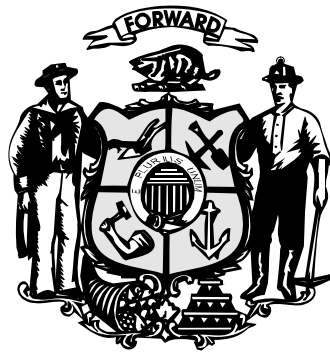


General Records Schedule

Information Technology Business Records

December 2007



**First Edition- Approved September, 2007
Amended May, 2008**

**For use by
State of Wisconsin Government Agencies
RDAs IT000001-IT000035**

TABLE OF CONTENTS

Procedures and Form for Agency Adoption of the Information Technology Business
General Records Schedule - See Appendix 2.

Purpose.....	3
Who May Use General Schedules	4
Record Schedules Do Not Require Creation of Records	4
Records Management.....	4
Records Management within an Individual State Agency	4
Records Management among State Agencies.....	5
Records Management within the University of Wisconsin System.....	5-6
Records Series Titles and Categories.....	6
Electronic Records.....	6
Retaining Records	6-7
Confidentiality of Records.....	7
Personally Identifiable Information	7
Definitions	7-8
Legal Term Glossary	8-9
IT Term Glossary.....	9-13
For Additional Information and Assistance	13
Appendix 1 - Summary of Approved Statewide General Records Schedules	30-31
Appendix 2 – Agency Agreement to Use General Schedule Policies and Procedures	32-33
Appendix 3 – Notification of General Records Schedule Adoption	34

PURPOSE

A General Records Schedule provides legal authorization to dispose of common records on a regularly scheduled basis. The purpose of this schedule is to:

- Provide agencies with uniform guidelines for the retention and disposition of common records in all forms, including electronic and hard copy data and information.
- Ensure that agencies maintain adequate documentation of Information Technology transactions and activities to meet internal administrative needs, legal mandates, and program and financial audit requirements.
- Promote the cost-effective management of records.
- Provide agencies with legal authorization to dispose of obsolete records on a regularly scheduled basis after minimum retention periods have been met.

The *General Records Schedule for Information Technology (IT) Business Records* covers records series created, received, used, dispersed and managed by IT business organizations including state-wide IT processing centers, central agency IT operations, or administered by decentralized IT staff located in agency program organizations.

INTENTIONAL OMISSIONS

Automated Applications

IT holds records and facilitates data processing/web presentation for the customers they serve. As a result, IT is not the owner of customer business records. Program and system application records are covered by separate Records Retention / Disposition Authorizations (RDAs) or other General Records Schedules (GRS) based on the business needs of the area responsible for the related program or system application.

- **Computer Applications**

The data collected, processed and outputted from computer applications belongs to programs and must be scheduled by the program. IT may facilitate the retention/disposition of that data as documented in the program RDA.

- **Web Content**

This GRS does not address static or dynamic content presented on the internet/intranet. Subject matter experts (i.e., program / business area staff) are the web content owners and have the responsibility for scheduling and retaining web records to meet the program business needs

Backup Processes

As the use of back-up storage is currently inconsistent among state agencies, and no consensus has been reached, this issue will be addressed in future updates to the IT General Schedule.

A "backup" process refers to making copies of original data so the copies are available for restoring if the original data is lost. Those additional copies are typically called "backups." Backups are used for two reasons: 1) to restore a computer/server to an operational state following a major loss of data (disaster recovery) and 2) to restore small numbers of files after they have been accidentally deleted or corrupted.

Backups are not designed to be used for records retention. In those cases where agencies are currently depending on backups for records retention purposes, the back-ups must be scheduled for the longest retention period of any information carried on the medium. Retained backups may be subject to discovery requests.

WHO MAY USE GENERAL SCHEDULES

General schedules apply to all Wisconsin state agencies. Any state agency may adopt any or all of the authorizations in any general records schedule approved by the Public Records Board by opting in or out in whole or in part. See the related policies and procedures associated with opting in and out of general records schedules. These schedules will be located on the [Public Records Board's website](#).

RECORD SCHEDULES DO NOT REQUIRE CREATION OF RECORDS

It is understood that all agencies may not have all the records listed in this schedule. This schedule does not require records to be created by agencies, rather it provides guidance for actual records that are created or received by agencies.

RECORDS MANAGEMENT

Under Wisconsin law, each state agency is responsible for properly managing its records with approval from the Public Records Board. Proper records management can become complex, however, especially when: the same records are held by more than one department within a state agency, or multiple state agencies possess the same records. Accordingly, this schedule provides guidance for:

- A) Records management among the departments of a single state agency, all of which have custody of the same or similar records; and
- B) Records management among different state agencies, all of which have custody of the same or similar records.

A. Records Management within an Individual State Agency:

For every record series, each state agency must identify the location of the official record. The official record is retained to satisfy records schedules approved by the Public Records Board. All copies of the official record that are maintained by different departments or programs within the same agency are classified as duplicates under the law. It is important to understand that duplicates of a record are not regulated by statute, therefore in the interest of efficient resource allocation, duplicate records should be retained only so long as needed in order to complete work projects and thereafter destroyed. Wis. Stats. § 16.61(2)(b).

Also note that duplicates, as well as public records that have been retained beyond their approved retention period, may have to be provided in response to relevant: public records requests, audits and litigation. For this reason, it is important to destroy duplicates as soon as they are no longer needed. Similarly expired records should be disposed of as soon as they've reached the proper retention, provided there is no pending open records request, audit or lawsuit.

B. Records Management among State Agencies that have Custody of the Same Records:

Records management is also challenging when the same records are in the custody of more than one state agency. For example, program records are created by one state agency and often cross matched against another agency's program records to provide better customer service or to reduce fraud, delinquent payments, and overpayments. Thereby, two state agencies possess the same records. In order to make this process easier to understand and manage, the following information is provided.

Requirement:

Each state agency must understand that if a record is created and thereafter submitted to another state agency for review or use, then under Wisconsin law both the creator and the receiver of the record must properly maintain the same record. Wis. Stats. § 16.61(2).

Guideline:

Each state agency has authority to recommend to the Public Records Board retention periods for every record, or record series, in the custody of that agency. Wis. Stats. § 16.61(4). In other words, just because two state agencies bear responsibility for properly managing the very same record, they are able to assign different retention periods for that record, so long as the Public Records Board approves.

Example:

If the Department of Workforce Development (DWD) created an Unemployment Insurance (UI) record and then submitted that record to the Department of Revenue (DOR) for data cross match purposes, then DWD and DOR would possess the same record. However, if DOR no longer needs to retain the record after the cross match is complete DOR could request permission from the Public Records Board to destroy its copy of the record upon process completion. In addition, DWD could request a different retention period for that record, in accord DWD/UI's business function for the record.

