

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
ADP IRM	<u>ITOM</u>	<u>INFORMATION TECHNOLOGY</u>		
	ITOM – 1 ✦	IT Performance Measurements and Benchmarks Correspondence, Reports and Plans Statistical performance data for systems and networks; System availability reports; Sample performance indicators	<u>TEMPORARY:</u> Destroy/delete 5 years after the project/activity/transaction is completed or superseded.	GRS 3.1, Item 040
	ITOM – 2 ✦	IT Oversight and Compliance Correspondence, Reports, C&A and Quality Assurances. Target IT architecture reports; Systems development lifecycle handbooks; Network assessments; Contractor evaluation reports; Market analyses; Performance surveys; Cost-benefit analyses; Histograms; Corrective action reports	<u>TEMPORARY:</u> Destroy/delete 5 years after the project/activity/transaction is completed or superseded.	GRS 3.1, Item 040
	ITOM – 3 ✦	IT Facility Management and Equipment Support Correspondence and Reports Listing of facilities; Inspection reports	<u>TEMPORARY:</u> Destroy/delete 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.	GRS 3.1, Item 020
	ITOM – 4 ✦	IT Inventories Correspondence, Reports, Equipment Control Network Circuits, Circuitry and Diagrams Inventories of IT assets, network circuits, and building or circuitry diagrams, including equipment control systems such as databases of barcodes affixed to IT physical assets.	<u>TEMPORARY:</u> Destroy/delete 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.	GRS 3.1, Item 020
	ITOM – 5 ✦	IT Configuration and Change Management Correspondence and Reports – Data and detailed reports on implementation of systems, applications and modifications; application sizing, resource and demand management; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution and release or version management.	<u>TEMPORARY:</u> Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes.	GRS 3.1, Item 030

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
	ITOM – 6 ✦	<p>System Backups Incremental</p> <p>Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.</p> <p>**NOTE: See ITOM – 33 for backups of master files and databases.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.</p>	GRS 3.2, Item 040
	ITOM – 7 ✦	<p>System Backups Full</p> <p>Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.</p> <p>**NOTE: See ITOM – 33 for backups of master files and databases.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete full backup tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.</p>	GRS 3.2, Item 041
	ITOM – 8	<p>Library Tapes</p> <p>Library tape records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy when no longer needed.</p>	GRS 4.1, Item 010
	ITOM – 9 ✦	<p>IT Maintenance</p> <p>Correspondence, Reports and Work Orders</p> <p>Records of routine IT maintenance on the network infrastructure documenting preventative, corrective, adaptive and perfective enhancement, maintenance actions, including requests for service, work orders, service histories, and related records.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.</p>	GRS 3.1, Item 020
ADP 2	ITOM – 10 ✦	<p>IT System Security and Disaster Recovery Plans</p> <p>Correspondence, Reports and Plans</p> <p>a. System Security Plans and Disaster Recovery Plans.</p> <p>Computer technical manuals; Continuity of Operations plans; Disaster exercise evaluations; Disaster exercises; Disaster recovery plans; Risk surveys; Security plans for IT infrastructure; Vulnerability assessments by IG; Vulnerability assessments/studies</p> <p>b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks,</p>	<p><u>TEMPORARY:</u></p> <p>Destroy 1 year after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.</p>	GRS 3.2, Item 010

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
		<p>implementation of risk action plan, service test plans, test files and data.</p> <p>Risk management analyses; Security directives; Security policy analysis; Virus handbooks; Vulnerability analyses</p>		
	ITOM – 11 ✦	<p>System Access Records</p> <p>These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as:</p> <ul style="list-style-type: none"> • user profiles • log-in files • password files • audit trail files and extracts • system usage files • cost-back files used to assess charges for system use. <p>Exclusion 1: Records relating to electronic signatures.</p> <p>Exclusion 2: Does not include monitoring for agency mission activities such as law enforcement.</p>		
		<p>a. Systems not requiring special accountability for access.</p> <p>These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy when business use ceases.</p>	<p>GRS 3.2, Item 030</p>
		<p>b. Systems requiring special accountability for access.</p> <p>These are user identification records associated with systems which are highly sensitive and potentially vulnerable.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy 6 years after password is altered or user account is terminated.</p>	<p>GRS 3.2, Item 031</p>
	ITOM – 13 ✦	<p>IT Computer Security Incident Reporting</p> <p>Correspondence and Reports</p> <p>Reports and documentation of Web site defacement; Hacks; Break-in records; Improper usage by staff; Misuse of system; Security breaches; Security break-ins; Security failures; Unauthorized intrusions; Virus threats</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete 3 years after all necessary follow-up actions have been completed.</p>	<p>GRS 3.2, Item 020</p>
	ITOM – 14 ✦	<p>IT Operations Routine Schedules</p> <p>Correspondence, Reports, Work Load and Maintenance Schedule, and support activities</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete 3 years after agreement, control</p>	<p>GRS 3.1, Item 020</p>

