General Records Schedule

Information Technology and Related Records

Approved by the Public Records Board:

November 10, 2014

Revised: November 16, 2015

Expiration: November 10, 2024

For use by all units of Wisconsin Government at the State, County, and Municipal level

SCOPE

This schedule governs the records retention obligations of state agencies pursuant to Wis. Stat. § 16.61, and applies to "public records" as defined in Wis. Stat. § 16.61(2)(b). These "public records" are referred to as "records" in this schedule.

This schedule covers records that most state agencies, including the University of Wisconsin System Administration, the University of Wisconsin Institutions, all Wisconsin counties, municipalities and other units of local government create and use in conducting information technology (IT) business or administered by decentralized IT staff located in agency program organizations. This schedule is applicable to all IT records regardless of format or media.

This general schedule may *not* include records that are unique to the mission of a single government unit. Records that are unique to the mission of a specific government unit require a separate Records Disposition Authorization (RDA). The department or institution is responsible for creating a RDA that must be submitted to, and approved by, the Public Records Board (PRB).

See the Introduction to General Records Schedules for additional information about how to use this schedule. In particular please review the restrictions on conditions that might preclude the authorized destruction of documents in the normal course of business including open records requests; ongoing legal holds or audits currently underway or known to be planned.

This schedule goes into effect upon final approval by the Public Records Board.

INTENTIONAL OMISSIONS

Automated Applications
IT holds records and facilitates data processing and the web presentation of business records 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 and processed by, and output from, computer applications belongs to programs and must be scheduled by the program. IT may facilitate the retention and disposition of that data as documented in the program RDA.
- **Web Content/Social Media**
  This GRS does not address business records presented on the internet/intranet or in social media. Subject matter experts (i.e., program or business area staff) are the content owners and have the responsibility for scheduling and retaining those records to meet the program business needs.

Backup Processes
A “backup” process refers to making copies of original data so the copies are available for a restore 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 files that 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 backups must be scheduled for the longest retention period of any information carried on the medium. Retained backups may be subject to discovery or open records requests.

RECORDS FORMAT

Records covered in this schedule may be in paper, electronic, or other formats. Electronic format examples include those created or transmitted via e-mail, data contained in database systems, and tapes/cartridges. To safeguard the information contained in records maintained *exclusively* in electronic format, agencies must meet the standards and requirements for the management of electronic records outlined in Wis. Admin. Code ch. Admin 12.

PERSONALLY IDENTIFIABLE INFORMATION

Wisconsin law requires authorities to specifically identify certain record series within a general records schedule that contain Personally Identifiable Information (PII). Wisconsin Stat. § 19.62(5) defines PII broadly as “information that can be associated with a particular individual through one or more identifiers or other information or circumstances.” Despite this broad definition, Wis. Stat. § 16.61(3)(u)2.a.-f. provides that record series within a schedule containing the following types of PII need not be identified as such: a) the results of certain computer matching programs; b) mailing lists; c) telephone or e-mail directories; d) record series pertaining exclusively to agency employees; e) record series that contains PII incidental to the primary purpose for which the records series was created; and f) those relating to state agency procurement or budgeting. If in doubt as to whether a specific record series contains PII, check with your agency legal counsel.

Information about identity theft and information security is available at http://itsecurity.wi.gov/.

CONFIDENTIALITY OF RECORDS

Most records are not confidential and are open to public disclosure; however, there are exceptions. This GRS will identify any record series that may contain information required by law to be kept confidential or specifically required to be protected from public access, identifying the state or federal statute, administrative rule, or other legal authority that so requires. If in doubt as to whether or not a specific record, or content in that record, is confidential, check with your agency legal counsel. A record series should be identified as

confidential even if not all records in the series contain confidential information, and not all parts of records covered by the series are confidential.

SUPERSEDED RECORD SERIES

“Superseded” means that a new record series or RDA number has been used to cover records that were previously identified differently. The The “Superseded” section provides a cross walk between new and any superseded RDA numbers. When revising a GRS, an attempt is made to retain the previous RDA number, providing the underlying records remain the same.