Management of Records within the University of Wisconsin System:

The University of Wisconsin System bears a unique structure comprising fifteen distinct and autonomous educational institutions, all of which are governed by a single corporate board: The University of Wisconsin Board of Regents.

The Board of Regents' governance authority over these fifteen educational institutions is defined by statute: "The primary responsibility for governance of the system shall be vested in the board which shall enact policies and promulgate rules for governing the system...and promote the widest degree of institutional autonomy within the controlling limits of system-wide policies and priorities established by the board. Wis. Stats. § 36.09(1). Moreover, the Board of Regents may delegate authority to the each Institution within the University of Wisconsin System:

The board shall delegate to each chancellor the necessary authority for the administration and operation of the institution within the policies and guidelines established by the board. The board may also delegate or rescind other authority to chancellors, committees of the board, administrative officers, members of the faculty and students or such other groups as it deems appropriate." Wis. Stats. § 36.09(1)(f).

In accordance with these statutes, the University of Wisconsin Board of Regents is responsible for the proper management of the University's records. However, the Board

may, and often does, delegate or rescind the administration and operation of records management to chancellors, committees of the board, administrative officers, members of the faculty, students, and other appropriate groups.

Therefore, it is important for University employees who manage University records to ascertain whether, and to whom, the Board of Regents has delegated the administration and operation of these records. Thereafter, the delegated authority shall properly manage public records on behalf of the Board of Regents of the University of Wisconsin System and in accordance with records schedules, which have been approved by the Public Records Board.

Records Series, Titles, and Categories:

Individual general schedules provide a listing of each record series, summarizing the retention requirements for official records and suggestions for working copies of the records.

All items within a series relate to the same topic and have the same retention requirements. Each record series in a functional area is described in narrative detail, and may include lists of forms, reports and other items included within the series.

General record schedules must be interpreted and applied to specific records. However, the titles of record series contained within general schedules may not be the exact titles used by an agency for their records or records series. See the section entitled: "For Additional Information and Assistance" for resources to consult.

Electronic Records:

General record schedules cover records in all media. Administrative Rule 12, Electronic Records Management-Standards and Requirements, became effective May 1, 2001. The rule and related information regarding records management for electronic records can be found at

http://www.doa.state.wi.us/section_detail.asp?linkcatid=761&linkid=127&locid=0&sname.

The purpose of this rule is to ensure that public records in electronic format are preserved, maintained, and remain accessible for their designated retention period. Because of frequent technological change, including hardware and software obsolescence and media degradation, agencies must take steps to manage and protect electronic records for as long as they are needed. To meet business needs and protect the legal, financial and historical interests of internal business operations and Wisconsin citizens, agencies must prepare and execute migration plans for electronic records as necessary to prevent them from becoming inaccessible during their retention periods.

Retaining Records:

Records may be delayed from destruction, but only under the following conditions:

- Records are required for an IT system, business program, performance, financial, or security forensic audit;
- Records are relevant to an actual or imminent legal proceeding; or
- A relevant public record request has been received and not completed.

Before disposing of a record, the office managing the record must determine if an audit, litigation, or public record request is pending. And notably, after a public records request has been filed, Wisconsin law forbids the destruction of any relevant record until the

request is granted, or at least 60 days after the request is denied, and court orders may extend this time period. Wis. Stats. § 19.35(5). If agency staff members have questions regarding Wisconsin's Public Records Law, then the agency's legal custodian of records will provide further guidance.

Official records that are inactive, but not yet expired should be transferred to a low-cost, record storage facility, such as the State Records Center.

Confidentiality of Records:

Some records series, in whole or in part, contain confidential records as related to security, and protected personal information. If in doubt as to whether or not a specific record is confidential, it is always a good idea to check with agency legal counsel. If your agency does not have a legal counsel, an Assistant Attorney General in the Department of Justice will provide advice.

Personally Identifiable Information (PII):

Some records in this schedule contain personally identifiable information as defined by Wisconsin law. Wis. Stats. § 19.62(5). Public access to and security of personally identifiable information is often restricted by law. Therefore, agencies should be aware of the requirements in Wisconsin Statutes, Chapter 19, as well as all applicable program specific laws or regulations. If in doubt as to whether a specific record contains personally identifiable information, it is a good idea to check with agency legal counsel. If your agency does not have a legal counsel, an Assistant Attorney General in the Department of Justice will provide advice.

DEFINITIONS

Official Record: The official record is the document that is most likely to be used for multi-agency audit purposes. This record is usually located in the central office of an agency. In decentralized organizations, the official record may be located in an institution, district, field office, cost center, or department.

Duplicate or Working Copies: All duplicate, working, and convenience copies of official records are classified as non-records under Wis. Stats. § 16.61. Therefore, in the interest of efficiency, non-records should not be kept longer than needed, and should be destroyed as soon as possible. It is also important to understand that under Wisconsin law, if non-records are not properly destroyed, then they must be provided to a requester in response to relevant: public records requests, audits, and litigation, even if the official record previously expired and was destroyed in accordance with approved records schedules. Finally, non-records should not be sent to the State Records Center, because they will not be accepted.

Confidential Records: Records marked confidential in these schedules will not be published for general access on the web or disclosed under Open Records requests unless the designated agency authority has performed a balancing test and determined greater public good is served by disclosing the records than not.

Retention Period: The retention period is the minimum length of time an office must keep particular records. This is usually expressed in terms of years, months, days and may be contingent upon an event date or specification date that triggers the “clock.” Most often, retention periods are triggered at: creation (CR), event (EVT), or fiscal (FIS).

Creation (CR): The retention period starts when a record is created or received.

Event (EVT): The retention period is triggered or tied to event dates; thus, retention does not begin until the specified event occurs. For example, if a record series has a retention of EVT+ 1 year and the event is defined as the life of an asset, then all records in this category would be retained one year after the asset is sold, scrapped, or otherwise taken out of service.

Fiscal (FIS): This retention period is tied to the current fiscal year, and unlike CR and EVT retention periods, FIS record series are managed in blocks by fiscal year. For example, “FIS+4 years” indicates that records must be retained for the current fiscal year and four complete additional fiscal years.

Disposition: The final state in a record’s life cycle, involving: destruction or transfer to either the Wisconsin Historical Society or University of Wisconsin Archives for permanent preservation.

Transitory Record

Temporary documents of short-term interest that have no evidential value or are not required by federal recordkeeping requirements or for security purposes.

LEGAL TERMS GLOSSARY

Public Records

Public records are defined as: “all...materials, regardless of physical form or characteristics, made, or received by a state agency or its officers or employees in connection with the transaction of public business.” Wis. Stats. § 16.61(2)(b).