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
		Cycle time reports; Maintenance schedules; Run reports; Workload schedules	measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.	
	ITOM – 15 ✦	IT Operations Problem Reports Correspondence and Reports Problem reports and related decision documents relating to the software infrastructure of the network or system.	<u>TEMPORARY:</u> Destroy/delete 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.	GRS 3.1, Item 020
	ITOM – 16 ✦	IT Operations Benchmarking Correspondence and Reports Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring; and management reports.	<u>TEMPORARY:</u> Destroy/delete 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.	GRS 3.1, Item 020
	ITOM – 17 ✦	IT COTR Files <i>(NOTE: Copies of records needed to support contracts should be in procurement files.)</i> Correspondence, Reports, Project Files, Finance and Performance Criteria a. Agreements formalizing performance criteria for quantity and quality of service, including definition of responsibilities, response times and volumes, charging, integrity guarantees, and non-disclosure agreements. b. Files related to managing third-party services, including records that document control measures for reviewing and monitoring contracts and procedures for determining their effectiveness and compliance. c. Records generated in IT management and service operations to identify and allocate charges and track payments for computer usage, data processing and other IT services EXCLUDING records that are part of the agency's cost accounting system.	<u>TEMPORARY:</u> Destroy/delete 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded.	GRS 3.1, Item 020
	ITOM – 18	IT Help Desk Correspondence, Reports, FAQ and Logs	<u>TEMPORARY:</u> Destroy/delete 1 year after record is superseded or obsolete or no longer	GRS 24, Item 10(a), 10(b)

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
			needed, whichever is later.	
	ITOM – 19 ✦	<p>IT Infrastructure Design and Implementation Files</p> <p>Correspondence, Reports, Design, Installation and Testing Requirements.</p> <p>a. Implemented</p> <p>b. Not Implemented</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete 5 years after project is terminated.</p>	GRS 3.1, Item 010
	ITOM – 20 ✦	<p>System Development Records</p> <p>Records that relate to the development of Information Technology (IT) systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving.</p> <p>(Includes but not limited to: project plans, feasibility studies, cost analyses, requirements documents, compliance documents (Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), Security Plan, Information Protection Plan), change control records, Project Schedule, Plan of Action and Milestones (POA&M), Configuration Management Plan, Resource Management Plan, Risk Assessment/Mitigation Plan, Security Plan, Disaster Recovery Plan, Test/Acceptance Plan, Quality Control Plan, Deployment Guide, User Guide, and Training Guide.)</p> <p>Exclusion: This does not apply to system data or content.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes.</p>	GRS 3.1, Item 011
	ITOM – 21 ✦	<p>Special Purpose Computer Programs and Applications</p> <p>Computer software programs or applications that are developed by the agency or under its direction solely to use or maintain a master file or database authorized for disposal in a GRS item or a NARA-approved records schedule.</p> <p>Exclusion 1: This does not include software or applications necessary to use or maintain any scheduled/unscheduled master file or database scheduled for transfer to the National Archives.</p> <p>Exclusion 2: This does not cover commercial, off-the-shelf (COTS) programs or applications, unless</p>	<p><u>TEMPORARY:</u></p> <p>Delete when related master file or database has been deleted.</p>	GRS 3.1, Items 012

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
		<p>the agency has modified such programs or applications considerably to perform a mission-related function.</p> <p>Note: Computer software needs to be kept as long as needed to ensure access to, and use of, the electronic records in the system throughout the authorized retention period to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20.</p>		
	ITOM – 22 ✦	<p>Electronic input/source records</p> <p>Electronic records used to create, update, or modify records in an electronic recordkeeping system. Including:</p> <ul style="list-style-type: none"> • electronic files that duplicate information from a source electronic system for input into another electronic system • electronic records received from another agency and used as input/source records by the receiving agency • computer files or records containing uncalibrated and unvalidated digital or analog data collected during observation or measurement activities or research and development programs and used as input for a digital master file or database • metadata or reference data, such as format, range, or domain specifications which is transferred from a host computer or server to another computer for input, updating, or transaction processing operations <p>Exclusion 1: Original electronic records maintained in the source system.</p> <p>Exclusion 2: Electronic input records required for audit and legal purposes.</p> <p>Exclusion 3: Electronic input records produced by another agency under the terms of an interagency agreement or records created by another in response to the specific information needs of the receiving agency.</p>	<p>TEMPORARY:</p> <p>Destroy immediately after data have been entered or otherwise incorporated into the master file or database and verified.</p> <p>Note: This retention is NOT medial neutral. This applies to electronic records only.</p>	GRS 4.3, Item 020
	ITOM – 24 ✦	<p>Hardcopy or Analog Input/Source Records</p> <p>This covers hardcopy or analog records incorporated into an electronic system in their entirety or converted to an electronic format in their entirety. The types of input records that may be included are:</p> <ul style="list-style-type: none"> • hardcopy forms used for data input • hardcopy documents that are scanned into an electronic recordkeeping system 		