CLOSED RECORD SERIES

When revising a GRS it is common for some previously included record series to be closed. The “Closed Series” section lists series containing records that are no longer created, nor are they expected to be in the future. See the “Closed Series” section included in this document.

RELATED RECORDS

The “Related Records Series” section provides information on other record series in approved GRSs which may relate to the broader functional area of this GRS. These record series are listed to facilitate a more complete understanding of all the record series within the broad scope of this function of government. It may not however contain a complete listing of all records series used within your agency for these types of business records. See the “Related Records Series” section included in this document.

REVISION HISTORY

See the “Revision History” section for a listing of changes to this GRS.

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT000001	**IT Strategic Plans**	Records include 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. Typically the agency submits annual plan and DOA submits biennial plan.	No	No	EVT + 6 years and transfer to appropriate archival repository (Wisconsin Historical Society [State Archives] or the UW-Madison Archives). Destroy copies, drafts, and routine material when no longer needed by agency.	EVT is the plan is completed superseded or revised.	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 three planning cycles.** **Examples:** Trend Analysis, Auditing Final report and presentations (IT to Sr. Mgt) **Reference:** Wis. Stat. §§ 16.971(2)(L), 16.971(2)(Lm), and s. 16.976
IT000003	**IT Management Reports and Metrics**	Records include 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.	No	No	EVT + 4 years and then destroy.	Event is the date the document is distributed.	Business or citizen surveys Availability Reports, Capacity Reporting, Status reports Key Performance Indicator (KPI) Reports Service Level Agreement Reports (tie back to KPIs)
IT000006	**Fiscal Year Planning Documents for IT Activity Levels**	Records include operational fiscal planning records that may be related to departmental, cross-departmental or external projects, 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. Operational type records related to how many IT hours (and costs per hour) will be allocated and paid for by the operating divisions.	No	Yes, state building plans and specifications per Wis. Stat. § 19.36(9) and Wis. Stat. § 16.851	EVT + 4 fiscal years and destroy confidential. Retention is in compliance with Federal Office of Management and Budget.	Event is the ending date of planning cycle.	Agency or enterprise fiscal IT plans for the provision of IT services within an agency or the enterprise. **Examples:** 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 PRS rates and supporting documentation

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT00006A	**Data Sharing Agreements**	Records include formal data sharing agreements between state agencies, a state agency and a federal agency, or another private entity that governs the specific terms and conditions under which information (typically formatted digital information) collected by the state agency may be shared between the parties to the agreement. Such agreements are generally authorized by state or federal law, or administrative regulation, for a specific public purpose. Data sharing agreements are typically signed by the agency head or designee of both the sending and receiving agencies and may be either ongoing or established for a set period of time as identified in the agreement. State agencies that enter into data sharing agreements that specify computer matching must comply with the requirements of Wis. Stat. § 19.69.	No	No	EVT + 4 years and destroy.	Event is the date the agreement is either terminated or superseded.	**Examples:** Agreements to share tax information between the state Department of Revenue and Department of Employee Trust Funds Agreement between the lottery program administered in DOA and state and federal tax authorities to check for back taxes before payouts of certain high value winnings. **Note: Memorandums of Understanding (MOU) and Service Level Agreements (SLA) should be retained under ADM00029.**
IT000007	**Performance Measures**	Records include annual accomplishments for the technical, application and production sections of an IT operation.	No	No	EVT + 6 years and destroy.	Event is the date the document is distributed.	Prescribe and revise as necessary performance measures to ensure financial controls and accountability, optimal personnel utilization, and customer satisfaction for all information technology functions in the executive branch outside of the UW System and annually, no later than March 31, report to the joint committee on information policy and technology and the board concerning the performance measures utilized by the department and the actual performance of the department and the executive branch agencies measured against the