Exceptions to Public Records. Public records do not include: (a) **Wisconsin Legislators:** records and correspondence of any member of the legislature; (b) **State Depository Library:** any state document received by a state document depository library; (c) **Duplicates:** duplicate copies of materials the original copies of which are in the custody of the same state agency and which are maintained only for convenience or reference and for no other substantive purpose; (d) **Library Materials:** materials in the possession of a library or museum made or acquired solely for reference or exhibition purposes; (e) **Unsolicited Notices:** notices or invitations received by a state agency that were not solicited by the agency and that are not related to any official action taken, proposed, or considered by the agency; (f) **Preliminary Materials:** drafts, notes, preliminary computations and like materials prepared for the originator’s personal use or

prepared by the originator in the name of a person for whom the originator is working; and (7) **Routing**: routing slips and envelopes. Wis. Stats. § 16.61(2)(b).

Personally Identifiable Information (PII)

This is information that can be associated with a particular individual through one or more identifiers or other information or circumstances. Wis. Stats. § 19.62(5).

Responsibilities of State Agencies

The term “state agency” is defined as: “any officer, commission, board, department or bureau of state government.” Wis. Stats. § 16.61(2)(d). And “all public records made or received by, or in the custody of, a state agency shall be the property of the state, and these public records may not be disposed of without written approval from the Public Records Board.” Wis. Stats. § 16.61(4).

IT TERMS GLOSSARY

Application

A combination of programs and services designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of applications include word processors, database programs, Web browsers, development tools, drawing, image editing programs, and communication program.

Component

Individual parts of the whole. The discrete parts that must be combined to produce a working and useful result. In programming and engineering disciplines, a component is an identifiable part of a larger program or construction. Usually, a component provides a particular function or group of related functions. Examples of technology infrastructure components include hardware platforms, operating systems, database systems, networks, etc.

Configuration

Generally, a configuration is the arrangement - or the process of making the arrangement - of the parts that make up a whole. Examples of configurations include: In computers and computer networks, a configuration often refers to the specific hardware and software details in terms of devices attached, capacity or capability, and exactly what the system is made up of. In networks, a configuration means the network topology. In installing hardware and software, configuration is the methodical process of defining options that are provided.

Conversion

The process of changing records from one file or database format to another while maintaining authenticity, integrity, reliability, and usability.

Data

Numbers, characters, images, or other method of recording, in a form which can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital channel. Computers nearly always represent data in binary format. Data on its own has no meaning, only when interpreted by some kind of data processing system does it take on meaning and become information. People or computers

can find patterns in data to perceive information, and information can be used to enhance knowledge. Since knowledge is prerequisite to wisdom, we always want more data and information.

Structured Data is data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data. Typically, structured data is managed by technology that allows for querying and reporting against predetermined data types and understood relationships.

Unstructured Data is data that does not reside in fixed locations. Free-form text in a word processing document is a typical example. In unstructured content, there is no conceptual definition and no data type definition – for example, in textual documents, a word is simply a word.

Database

In computing a database can be defined as a structured collection of records or data that is stored in a computer so that a program can consult it to answer queries. The records retrieved in answer to queries become information that can be used to make decisions. The computer program used to manage and query a database is known as a database management system (DBMS). The properties and design of database systems are included in the study of information science.

Data Management

Data management is the function of controlling the acquisition, analysis, storage, retrieval and distribution of data. Data management can involve protecting the physical security of data, ensuring back up and recovery procedures are in place, protecting confidential or private information in data, reducing redundancy in data, and establishing an enterprise data architecture.

Information Technology (IT)

IT (information technology) is a term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia, and other forms, including those not yet conceived). It's a convenient term for including both telephony and computer technology in the same word. It is the technology that is driving what has often been called "the information revolution."

Infrastructure

The basic framework of an organization or operation. Infrastructure components are units of technology (hardware, software, networks, platforms, etc.) that support the flow and processing of information, determine how it functions and how flexible it is to meet future requirements.

Log Files

Where logging refers to the action of tracking modifications or activity of a user or application within a computing system, three broad log categories have been defined in this document: (1) system operational and other automated logs, (2) application access logs (that is, logs written by an application to record events and activities occurring within the application itself), and (3) employee internet use logs. A log can serve at least two purposes: (1) to record general system or application events, or (2) to serve as an audit

record for activity in an electronic system, including records of access or updates to system resources (access to the internet, access and updates to files and updates to security rules).

Metadata

In general, metadata is "data about data" and describes the structure, data elements, interrelationships and other characteristics of electronic information. When describing structured data (such as that in a data warehouse), metadata includes how, when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses. When describing unstructured data (such as e-mail, web pages, reports, etc.) metadata describes the context, content, and structure of the electronic records. Metadata can be used in the management of records to track message origin and destination, date/time sent/received, sender's identity, addressee(s) identity, subject, attachments and return receipts, among other things.

Methodology

A detailed and structured approach, containing generic and tool related step-by-step guidelines, to developing, upgrading, improving or replacing application systems. Sometimes also called a "blueprint."

Migration

The process of moving data from one information system or storage medium to another to ensure continued access to the information as the system or medium becomes obsolete or degrades over time. The act of moving records from one system to another while maintaining authenticity, integrity, reliability, and usability.

Network

In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub-networks.

Policies

A policy is a formal set of statements that define operating rules within the enterprise. Policies are established as a means of maintaining order, security, consistency, or other ways of successfully furthering a goal or mission.

Project Management

The formalized process of managing a large project. Project management is the planning, scheduling, and controlling of project activities to effectively and efficiently reach a major goal, such as developing a program or building a facility.

Resource Management System (RMS)

The RMS software and hardware provides the infrastructure needed to perform problem, change and IT inventory management for the State of Wisconsin executive branch agencies.

Security

Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the

oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized external access and from internal misuse. Security must be balanced against the need for access and the rights of citizens to privacy.

Security Forensics

Security forensics means use computer technology to investigate and establish facts in criminal or civil courts of law. As computer crimes increase, the demand for forensics understanding of systems and/or systems security breaches is needed. Evidence collection and investigation procedures in the digital world are much different than in the "real world."

Server

Server has several related meanings. In information technology, a server (also called a server application) is "an application program that accepts connections in order to service requests by sending back responses." Server is an adjective in the term server operating system. A server operating system is intended, enabled, or better able to run server applications.

Standard

Standards are a set of criteria (some of which may be mandatory), voluntary guidelines and best practices. The word standard can also be used to mean commonly accepted.

Structured Data (see Data)

System

A set of elements so connected or related as to perform a unique function not performable by the elements alone (Rechtin 1991). A system takes into account the interdependence of people and events, actions and conditions and institutions and organizations. A systems approach takes into consideration various "production lines" of related tasks and procedures (operating system, decision-making system, financial system, administrative system) to perform certain functions.

