be considered to be a component of an agency's Records Management methodology unless the agency specifically identifies it as such.

Electronic records captured during Records Management that exceed their specified retention period shall be disposed of in a systematic and controlled manner, subject to an appropriately defined and invoked Legal Hold of specific records ([SS-08-034](#) [12], [SS-08-035](#) [13], [SS-08-043](#) [14]). Media devices (magnetic tapes, optical storage, Network Attached Storage) may be reused if possible.

Nothing in this guideline is intended to supersede any regulatory requirements imposed on an agency concerning Data Backup or backup media.

BACKGROUND

Information systems use stored data for a variety of purposes for daily usage in active databases, for recovery from loss with a system of data backup and for business purposes in Records Management storage. Media used for these storage purposes may include magnetic tape, hard disk, optical storage or a large variety of others.

One component of managed infrastructure services implemented in the State's enterprise data center in 2009 is a managed inventory of stored electronic media resulting in agency-itemized billing for media upon which electronic records are stored. The resulting costs indicate that electronic records in storage appear to be exceeding reasonable retention periods, and storage costs are soaring. Data storage requirements can be significant and the agency should be cognizant of cost drivers when selecting frequency and method of backup.

Backup

Backup is defined as copying data to protect against loss of integrity or availability of the original data. Backup is one of the three linked techniques of backup, verification and recovery. An agency needs processes to verify stored backups to ensure that data can be recovered when needed and to ensure recovery can be accomplished in the event of loss. Because of costs, a major premise of backing up systems is to avoid performance impact in key or critical business systems in the event of a loss event. The agency should not incur the cost of backing up a system if the impact of loss is merely an inconvenience. Any digital media created to permit recovery in the case of disaster has value for only a short period of time. Current recommended practices argue for maintaining backup or disaster recovery media for no more than one year or twelve rolling months. After that period, changes in active data or even the system itself may make the data obsolete.

Records Management

The Georgia Records Act requires agencies to manage their official records and includes the retention of both paper and electronic records which are necessary for the conduct of agency business. Georgia Law provides that Agency Heads have the authority to determine the nature and form of records required in the administration of the agency. In addition, federal laws and regulations may impact records retention of agencies operating under federal programs. The Georgia Records Act designates the definitive source in State government for information and assistance in building an appropriate records management organization as well as records retention master schedules upon which agencies may build schedules that meet their specific needs.

Because of overlap in technology, **backing up** electronic systems is often confused with **Records Management**. Electronic records derived from Records Management processes may contain the primary copy of records set aside as documentation of agency business activities, and are often made to satisfy long-term business or legal requirements. A good Records Management process ensures:

- That records with little to no business impact are not retained,
- That records are retained only as long as legally and operationally required, and
- That at the end of their retention period, obsolete records are disposed of in a systematic and controlled manner.

The process requires a means to verify that data can be recovered to a usable form, and includes a means to extend the retention period, if necessary, for selected data. Records retention schedules are set by

State agencies to meet, at least, minimum requirements of applicable laws and regulations as well as for future business access.

GTA has published an enterprise policy and standard addressing components of backup. Please reference Business Continuity and Disaster Recovery [PS-08-025](#) [17] and Disaster Recovery System Backups - [SS-08-046](#) [10]. These items can be found on [GTA's public web site](#) [18].

Each agency must interpret its own needs for backup and for records management activities, issue agency policies in support of these needs and enforce the policies in practices. The procedural requirements are not trivial and at times quite complicated.

FREQUENTLY USED TERMS

Backup (or Data Backup) - Copying data to protect against loss of integrity or availability of the original.

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

Business Continuity Management ? The act of anticipating incidents which will affect critical functions and processes for the organization, and ensure that the organization responds to any incident in a planned and rehearsed manner.