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
							performance measures then in effect. **Reference:** Wis. Stat. § 16.973(7)
IT000008	**IT Project Investment Documenta-tion**	Investment documentation records involved with the decision-making and approval process to proceed with IT projects and technology selection. **NOTE:** These may be generated by different groups of people and kept in multiple places but it is recommended that a master file be kept in one place.	No	No	EVT + 3 years and destroy.	Event is the date the system/infrastructure is retired, or the project is abandoned.	Pre-project proposals, cost benefit analysis, risk assessments, executive summary, sign-off and decision documents, fit/gap analysis for project work, progress rpts, plans and accomplishments, staffing, work breakdown schedule, budget, communication plan, change management plan, change management risk plan, support transition plan. **Examples:** STAR, Cherwell
IT000009	**IT Project Files**	Records include those pertaining to the development, redesign or modification of a computer system or application.	No	No	EVT + 5 years and destroy. **NOTES:** 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 info and final documentation should be	Event is the date project is completed or abandoned.	Change logs, data cleanup procedures and stats, code migration procedures, transition to production tasks, authorization setup, process scheduling, post-implementation review, project correspondence. Project charters to include scope, requirements, roles, timeline, budget, control strategies. **Examples:** Network plan and implementation files. Telecom project documentation. Website design records.

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
					contained in system and application documentation files.		
IT000010	**Systems Specs Documenta-tion and Quality Control Files**	Records include user and operational documentation describing how an application system operates from a functional user and IT point of view. 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. Data documentation (or 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.	Yes	Yes, may include information that is trade secret and cannot be disclosed pursuant to Wis. Stat. § 19.36(5) and § 134.90(1)(c); computer programs that cannot be disclosed pursuant to Wis. State. § 19.36(4); or other legally protected intellectual property (copyright, etc.); follow any agency-specific statutory citations	EVT + 4 years and destroy confidential. Current and accurate information on how an application system operates is needed throughout it's life cycle. System documentation may be needed 4 years after the system is discontinued or modified for the admissibility of electronic records in legal proceedings, retrospective analysis, and remedying errors.	Event is defined as a major upgrade or discontinued use of system, but not before system data is destroyed or transferred to new operating environment.	Procedures for operations and support of a user application. Workflow diagrams, data definitions, data conversion mappings, naming standards, architecture diagrams, and file designs. Test plans including processing test results, accessibility compliance results, web usability tests and results; data conversion results. **Examples:** System administration and security IT operation procedures User manuals and guides Data documentation/ metadata LAB audit reviews Release mgt documentation Test procedures related to release/upgrade of soft-ware or application code Data element dictionary, file layout, codes and other records that explain meaning, purpose, structure, logical relationships, ownership, use and origin of data. System and program flowcharts; program descriptions and documentation; job control or workflow records; records

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
							disposition process; input and output specifications; records used to validate the authenticity of the electronic record in the unstructured world.
IT000011	**Source Code**	Records include source code that is used to construct and operate an automated information system. Series includes change orders to source code.	Yes	Yes, may include information that is trade secret and cannot be disclosed pursuant to Wis. Stat. § 19.36(5) and § 134.90(1)(c); computer programs that cannot be disclosed pursuant to Wis. State. § 19.36(4); or other legally protected intellectual property (copyright, etc.); follow any agency-specific statutory citations	EVT + 3 years and destroy confidential.	Event is the date code is superseded or replaced.	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. **Examples:** Source code audits ITIL release management function and auditing application program changes Post conversion troubleshooting Templates, style sheets and code that determine web site architecture **NOTE:** Data used for testing system functionality (the testing data sets) are not considered records