Systems Management

Systems management is the management of the information technology systems in an enterprise. This includes purchasing of equipment and software, distributing it to where it is to be used, configuring it, maintaining it with enhancement and service updates, setting up problem-handling processes, and determining whether objectives are being met.

Technology

Tools or tool systems by which we transform parts of our environment and extend our human capabilities (Tornatzky and Fleischer 1990).

Unstructured Data (see Data)

Version Control

Version Control is the process of controlling, maintaining, and documenting maintenance and updates to programs, data, and other electronic assets. Version control systems help define the constraints on how a resource can be updated and keeps historically accurate and retrievable logs of a file's revisions.

Workflow

A term used to describe the tasks, procedural steps, organizations or people involved, required input and output information, and tools needed for each step in a business process.

FOR ADDITIONAL INFORMATION AND ASSISTANCE

Agency personnel should also consult with the following resource staff for additional information and assistance with records management concerns.

Records Officer: Each agency has a designated records officer who serves as liaison to the Public Records Board. The records officer is responsible for agency-wide records management planning, program development, and assistance.

DOA Records Management Section: The DOA Records Management Section provides free training sessions, as needed, on implementation of general records schedules. Further information regarding both training sessions and records management can be accessed at the [State Records Center website](#).

Public Records Board: The board's Executive Secretary can offer technical assistance and training to assist agencies with records management, including records scheduling and interpretation of schedules.

Archival Repositories: For some records series that have been appraised to have archival value, the disposition will indicate 'transfer to an archival repository.' An archival repository is responsible for processing the records, making them available to researchers, and providing for their safe-keeping and preservation. An official archival repository is one that has been reviewed and designated as such by the Wisconsin Public Records Board according to Wis Stats. 16.61(13)(b). In general, transferring to an archival repository means transferring records to either the Wisconsin Historical Society (State Archives) or the University of Wisconsin Madison Archives:

Wisconsin Historical Society: The Wisconsin Historical Society (WHS) assists agencies with records management, particularly in identifying the small percentage of records that have historical value.

University of Wisconsin Institution Archives: University of Wisconsin Institutions have delegated authority to operate archives for historical institutional records. Often, the University of Wisconsin archives also function as the focus for records management related activities on the campus.

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000001	IT Strategic Plans	Agency IT Strategic Plans, IT services plans, and related records used to plan for information systems development, technology acquisitions, IT services provision, or related areas. This category includes final plans within agencies as well as the agency wide plan submitted to the Department of Administration.	Retain master copy of plan and essential background documentation for 6 years after (event) the plan is completed, superseded, or revised, and transfer to the appropriate archival repository (Wisconsin Historical Society (State Archives) or the University of Wisconsin Madison Archives) Destroy copies, drafts, and routine material when no longer needed by agency.	<p>Planning records often have value for budgetary and planning purposes for a number of years or planning cycles after they become inactive. The state has a two-year planning cycle and information from prior plans may be relevant for 3 planning cycles.</p> <p>Examples: Trend Analysis, Auditing</p> <p>Reference: Agency Annual Strategic IT Plan, 16.971 (L) and s. 16.976</p> <p>Agency Annual Strategic IT Plan – Biennial Supplement 16.971 (Lm)</p>
IT000002	IT Policies and Standards	Records of IT policies, standards and procedures which may include those covering access and security, systems development, data retention and disposition, data ownership, and administrative operating practices and procedures.	Retain 7 years after (event) policy/standard is withdrawn, revised, updated, or superseded, and transfer to the appropriate archival repository (Wisconsin Historical Society (State Archives) or the University of Wisconsin Madison Archives)	<p>Policies may be needed for reference and management audit purposes for a number of years after they are no longer in force.</p> <p>Examples: Employment actions</p> <p>Use as templates for similar policies</p>
IT000003	IT Management Reports and Metrics	Reports and metrics shared outside the IT organization which may include staff and contractor reports, external surveys, trend reports, focus groups, and critical performance indicators.	Destroy 7 years after (event) document distribution.	<p>Examples: Business or citizen surveys</p> <p>Availability Reports, Capacity Reporting</p>
IT000004	IT Steering/Policy Committee Documentation	Minutes and associated documents of IT Steering or Policy Committee meetings. These often document official actions of the committee on policy	Retain 3 years after (event) minutes are published and transfer to the appropriate archival repository (Wisconsin Historical Society (State	<p>For an agency, this would apply to only the top level IT steering group within that agency.</p> <p>Agency oversight or enterprise</p>

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
		recommendations, IT investment decisions, and other general IT business of the agency.	Archives) or the University of Wisconsin Madison Archives).	oversight, like DOT's ITOC, TLC, the old Business Leadership Council, Enterprise Steering Team.
IT000005	IT Topical Committee Documentation	Agendas, notices, minutes and relevant supporting materials of IT committees that set or revise policy through decision making. Committees may be ongoing or ad hoc.	Destroy 3 years after (event) distribution.	These groups are more topical in nature, like WEAT, old Domains, Security (ISAS), GIS Committee, directory working group. Project working committees that keep minutes would follow the project RDA, IT000009.
IT000006	Fiscal Year Planning Documents for IT Activity Levels	Operational fiscal planning records which may be related to departmental, cross-departmental or external, used for a variety of reasons related to provision of services. These records may contain information about specific infrastructure projects planned for the next fiscal year that may impact the organization, including information about enterprise-wide projects.	Destroy 4 fiscal years after (event) ending date of planning cycle. "This is in compliance with the Federal Office of Budget and Management Common Rule for Uniform Administrative Requirements for Grants and Cooperative Agreements with State and Local Governments" and Part 42 Retention and Access Requirements for Records, page 81 of the Federal Register Volume 53, No. 48.	Agency or enterprise fiscal IT Plans for the provision of IT services within an agency or the enterprise. Examples: Service Level Agreements (SLA); Memorandums of Understanding (MOU); Agency Fiscal Year IT Budget; IT Rate Schedule; estimating and documenting levels of ongoing maintenance and support; costs associated with various facets of program operation and support
IT000007	Performance Measures	Annual accomplishments for technical, application and production sections of an IT organization.	Destroy 6 years after (event) document distribution.	Examples: Projects completed, technical load reports (volume of processing reports), availability reports. Reference: Performance measures from agencies are required in Chapter 16.973, Sub 7.
IT000008	IT Project Investment and Development	Project records involved with the decision-making and approval	Destroy 3 years after (event) the system/infrastructure is	Investment process tracking