Contingency Plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or disaster. Below are other terms often used interchangeably but actually refer to a suite of plans developed to prepare for and to execute contingency efforts:

- **IT Contingency Plan** - The dynamic development of a coordinated recovery strategy for IT systems (major application or general support system), operations, and data after a disruption
- **Business Contingency Plan** - The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption
- **Disaster Recovery Plan** - A written plan that details how an organization's applications and/or infrastructure will be recovered or rebuilt and returned to normal operations after a major hardware or software failure or destruction of facilities.
- **Continuity of Operations Plan** - A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Legal Hold - A process which an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated

Operational Priority ? A categorization of the criticality of a business application to the core mission of an agency:

Priority	Description

P0	A Priority 0 Application is one that has a hardware and software infrastructure that is architected for high availability (e.g. failover). An example of a Priority 0 Application is one that is associated with life/limb services.
P1	A Priority 1 Application is an application that performs critical business functions and is critical to the agency performing its core mission.
P2	A Priority 2 Application is an application that performs key functions that are ancillary to the critical business applications.
P3	A Priority 3 Application is an application that performs administrative functions that do not impact critical applications but that are key to an agency.
P4	A Priority 4 Application is any other applications that are not critical or key but are needed for miscellaneous functions.

Records Management - The development and implementation of a life-cycle management process from the creation and receipt of records, through their active life, storage, and to their final disposition. According to the Georgia statute "Records management" means the application of management techniques to the creation, utilization, maintenance, retention, preservation, and disposal of records undertaken to reduce costs and improve efficiency of record keeping. "Records Management" includes management of filing and microfilming equipment and supplies; filing and information retrieval systems; files, correspondence, reports, and forms management; historical documentation; micrographics; retention programming; and vital records protection.

Records - All documents, papers, letters, maps, books (except books in formally organized libraries), microfilm, magnetic tape, or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in performance of functions by any agency (The Georgia Records Act).

Records Retention ? The term "Records Retention" may refer to a process or refer to a period of time that records are stored. It is the process of storing electronic records for legal and operational requirements. When used to refer to a period of time, the term describes period of time that an agency must retain specific electronic records.

Records Series - Documents or records having similar physical characteristics or relating to a similar function or activity that are filed in a unified arrangement

Recovery ? Recovery means the restoration of a system, program, database, or other system resource to a prior state following a failure or externally caused disaster; for example, the restoration of a database to a point at which processing can be resumed following a system failure.

Retention Schedule - A set of disposition instructions prescribing how long, where, and in what form a record series shall be kept (The Georgia Records Act).

Security Classification ? Security classifications of "Low", "Moderate" or "High" are assigned to data and processing systems according to the potential impact of loss or compromise of the information and/or processing system, based on an assessment of risk, business objectives and the security objectives of

confidentiality, integrity and availability. Georgia has adopted the definitions from Federal Information Processing Standards (FIPS) 199 (SS-08-014).

EXISTING GEORGIA ENTERPRISE POLICIES AND STANDARDS

[Business Continuity and Disaster Recovery PS-08-025](#) [17]

[Disaster Recovery System Backups SS-08-046](#) [10]

[Design Criteria for Electronic Records Management Applications SA-06-006](#) [19]

[Media Controls PS-08-026](#) [20]

[Surplus Electronic Media Disposal SS-08-034](#) [12]

[Systems Operations and Documentation SS-08-027](#) [11]

[Data Categorization ? Impact Level SS-08-014](#) [21]

REFERENCES

Georgia Records Act is found in the Official Code of Georgia Annotated (O.C.G.A.) 50-18-90

[NIST SP 800-34](#) [22] Contingency Planning Guide

[NIST SP 800-84](#) [23] Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

[ITL April 02](#) [23] Techniques for System and Data Recovery

[ITL June 02](#) [24] Contingency Planning Guide for IT Systems

BEST PRACTICES REFERENCES

The IT Governance Institute (ITGI) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly allocated, and IT performance is measured. ITGI developed [Control Objectives for Information and related Technology \(COBIT®\)](#) [25] and the [Information Technology Infrastructure Library \(ITIL\)](#). [26] COBIT® is a comprehensive set of resources that contains all the information organizations need to adopt IT governance and control framework. ITIL, a best practice product owned by ITGI, is the most widely accepted approach to IT service management in the world.

The Information Technology Laboratory (ITL) at the [National Institute of Standards and Technology \(NIST\)](#) [27] promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than

national security-related information in Federal information systems.

Source URL: <https://gta.georgia.gov/psg/article/retention-data-backup-media-and-records-management-media-guideline>