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT000012	**IT Software / Hardware Operating Procedures and Infrastructure Documenta-tion**	Records include procedures for entry of system operational parameters, system administration, hours of system operation, production control, and other aspects of an IT operation. **NOTE:** This may include vendor and/or manufacturer documentation.	No	Yes, state building plans and specifications per Wis. Stat. § 19.36(9) and Wis. Stat. § 16.851; may include information that is trade secret and cannot be disclosed pursuant to Wis. Stat. § 19.36(5) and § 134.90(1)(c); computer programs that cannot be disclosed pursuant to Wis. State. § 19.36(4); or other legally protected intellectual property (copyright, etc.); follow any agency-specific statutory citations	EVT + 3 years and destroy confidential.	Event is the agency no longer uses related software/ hardware and all data is transferred to and made useable in new software/ hardware environment.	Basis for subsequent operational procedures. Records may include: • operating manuals • hardware/operating system requirements • hardware configurations • equipment control systems **Examples:** System administration operation procedures; library procedures; installation procedures; backup procedures. Note: Procedures under this RDA have typically gone through a vetting process and are intended to support the agency's policies in a direct manner. This RDA does not necessarily include worker instructions which may be viewed as task-specific directions used to ensure compliance with policies and procedures.

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT000014	**Operating System and Hardware Migration Plans**	Records include migration plans and documentation for the replacement of equipment or computer operating systems. (Version changes, not release changes)	No	No	EVT + 3 years and destroy.	Event is a major upgrade or discontinued use of system, but not before system data is destroyed or transferred to new operating environment.	Planning for subsequent migrations. (Release version documentation would be covered under IT00008.) Product research materials Plans may be needed for a longer period of time for critical information systems, migration planning, or after migrations for reference and to deal with unforeseen issues and problems.
IT000015A **DO NOT USE** **Superseded by FAC00090**	**Disaster Recovery Records**	Records include those created during the disaster recovery process. Per FEMA: "Record Keeping. It is critical that the applicant establish and maintain accurate records of events and expenditures related to disaster recovery work."	Yes	Yes, follow agency-specific statutory citations	EVT + 3 years and destroy confidential. FEMA Public Assistance Guide – Chapter 5: Project Mgt	Event is defined as the recovery process is completed.	Information required for documentation describes the "who, what, when, where, why and how much, for each item of disaster recovery work. Indexes, inventory lists, computer logs, working papers, and correspondence. This series also includes computer tapes, or other media held in reserve in the event that an information system fails to function and records need to be recovered and restored.
IT000016	**IT Service Support Documenta-tion**	Records include warranty and maintenance contract information including vendor contact information for servers, networks, and personal computing equipment. Documentation of support service provided for servers, networks, and personal computing equipment. **NOTE:** This may include vendor and/or manufacturer documentation.	No	No	EVT + 1 year and destroy.	Event is the date the equipment is retired.	Information on the warranty or maintenance/support contracts for computer equipment. This can include contact information needed to place service calls. Documentation of requests to vendors for technical assistance or repairs and responses to these requests. Information or reports on the use of computer equipment for

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
							program delivery, security, or other purposes such as trend analysis. **Examples:** Warranty information Maintenance/support contract information Site visit reports Trouble reports Related correspondence and memoranda
IT000020	**Network Support or Circuit Installation and Service History and Summary**	Records include site visit reports, trouble reports, service history, network upgrade documentation and other related correspondence, including work orders, work schedules, building/circuit diagrams, network outages and application outages. History and summary records related to the provision, quality, and availability of network support services. Requests by agencies to DOA or contracted service provider for data communication service, installation, or repair and response to the request.	No	Yes, state building plans and specifications per Wis. Stat. § 19.36(9) and Wis. Stat. § 16.851	EVT + 5 years and destroy confidential. **Note**: The longer retention period is desired for audit purposes.	Event is defined as when the request is completed.	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 Agency reconciliation/cleanup process Work orders Correspondence / memoranda Work schedules Copies of building or circuitry diagrams Network design documents
IT000021	**Telecom and Data Circuit Inventories**	Records include support documentation for telecommunication and network equipment. Circuit inventories used by the agency, which may include phone wires, circuit number, vendor, cost per month, type of connection, terminal series, software, contact person and other relevant information about the circuit.	No	No	EVT and destroy. **NOTE**: If there is not a summary report as in IT000020, these records will need to be retained 4 fiscal years after	Event is superseded.	**Examples:** Agency reconciliation/cleanup process Billing account information Telecommunication service inventory Current call flows System configurations User guides and instructions