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
	Documentation	process to proceed with IT projects and technology selection.	retired. Note: These may be generated by different groups of people and kept in multiple places but it is recommended that a master project file be kept in one place.	Examples: IBIS, RATS, E-mail, Release Versions Records may include project proposal, project charter, cost benefit narrative, cost benefit spreadsheet, risk analysis, scope change, executive summary, project milestone reports, and others produced for the project: <ul style="list-style-type: none"> • project management records • management status reports • final business requirements • final project and subsystem specifications • project close-out or post-mortem documentation • correspondence • documents reflecting official approval of projects or project planning decisions
IT000009	Project Files	Project files created and used in the development, redesign, or modification of an automated system or application.	Destroy 5 years after (event) project completion or abandonment. Note: Records may be needed up to 5 years after the conclusion of a project for reference or for management audit purposes. In some circumstances, agencies may wish to maintain these files longer for reference. All relevant information and final documentation should be contained in system and application documentation files.	Records may include project proposal, project charter, cost benefit narrative, cost benefit spreadsheet, risk analysis, scope change, executive summary, project milestone reports, and others produced for the project: <ul style="list-style-type: none"> • project management records • management status reports • final business requirements • final project and subsystem specifications • project close-out or post-mortem documentation • correspondence • documents reflecting official approval of projects or project planning decisions Examples:

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
				<p>Network plan and implementation files which may include reports, justifications, working diagrams of proposed network, wiring schematics, and diagrams.</p> <p>Telecom project documentation. Records created and used in the development, redesign, or modification of a telecom project.</p>
IT000010	Systems Specifications Documentation	User and operational documentation describing how an application system operates from a functional user and IT point of view.	<p>Destroy 3 years after (event) major upgrade or discontinuance of system, but not before system data is destroyed or transferred to new operating environment.</p> <p>Current and accurate information on how an application system operates is needed throughout its life cycle. System documentation may be needed 3 years after the system is discontinued or modified for the admissibility of electronic records in legal proceedings, retrospective analysis, and remedying errors.</p>	<p>Procedures for entry of system operational parameters, system administration, hours of system operation, production control, and other aspects of an IT operation.</p> <p>Examples:</p> <p>System administration operation procedures; Tape library procedures; Installation procedures; Backup procedures.</p> <p>Tape Control Library: Procedures used to control the location, maintenance, and disposition of magnetic media in a tape library.</p> <p>Records may include:</p> <ul style="list-style-type: none"> • records documenting data entry, manipulation, output and retrieval (often called "system documentation records") • records necessary for using the system

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
				<ul style="list-style-type: none"> • user guides, system or sub-system definitions • system and program flowcharts • program descriptions and documentation (or other metadata) • job control or workflow records • system specifications • system change notices scripts • input and output specifications
IT000011	Source Code	Source code which is used to construct and operate an automated information system. Change orders to source code need to be retained.	Destroy 3 years after (event) code is superseded or replaced.	<p>Instructions used to operate a system or infrastructure. After the code is modified or replaced it has no administrative or legal value. Proprietary, vendor-supplied code follows individual license agreements for retention.</p> <p>Examples: Source code audits; ITIL Release Management function and auditing application program changes; Post conversion troubleshooting</p>
IT000012	IT Operating Procedures	<p>Procedures for entry of system operational parameters, system administration, hours of system operation, production control, and other aspects of an IT operation.</p> <p>Note: this may include vendor and/or manufacturer documentation.</p>	Destroy 3 years after (event) procedure is withdrawn, revised, updated, or superseded.	<p>Basis for subsequent operational procedures.</p> <p>Examples: System administration operation procedures; Tape library procedures; Installation procedures; Backup procedures.</p>

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000012A	IT Operating Procedures - Critical Information Systems	<p>Procedures for entry of system operational parameters, system administration, hours of system operation, production control, and other aspects of an IT operation.</p> <p>Note: this may include vendor and/or manufacturer documentation.</p>	<p>Destroy 7 years after (event) procedure is withdrawn, revised, updated, or superseded.</p> <p>Note: Operating procedures must be retained and accessible as long as they are in force. Outdated procedures for critical information systems may be necessary for reference and management audit purposes for up to 7 years after they are no longer used for active administration.</p>	<p>Examples: System administration operation procedures; Tape library procedures; Installation procedures; Backup procedures.</p> <p>ETF Annuity System</p>
IT000013	IT Software/Hardware Infrastructure Documentation	<p>Use, operation, and maintenance of an agency's IT equipment.</p> <p>Note: this may include vendor and/or manufacturer documentation.</p>	<p>Destroy 1 year or after (event) the agency no longer uses related software/hardware and all data is transferred to and made useable in new software/hardware environment.</p>	<p>Records may include:</p> <ul style="list-style-type: none"> • operating manuals • hardware/operating system requirements • hardware configurations equipment control systems <p>These need to be kept as long as the software/hardware is being used.</p>
IT000014	Operating System and Hardware Migration Plans	<p>Migration plans and documentation for the replacement of equipment or computer operating systems. (Version changes, not release changes)</p>	<p>Destroy 3 years after (event) major upgrade or discontinuance of system, but not before system data is destroyed or transferred to new operating environment.</p>	<p>Planning for subsequent migrations. (Release version documentation would be covered under IT000008.)</p> <p>Major Systems Examples: OS2 to NT NT to 2000, 2003 OS390 to ZOS Sun to I Series</p> <p>Plans may be needed for a longer period of time for critical information systems,</p>

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
				migration planning, or after migrations for reference and to deal with unforeseen issues and problems.
IT000015	Disaster Preparedness and Recovery Plans	Plans and documentation for the protection and reestablishment of IT services and equipment in case of a disaster. NOTE: This record set may be classified as confidential.	Destroy after (event) superseded by revised plan.	Examples: Living Disaster Recovery and Planning System (LDRPS) version of IT documents IT COOP documentation
IT000016	IT Service Support Documentation	Files document support service provided for servers, networks, and personal computing equipment. Note: this may include vendor and/or manufacturer documentation.	Destroy 2 years after closure/completion	Documentation of requests for technical assistance and responses to these requests, as well as to collect information or report on the use of computer equipment for program delivery, security, or other purposes such as trend analysis. Examples: Site visit reports; Trouble reports; Related correspondence and memoranda