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
					(event) ending date of planning cycle.		Support manuals Cross-connection information Binding post information Backup procedures
IT000023	**Operational and Other Automated Logs**	Records include logs created to monitor usage. The logs may include network or operating system logs (that are not security related). Lists of holdings, control logs and information on the destruction of files stored on electronic media (does not include the data on the media).	No	Yes, metadata may contain confidential information. Follow agency-specific statutory citations.	EVT and destroy confidential.	Event is superseded or reviewed.	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. **Examples:** System usage files Storage manager reports TSM logs Software Library Computer run logs and related records may include: • daily schedules • Oracle server storage reports • 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
IT000026	**Access Logs**	Records include electronic files, automated logs, or film logs created to monitor access and use of agency services. Includes compiled application, security, and system logs.	Yes	Yes, follow agency-specific statutory citations	CR + 1 year and destroy confidential, but NOT before relevant audit (federal, state, etc.) or incident	Creation	Logs may relate to access of agency-provided services. They are needed for incident resolution, such as litigation and customer complaints. Logs are also retained to reveal unauthorized access and intrusions.

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
					litigation issues have been resolved and documentation requirements have been met. IRS records retention for tax information security events for state and local agencies with FTI data access is covered under IRS Pub 1075; Section 9.3.3.3., Audit events (AU-2), describes relevant Security related events and Section 9.3.3.5., Audit Storage Capacity (AU-4), Provides retention requirements.		**Examples:** Security logs, such as those related to file and folder access, account and group management, and user log-on and log-off. Agency Internet Services logs Access and usage trends Statistics Internet and Intranet logs Web server logs Web Site posting logs indicating when pages were posted, updated or removed File transfer logs Service access logs Film logs
IT000027	**Employee Internet Use Logs**	Records include electronic files or automated logs created to monitor and control use of the Internet by agency employees.	Yes	Yes, follow agency-specific statutory citations	EVT + 3 months and destroy confidential, unless required for security purposes. While one-year retention is likely to be desirable in order to respond to employee supervisory issues, a shorter-	Creation	Logs may relate to employment actions and performance management. **Examples:** Proxy server logs and web filtering reports from applications such as Zscaler Elsa logs

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
					term retention period is acceptable for internet usage logs because they create a large volume of records for the 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**	Records include reports of web usage retained for trend analysis and customer service performance or related usage tracking data.	No	No	CR + 1 year and destroy.	Creation	**Examples:** Web Trends Google Analytics Urchin Associated reports to management
IT000029	**Telephone System Call Detail**	Records include documentation created for functions associated with the telephone system call detail.	No	No	CR + 5 years and destroy	Creation	**Example:** Phone bill details – usage detail
IT000031	**Telecom Maintenance Work Order Files and Logs**	Records include user change/ trouble requests, internal service order documentation, service order submitted to vendor, and maintenance and order logs.	No	No	EVT + 1 year and destroy. **NOTE:** If there is no summary report as in **IT000020,** these records will need the following, "Destroy 4 fiscal years after (event) ending date of planning cycle.	Event is close of contract or provision of service.	**Examples:** Reports of routine phone/phone line repairs done by vendor. Work orders submitted to the vendor.