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000017	Technology Selection Documentation	Research, analysis, review and recommendation records regarding selected software/hardware for agency use, including vendor information and related material.	<p>Minimum Retention: Purchasing and Procurement GS 90112, Request for Bid Proposal, EVT (procurement) plus 4 years.</p> <p>Destroy after (event) the technology is no longer used by agency.</p> <p>"This is in compliance with the Federal Office of Budget and Management Common Rule for Uniform Administrative Requirements for Grants and Cooperative Agreements with State and Local Governments" and Part 42 Retention and Access Requirements for Records, page 81 of the Federal Register Volume 53, No. 48.</p>	<p>Subsequent Procurements Contested Procurements Open Records Requests LAB Audit Reviews</p> <p>Documentation and process used to choose technology to perform the functions.</p> <p>Examples: Comparison charts; Technology research organization reviews; Total Cost of Ownership comparisons; Trade press literature review; Bid & RFP evaluations; Requirements</p>
IT000018	Quality Control Files	Quality control/data input records that may be used to verify data entered into a production file or database system upon initial creation or when significantly modified through batch type operations.	<p>Destroy 4 fiscal years after (event) ending date of planning cycle.</p> <p>"This is in compliance with the Federal Office of Budget and Management Common Rule for Uniform Administrative Requirements for Grants and Cooperative Agreements with State and Local Governments" and Part 42 Retention and Access Requirements for Records, page 81 of the Federal Register Volume 53, No. 48.</p>	<p>Examples: LAB Audit Reviews; Release Management Documentation Test Procedures related to Release or Upgrade of Software or Application Code</p>

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000019	Data/Backup Library Control Files	Lists of holdings, control logs, and information on the destruction of files stored on electronic media in a library. NOTE: Does not include the data on the media.	Destroy after superseded.	Examples: Storage manager reports; Log files; TSM logs
IT000020	Network Support Service History and Summary	History and summary records related to the provision, quality, and availability of network support services.	Destroy 1 year after the close of contract or 5 years, which ever is greater. Note: The longer retention period is desired for audit purposes. It is assumed that the summary will contain summary information of IT000021 and IT000022, so these individual records would not need to be retained for as long of a period.	In general these network support services are provided by a third party vendor(service provider), and these documents are necessary in evaluating the quality of service, and assisting in the resolution of issues / trouble tickets with the service provider. Examples: AT&T outage report
IT000021	Inventories of Circuits	Network circuit inventories used by the agency, which may include circuit number, vendor, cost per month, type of connection, terminal series, software, contact person, and other relevant information about the circuit.	Destroy after superseded.	Examples: Agency reconciliation/cleanup process
IT000022	Network or Circuit Installation and Service Files	Requests by agencies to DOA or contracted service provider for data communication service, installation, or repair and response to the request.	Destroy 1 year after (event) request is filled or repairs are made.	Examples: Work orders; Correspondence / memoranda; Work schedules; Copies of building or circuitry diagrams; Network design documents Records should be retained 1 year for management analysis and planning.

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000023	Operational and Other Automated Logs	Logs created to monitor usage. The logs may include network or operating system logs (that are not security related). These are considered transitory.	Destroy when no longer needed.	<p>Network usage logs, performance management, troubleshooting or other network monitoring (modem pool logs, network flows generated by routers, DHCP logs, e-mail server logs, etc), and other records created to document computer usage for reporting or other purposes.</p> <p>Examples: System usage files</p> <p>Computer run logs and related records may include:</p> <ul style="list-style-type: none"> • daily schedules • run reports / requests • internally-generated program logs or any other automated logs that have limited business value to the agency • metadata • other records documenting the successful completion of a run
IT000024	Data Documentation / Metadata	<p>Data documentation (also known as metadata) that is generally created during development or modification of an automated system. Data necessary for the access, retrieval, manipulation and interpretation of data in an automated system may include the data element dictionary, file layout, codes, and other records that explain the meaning, purpose, structure, logical relationships, ownership, use and origin of data.</p> <p>In unstructured information,</p>	Destroy after (event) the application's data is destroyed or migrated to a new structure or format.	<p>These records are essential for managing electronic records in agency automated information systems that have been discontinued or modified and have value as long as the data/electronic records are retained. In some cases, agencies will retain data for extended periods of time, sometimes off-line. In such cases, it is essential that related documentation be retained in an accessible format.</p> <p>Used to validate the authenticity of the electronic record in the unstructured world.</p>

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
		metadata is similarly used to identify the context of the record.		
IT000025	Test Data	<p>This is data used for testing system functionality.</p> <p>NOTE: Loading data from a production system, obfuscating it, and using as test data does not create a new record.</p> <p>NOTE: This record set may be classified as confidential.</p>	Destroy when no longer needed.	Data sets, including copies of production data or sample structured or unstructured data sets, used for the purpose of validating an application's functionality. The data sets used for this purpose are not considered to be records.
IT000026	Application Access Logs	<p>Electronic files or automated logs created to monitor access and use of agency services.</p> <p>NOTE: This record set may be classified as confidential.</p>	Destroy 1 year after (event) log creation but not before relevant audit (federal, state, etc.) and documentation requirements have been met.	<p>Logs may relate to access of agency-provided services. They are needed for incident resolution, such as litigation and customer complaints.</p> <p>Examples: Agency Internet Services logs; Access and usage trends; Statistics; Internet and Intranet logs Web server logs File transfer logs Service access logs</p>
IT000027	Employee Internet Use Logs	<p>Electronic files or automated logs created to monitor and control use of the Internet by agency employees.</p> <p>NOTE: This record set may be classified as confidential.</p>	<p>Destroy 3 months after (event) log creation unless required for security purposes.</p> <p>While a one-year retention is likely to be desirable in order to respond to employee supervisory issues, a shorter-term retention period is acceptable for internet usage logs because they create a large volume of records for the</p>	<p>Logs may relate to employment actions and performance management.</p> <p>Examples: Proxy server logs and web filtering, such as Web Sense and Surf Control.</p>

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
			business value received. Often data extraction is difficult due to the disarranged data format and the large volume of data generated.	
IT000028	Website Usage Reports	Reports of web usage retained for trend analysis and customer service performance or related usage tracking data.	Destroy after superseded.	Examples: Web trends
IT000029	State Telephone System Call Detail	Documentation created for functions associated with the state telephone system call detail.	Destroy 5 years after creation	Examples: Phone bill details – local usage detail (LUD)
IT000030	Telecom Inventory Support	Support documentation for telecommunication equipment and phones wires and circuits and applications.	Destroy after superseded. Note if there is not a summary report as in IT000020 these records will need the following, "Destroy 4 fiscal years after (event) ending date of planning cycle.	This includes billing account information, telecommunication service inventory, current call flows, system configurations, user guides and instructions, support manuals, cross-connection information, binding post information, backup procedures.
IT000031	Telecom Maintenance Work Order Files and Logs	Users change/trouble requests, internal service order documentation, service order submitted to vendor, and maintenance and order logs.	Destroy 1 year after (event) close of contract. Note if there is not a summary report as in IT000020 these records will need the following, "Destroy 4 fiscal years after (event) ending date of planning cycle.	Examples: Reports of routine phone/phone line repairs done by vendor. Work orders submitted to the vendor.
IT000032	User Access Requests and Authorizations	Records may include but are not limited to local and remote access and authorized logon id. NOTE: This record set may be classified as confidential.	Destroy 2 years after (event) departure of employee. Needed per LAB annual IT Security Audits, the current schedule calls for audit this information every other year, so it needs to be retained for at	Records may be needed for audits, system security, summary reports, planning.