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT000032	**User Access Requests and Authorizations**	Records include but are not limited to local and remote access and authorized logon id requests to agency systems or applications. **NOTE:** A user account on its own is not a record. This RDA covers the approvals/actions regarding access to an account. Any specific email records would be covered by a correspondence or project RDA in the ADM GRS (ADM0009, ADM00010, ADM00026, ADM00027), or a program-specific RDA.	Yes	Yes, follow agency-specific statutory citations	EVT + 2 years and destroy confidential.	Event is departure of employee requesting authorization	Records may be needed for audits, system security, summary reports, planning. **Examples**: Access requests Access authorizations
IT000033	**Employee / Contractor / Vendor Responsibility Acknowledgement Agreements, Trusted Use Agreements**	Records include employee acknowledgement of security-related responsibilities and trusted use agreements.	Yes	Yes, follow agency-specific statutory citations	EVT + 8 years and destroy confidential. If records are placed in the employee personnel file, the retention period would follow HR000190 (8 years after termination).	Event is departure of employee, contractor or vendor	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 regarding who has administrative access privileges to applications.	Yes	Yes, follow agency-specific statutory citations	EVT + 4 years and destroy confidential. In compliance with the Federal Office of Management and Budget Circular A-102, "Grants and Cooperative Agreements with State and Local Governments.	Event is departure of security officer or personnel granted administrative privileges or (event) revocation of such privileges.	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 has administrative access privileges to applications.

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT000035	**Computer Security, Incident and Investigation Reports**	Records include those of incidents involving unauthorized entry attempts, probes, and/or attacks on data processing systems, information technology systems, telecommunication networks, and electronic security systems including associated software and hardware. This would include official reports and other documentation if appropriate.	Yes	Yes, follow agency-specific statutory citations	EVT + 5 years and destroy confidential. In compliance with the Federal Office of Management and Budget Circular A-102, "Grants and Cooperative Agreements with State and Local Governments.	Event is relevant audit or incident litigation issues have been resolved and documenta-tion requirements have been met.	These reports may be retained for 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 applications Security breaches Computer investigations
IT000040	**User Support Records**	Records include documentation of troubleshooting and problem-solving assistance provided by the agency's information systems personnel to users of the systems.	No	No	EVT and destroy	Event is case is resolved or report is no longer needed for business purposes.	**Examples:** Help desk assistance requests Resolution records Help desk application reports Cherwell help desk tickets Requests for account security management types of activities (password resets, unlocks, enables) must follow IT000026. New User Access requests follow IT000032.
IT000041 **NEW**	**Software Management Records**	Records include documentation of the use of software in agency information systems to insure that agency software packages are compatible, license and copyright provisions are complied with, and upgrades are obtained in a timely manner.	No	No	EVT + 1 year and destroy	Event is software is disposed of or upgraded.	**Examples:** Software inventories Software licenses Site licenses Related correspondence and memoranda

RDA Number	Records Series Title	Series Description	PII	Confidential	Minimum Retention and Disposition	Event Description	Examples/Notes
IT000042 **NEW**	**Web Management and Operations**	Records include documentation of the management of a website that provides context and structure related to the site.	No	No	EVT and destroy	Event is superseded or the website is updated.	Records that: • specify an agency's web policies and procedures; • provide detailed procedures for documenting how records are selected, created and approved for web posting, and how they will be revised or removed; • specify what records will be created and how they will be created for interactive sections of web sites; • document procedures used in the operation of the site; • specify the relationship of the webmaster and other staff involved in preparing and posting web documents

SUPERSEDED RDAs "Superseded" means that a new record series or RDA number has been used to cover records that were previously identified differently.				
RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000002 **Superseded by ADM00023**	**IT Policies and Standards**	Records of IT policies, standards and procedures that 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 WI-Madison Archives.)	Policies may be needed for reference and management audit purposes for a number of years after they are no longer in force.
IT000004 **Superseded by ADM00026**	**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 recommendations, IT investment decisions, and other general IT business of the agency.	Retain 3 years after (event) minutes are published and transfer to the appropriate archival repository (Wisconsin Historical Society [State Archives] or the University of Wisconsin Madison Archives).	For an agency, this would apply to only the top level IT steering group within that agency. Agency oversight or enterprise oversight, like DOT's ITOC, TLC, the old Business Leadership Council, Enterprise Steering Team.
IT000005 **Superseded by ADM00027**	**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, State Email Administrators, old Domains, Security (ISAS), GIS Committee, directory working group. Project working committees that keep minutes would follow the project RDA, IT000009.
IT000012A **Superseded by IT000012**	**IT Operating Procedures - Critical Information Systems**	Procedures for entry of system operational parameters, system administration, hours of system operation, production control, and other aspects of an IT operation. Note: this may include vendor and/or manufacturer documentation.	Destroy 7 years after (event) procedure is withdrawn, revised, updated, or superseded. **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	System administration operation procedures; Tape library procedures; Installation procedures; Backup procedures.

			reference and management audit purposes for up to 7 years after they are no longer used for active administration.	
IT000013 **Superseded by IT000012**	**IT Software/Hardware Infrastructure Documentation**	Use, operation, and maintenance of an agency's IT equipment. NOTE: This may include vendor and/or manufacturer documentation.	Destroy 1 year or after (event) the agency no longer uses related software/hardware and all data is transferred to and made usable in the new software/hardware environment.	Records may include: • Operating manuals • Hardware/operating system requirements • Hardware configurations equipment control systems
IT000015 **Superseded by ADM00008**	**Disaster Preparedness and Recovery Plans**	Plans and documentation for the protection and reestablishment of IT services and equipment in case of a disaster.	Destroy after (event) superseded by revised plan.	Living Disaster Recovery and Planning System (LDRPS) version of IT documents.
IT000017 **Superseded by Purchasing and Procurement GRS PUR00010**	**Technology Selection Documentation**	Research, analysis, review and recommendation records regarding selected software/hardware for agency use, including vendor information and related material.	Event (procurement) plus 4 years.	Subsequent procurements, contested procurements, open records requests, LAB audit reviews Documentation and process used to choose technology to perform the functions.
IT000018 **Superseded by IT000010**	**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.	Destroy 4 fiscal years after (event) ending date of planning cycle.	LAB audit reviews Release management documentation Test procedures related to release or upgrade of software or application code
IT000019 **Superseded by IT000023**	**Data/Backup Library Control Files**	Lists of holdings, control longs and information on the destruction of files stored on electronic media in a library.	Destroy after superseded	Storage manager reports Log files TSM logs
IT000022 **Combined with IT000020**	**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.	Work orders Correspondence/memoranda Work schedules Copies of building or circuitry diagrams Network design documents
IT000024 **Combined**	**Data Documentation / Metadata**	Data generally created during development or modification of an automated system. Data necessary for	Destroy after (event) the application's data is destroyed or migrated to a new structure	These records are essential for managing electronic records in agency automated information

with IT000010		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.	or format.	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. Used to validate the authenticity of the electronic record in the unstructured world.
IT000030 **Combined with IT000021**	**Telecom Inventory Support**	Support documentation for telecommunication equipment and phone 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.

CLOSED A closed series contains records that are no longer created, nor are they expected to be in the future.				
RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
IT000025 **CLOSED – not a record**	**Test Data**	Data used for testing system functionality **NOTE:** Loading data from a production system, obfuscating it, and using as test data does not create a new record.	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.

RELATED RECORDS

Information on other record series in approved GRSs which may relate to the broader functional area of this GRS. These record series are listed to facilitate a more complete understanding of all the record series within the broad scope of this function of government. It may not however contain a complete listing of all records series used within your agency for these types of business records.