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
			least 2 years.	
IT000033	Employee Responsibility Acknowledgement Agreements, Trusted Use Agreements	Employee acknowledgement of security-related responsibilities and trusted use agreements. NOTE: This record set may be classified as confidential.	Destroy 3 years after (event) departure of employee, contractor or vendor If records are placed in the employee personnel file, the retention period would follow PERS124 (8 years after termination).	Records may be needed for employment actions. Examples: Data confidentiality forms; Employee password security agreements; Dates of such acknowledgement
IT000034	Assignment and Authorization of Security Officer and Personnel with Administrator Privileges	Records may include the appointment, authorization, and approval from the agency head or delegated authority to the requesting agency's or the enterprise IT security officer and who had administrative access privileges to applications. NOTE: This record set may be classified as confidential.	Destroy 4 years after (event) departure of security officer or personnel granted administrative privileges or (event) revocation of such privileges. Per LAB audit needs and OBM Circular A-102.	Examples: Appointment, authorization or approval from the agency head or delegated authority to the requesting agency's or the enterprise IT security officer; Documentation of who had administrative access privileges to applications.
IT000035	Security Reports	Reports of security activities related to IT systems (e.g. applications, system software and hardware) network, employees, and others who may access IT related resources (e.g. general public, business partners). NOTE: This record set may be classified as confidential.	Destroy 5 years after creation, unless there are longer retention times specified by a federal program, federal Office of Budget Management (OMB) circular, or federal statutory language. Per LAB audit needs and OBM Circular A-102.	These reports may be retained for trend analysis and customer service performance or related usage tracking data for employment actions. Examples: Daily events; Restricted Logon ID log; Info-storage violations; Info-storage log; Data set traces; Logging and violations; Mainframe by-pass label processing; Resource tracing; Violation for all platforms and

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
				applications.
Other Relevant General Records Schedules				
9000021 Fiscal & Acct.	Computer Services Billing Records	Reports and other records from DET-DOA, detailing charges for use of computer services which may include monthly billing reports, copies of vouchers and bills.	Destroy after the current fiscal year plus 6 back fiscal years.	
9000021 Fiscal & Acct.	Records of Charge-backs to IT Service Users	Records used to document, calculate costs and bill program units for computer usage and IT services. These records are also used for cost recovery, budgeting, or administrative purposes.	Destroy after the current fiscal year plus 6 back fiscal years.	
90115 Purchasing & Procurement	Purchase Requisitions, Orders, and Billing Records for IT Services	Records used to document, calculate costs and bill program units for computer usage and IT services. These records are also used for cost recovery, budgeting, or administrative purposes.	Destroy 4 years after close of contract. Purchase records are usually maintained together in Contract Case File.	Copies of records created to initiate the purchasing process, authorize and provide funds for, or satisfy claims and expedite payments for private service providers including copies of purchase orders, invoice requests, receipts, agency vouchers, service reports, and other supporting documentation. Financial-related records must be retained FIS+6 years per Fiscal and Accounting General Schedule RDA#9000021
90115 Purchasing & Procurement	Maintenance Contracts Files	Maintenance contracts for IT equipment and related records including copies of contracts, service histories, and work orders.	Destroy 4 years after close of contract. Maintenance records are usually maintained together in Contract Case File.	
90129 Purchasing &	IT Product/Vendor and State Contracts	Information on IT equipment, software, and other products and	Destroy 4 years after date of warranty expiration or decision	Service/Product Warranty Case Files

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
Procurement	Reference Files	their vendors.	made that product is no longer required.	Records Not Covered: Master copies of State contracts are retained by each agency's central procurement office-see Procurement General Schedule RDA#90115.
Purchasing & Procurement	IT Procurement Files	Records used in the procurement of system hardware and software including request for proposals, proposals, quotations and bids, benchmark/acceptance testing information, correspondence, duplicate copies of contracts, purchase orders, technical reviews, and vendor information including references and literature on the firm or product line.	<p>RDA#90109 Encumbrances (Purchase Orders for Goods and Services) FIS+4 years and destroy</p> <p>RDA#90111 Request for Purchasing Approval/Authority (RPA) Evt+4 years and destroy</p> <p>RDA#90112 Request for Bid/Proposal (RFB/RFP) File EVT+4 years and destroy</p> <p>RDA#90114 Contract Case File EVT+4 years and destroy</p>	IT units may maintain key contract-related documents needed for litigation. These records must be retained 6 years after expiration of the contract to satisfy the statute of limitations on contract related litigation. Records not related to a contract may be needed for up to 3 years after the purchase for reference or audit.

Appendix 1: Summary of Approved Statewide General Records Schedules

Purchasing and Procurement General Records Schedule, April 2003

RDA #90100-90135

Covers all purchasing related records including purchase orders, bids, contracts, case files, and various reports that are required by the State Bureau of Procurement.

Covers all state agencies including UW System Administration and UW institutions.

Payroll and Related Records, Revised 2nd Edition, November, 1997

RDA #90200-90217

Includes DOA Central Payroll data, and payroll related records such as leave accounting records, pay adjustment records, and pay withholding authorizations for tax and benefit purposes.

Does not include UW System Administration and UW institutions that are not directly tied to DOA payroll, However UW System Administration has developed it's own general records schedule for payroll related records at UW Madison and all other UW institutions.

Worker's Compensation and Related Records, Revised July 1997

RDA #90300-90311

Includes all related records such as near miss reports, Workers Compensation claim files, and incident reports.

Covers all state agencies including UW System Administration and UW institutions.

Data Security and Related Records, July 2001

NOTE: This General Schedule has been superseded by the IT General Schedule and is closed as of August, 2007.

Includes all records related to security associated with access to computer related resources. Records include access control, completed confidentiality forms, logon requests, ACF2 Security Handbook, and security reports.

Common Records in Wisconsin State Agencies and Local Units of Government, May 2002

RDA #90500000-90500006

Includes common records in the following areas: routine activity/production reports for individuals; organizing tools; and routine materials such as transitory files and mailing address lists.

This schedule applies to all state agencies and UW institutions. It also applies to all local units of government.

Motor Vehicle Management Records, May 1999

RDA Fleet 001-014

Includes motor vehicle related subject files; project files and correspondence files. Also includes records related programs such as ride sharing and the state vanpool program. Also includes all records related to vehicle acquisition and disposition, maintenance, assignment and utilization and motor vehicle incident/accident reports.

Personnel and Related Records, July 1999

Includes over 140 types of personnel related records broken down into specific personnel related functions. Covers records at the Department of Employee Relations (now called Office of State Employment Relations), agency central human resources (personnel) departments and records maintained by supervisors related to personnel functions.