RDA Number	Records Series Title	Description	Minimum Retention and Disposition	Use Case/Example
ADM00008 Administrative Records	**Agency Final Continuity of Operations/Continuity of Government Operational Plan and Documentation**	Agency official copy and work papers of the COOP/COG plan. **NOTE:** This record set may be classified as confidential	Event and destroy confidential Event is superseded by revised plan	Disaster preparedness and recovery plans
ADM00023 Administrative Records	**Internal Policies and Procedures**	Established departmental policies and procedures. **NOTE:** May also be called Administrative Practices or Directives or Executive Directives.	Event + 7 years and destroy Event is the date the policy and procedure is superseded or made obsolete.	Manuals Manual codes Handbooks, etc. Includes IT policies and procedures
ADM00026 Administrative Records	**Team, Project, or Workgroup Documentation – Program/Policy Impact**	Records associated with teams, committees, projects, or workgroups established by or among agencies that have program and/or policy impact.	Creation + 5 years and transfer to the WHS or UW-Madison Archives	See ADM General Schedule for specifics, but includes IT Steering/ Policy Committee Documentation
ADM00027 Administrative Records	**Team, Project, or Workgroup Documentation – Internal and Routine Activities**	Records associated with teams, committees, projects, or workgroups established by or among agencies that have internal impact only.	Creation + 2 years and destroy	See ADM General Schedule for specifics, but includes IT Topical Committee Documentation
90000021 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.	
90000021 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.	
PUR00010 Purchasing & Procurement	**Contract and Request for Bid/Proposal File**	Records used to document, calculate costs and bill program units for computer usage and IT services. These records are also used for cost recovery,	Destroy 4 years after close of contract. Purchase records are usually	Copies of records created to initiate the purchasing process, authorize and provide funds for, or satisfy claims and expedite payments for

		budgeting, or administrative purposes.	maintained together in Contract Case File.	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
Purchasing & Procurement GRS	**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.	RDA PUR00007 Request for Purchasing Approval/Authority and Procurement Plans Evt+6 years and destroy	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.

REVISION HISTORY A listing of changes to this GRS.			
Revision Date	**RDA Number**	**Record Series Title**	**Revision Made**
Monday , 11-10-2014	IT000003	IT management Reports and Metrics	Retention decreased from 7 yrs to 4 yrs
Monday, 11-10-2014	IT000010	Systems Specs Documentation and Quality Control Files	Retention increased from 3 yrs to 4 yrs
Monday, 11-10-2014	IT000016	IT Service Support Documentation	Retention decreased from 2 yrs to 1 yr
Monday, 11-10-2014	IT000020	Network Support or Circuit Installation and Service History and Summary	Event and retention changed from '1 yr after close of contract or 5 yrs, whichever is greater' to 'when the request is completed plus 5 yrs'
Monday, 11-10-2014	IT000023	Operational and Other Automated Logs	Event changed from 'when no longer needed' to 'superseded or reviewed'
Monday, 11-10-2014	IT000028	Website Usage Reports	Event changed from 'superseded' to 'creation'
Monday, 11-10-2014	IT000033	Employee/Contractor/Vendor Responsibility Acknowledgement Agreements, Trusted Use Agreements	'Contractor/Vendor' added to title
Monday, 3-9-2015	IT000006	Fiscal Year Planning Documents for IT Activity Levels	MOU and SLA examples removed. Now retained under ADM00029.
Monday, 3-9-2015	IT00006A	Data Sharing Agreements	MOU example removed. Now retained under ADM00029.
Monday, 6-1-2015	IT000015A	Disaster Recovery Records	Superseded by new record series in Facilities Management GRS, FAC00090.

Monday, 8-24-2015	IT000012	IT Software / Hardware Operating Procedures and Infrastructure Documentation	Clarifying note regarding procedures added to Use Case/Examples.
Monday, 11-16-15	IT000026	Access Logs	Title changed, 'Application' removed. Description and Examples/Notes expanded.
Monday, 11-16-15	IT000040	User Support Records	Examples/Notes expanded.

Appendix A
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 tools, image editing programs, and communication program.

Configuration
Generally, a configuration is the arrangement—or the process of making the arrangement—of the parts that make up a whole. 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.

> **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).

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 backup and recovery procedures are in place, protecting confidential or private information in data, reducing redundancy in data, and establishing 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).

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. When describing unstructured data (such as email, 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.

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.

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.

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.

Unstructured Data (see Data)

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.

Appendix B
Topical Index