Budget and Related Records, March 2002

Includes 41 types of operating budget related records. Does not include the capital budget related records. A separate schedule is being developed for these records

Fiscal and Accounting Related Records

Forms Management Related Records

Library Operations and Related Records

Mail and Messenger Services and Related Records

Records Management Program Records and Related Documents

General schedules are listed as a major category on the [Public Records Board's Home Page](#).

If you need further assistance, contact your agency records officer or the DOA Records Management Section at 266-2996 or 266-2770.

Appendix 2: Agency Agreement to Use General Schedule-New Policies and Procedures

Currently when the Public Records Board (PRB) approves a general records schedule the implementation by each state agency is assumed. This new policy, effective March 1, 2006 requires an affirmative act on the part of agencies to adopt for their internal use General Records Schedules (GRS) approved by the Board.

Policy Statement

General records retention schedules, GRS, are a mechanism for systematic retention and disposition of similar types of records across State government. GRS's eliminate the necessity for agencies to develop and seek approval of their own retention schedules. They lend consistency to record keeping across state government and provide assurance of accountability to the public. The PRB supported the development of and approved several GRS in several functional areas. This policy statement outlines a process that State agencies must use to adopt for their internal use any GRS approved by the PRB.

Any state agency (including UW System Administration and all UW campuses) may adopt any or all of the authorizations in any general schedules approved by the PRB and identified for use by state agencies provided the agency head or deputy and agency records officer notifies the Board in writing of the intent to use the schedule. Adopting a Board approved GRS means that the agency agrees to implement the retention and disposition recommendations noted for each records series in the particular GRS. State agencies must choose one of the following options with regard to the adoption of GRS's:

- 1- **Opt in** Agreeing to opt in means the state agency agrees to use the recommendations noted in the GRS for its records.
- 2- **Opt in with revisions** State agencies choosing this alternative would agree to the recommendations of the GRS, but they will submit to the PRB a list of records series with retention and disposition recommendations that vary from the GRS. It is recognized that State agencies may have in some areas the need to retain items for a different period of time than that recommended by the GRS.
- 3- **Opt out** If a State agency opts out of adopting a GRS, it must then within six months in accordance with Wis. Stat.16.61 provide specific retention schedules for any record it maintains in the functional area covered by the GRS.

State agencies should be aware that current law (Wis. Stat. 16.61) requires authorization of the Board to destroy any state agency records. Therefore if a state agency chooses to opt out entirely or partially of any existing general schedule, they may not destroy any records until separate records disposition authorizations (RDA's) are prepared by the state agency and approved by the Board.

Implementing General Records Schedules

After adoption and notification, state agencies may use the identified general schedule for any applicable records in its custody. This means that following notification, records may be disposed on a continuing basis, provided that the minimum retention time period identified in the schedule has been met. If a general schedule identifies a record series with a disposition of transfer to an archival repository, those records must be offered to the archival repository rather than being destroyed. Disposal or transfer of records is contingent on record destruction restrictions contained in Wis. Stat. 19.35 (5) (Open Records Law). No records may be destroyed if litigation or audit involving these records has commenced.

State agencies may discontinue the use of all or portions of any general schedule, but the agency records officer must first notify the Board of the discontinuance. When an agency discontinues use of a general schedule (in whole or part), the records controlled by the applicable record series may no longer be destroyed or transferred until separate records disposal authorizations are prepared by the state agency and approved by the Board.

Discussion

The Board is implementing this new requirement to strengthen state agency compliance with records retention law and to increase efficiency in state records management. The requirement will be implemented on a “day forward” basis as the Board approves either new or updates to existing general schedules.

An approval form will be issued along with each approved general schedule. The form will identify the functional area (for example Fiscal and Accounting; Personnel; Information Technology) covered by the general schedule and have check boxes for the agency to affirm their intent to opt in to the entire general schedule, opt in with revisions or opt out all together. The form will have signature blocks for the Agency Head, Agency Records Officer, Board Executive Secretary and the State Archivist.

Agencies should not opt out of a GRS because your agency does not create or use all the types of records contained in a schedule. Agreeing to follow the record retention and disposition requirements within a GRS does not obligate an agency to create records. It only requires that records be retained in accordance with the retention time periods and dispositions if such records exist.

Since the general schedule contains the minimum time periods, the most likely reason that an agency will not use the time periods is because they have a business need to keep the records longer. The Public Records Board will not approve retention time periods in separately submitted record schedules shorter than those contained in the general schedule.

If a record series in a general schedule is identified as having potential historical value, that determination stays with that record series if an agency chooses not to adopt the general schedule. This means that if an agency proposes a separate schedule they should assume that the disposition for the series will be transfer to an archival repository, rather than destroy.

Agency compliance with records retention requirements is existing state law. Therefore agencies that choose to opt out of all or parts of a general schedule may not destroy any records that are controlled by these record series until the agency has prepared separate records disposal authorizations which are then approved by the Public Records Board.

For More Information Contact:

Harold Coltharp, Executive Secretary
Public Records Board
608 266-2770
harold.coltharp@wisconsin.gov
September 1, 2007

Notification of General Records Schedule Adoption

Schedule Title: _____ Date: _____

Instructions:

Complete and send the original and 2 copies to: State Archivist, Wisconsin Historical Society (WHS), 816 State St., Madison, WI 53706.

- Do not opt out of a record series because your agency does not create or use these types of records. Signing the form does not obligate an agency to create records. It only requires that records be retained in accordance with the retention time periods and dispositions if such records exist.
- Please attach a brief narrative explaining your rationale for opting out of each record series. Examples: Increased retention needed for business purpose, or federal or state regulation requires longer retention. When a separate schedule is prepared, identify that the record series is in lieu of the general schedule and cross reference the specific series.

NOTE: Destruction or transfer of records is not permitted until this form is signed by the WHS and the Public Records Board.

State Agency: _____

Address: _____

This is to notify the Wisconsin Historical Society and the Public Records Board that the state agency named above has reviewed the general records schedule.

Check appropriate box(es):

- The State Agency adopts the entire schedule.
- The State Agency opts out of the entire schedule.
(All applicable records disposition must cease until separate RDAs are developed and approved by the Public Records Board.) Please attach a brief narrative explaining your rationale.
- The State Agency opts out of the following record series.
Please list, identifying the specific RDA numbers and titles:

In those areas not covered, all records disposition will cease until separate RDAs are developed and approved.

Agency Head/Deputy Signature	Date Signed
Agency Records Officer Signature	Date Signed

The Public Records Board and Wisconsin Historical Society acknowledge your Notification of Adoption. You are hereby authorized to retain, transfer, and dispose of records as indicated on the schedule.

State Archivist Signature	Date Signed
PRB Executive Secretary Signature	Date Signed