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
		<ul style="list-style-type: none"> hardcopy or analog still pictures, sound records, motion picture film, or video recordings that were previously scheduled as temporary 		
		<p>a. Hardcopy or analog input/records previously scheduled as temporary.</p> <p>Records previously scheduled as temporary used to create, update, or modify electronic records incorporated in their entirety into an electronic system.</p>	<p>TEMPORARY:</p> <p>Destroy immediately after verification of successful conversion.</p> <p>Note: This retention is NOT medial neutral. This applies to hardcopy or analog records only.</p>	GRS 4.3, Item 010
		<p>b. Hardcopy of analog input/source records previously scheduled as permanent.</p> <p>Records previously scheduled as permanent that are used to create, update, or modify electronic records and whose content is incorporated in its entirety into an electronic system in accordance with NARA's electronic records standards.</p> <p>Exclusion: The following input records previously scheduled as permanent may not be destroyed when converted to an electronic format. The hardcopy must be transferred to NARA according to the agency's approved schedule:</p> <ul style="list-style-type: none"> hardcopy records that NARA has specifically designated as permanent records that must be transferred to NARA in hardcopy format hardcopy records when the electronic versions do not meet NARA's electronic records standards hardcopy records that are not incorporated in their entirety into an electronic system original hardcopy still pictures, graphic materials/posters, aerial film, maps, plans, charts, sound recordings, motion picture film, or video records <p>Legal citations: 36 CFR 1225.22 (h)(2); 36 CFR 1225.24 (a)(1)</p>	<p>TEMPORARY:</p> <p>Destroy 60 days after submitting notification to NARA per 36 CFR 1225.24 (a)(1) and verification of successful conversion.</p> <p>Note: This retention is NOT medial neutral. This applies to hardcopy or analog records only.</p>	GRS 4.3, Item 011
		<p>c. Hardcopy or analog input/source records not previously scheduled.</p> <p>Hardcopy or analog records, not previously scheduled, that are used to create, update, or modify electronic records and whose content is incorporated in its entirety into an electronic system.</p> <p>Exclusion 1: Hardcopy records when the electronic versions do not meet NARA's electronic records standards.</p>	<p>TEMPORARY:</p> <p>Destroy immediately after approval of a schedule for the electronic records and after verification of successful conversion.</p>	GRS 4.3, Item 012

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
		<p>Exclusion 2: Hardcopy records that are not incorporated in their entirety into an electronic system.</p> <p>Exclusion 3: Original hardcopy still picture, graphic materials/posters, aerial film, maps, plans, charts, sound recordings, motion picture film, or video recordings: Both original hardcopy records and any electronic versions must be scheduled by an agency-specific schedule.</p>		
	ITOM – 27 *	Electronic Version of GRS 1-16, 18, 22, and 23 Correspondence and Reports	<u>TEMPORARY:</u> Delete after the expiration of the retention periods authorized by the GRS or when no longer needed, whichever is later.	GRS20, Item 3(a)
	ITOM – 28 *	Electronic Records That Support Administrative Housekeeping Functions When The Records Are Derived From or Replace Hard Copy Records Authorized by NARA for Destruction in an Agency Specific Records Schedule—When Hard Copy Records are Retained to Meet Recordkeeping Requirements Correspondence and Reports	<u>TEMPORARY:</u> Delete electronic versions when the agency determines that it is no longer needed for administrative, legal audit or other operational purposes.	GRS 20, Item 3(b)(1)
	ITOM – 29 *	Electronic Records That Support Administrative Housekeeping Functions When The Records Are Derived From or Replace Hard Copy Records Authorized by NARA for Destruction in an Agency Specific Records Schedule—When Electronic Records Replace Hard Copy Records that Support Administrative Housekeeping Correspondence and Reports	<u>TEMPORARY:</u> Delete after expiration of the retention period authorized for the hard copy file, or when no longer needed, whichever is later.	GRS 20, Item 3(b)(2)
	ITOM – 30 *	Electronic Records That Support Administrative Housekeeping Functions When The Records Are Derived From or Replace Hard Copy Records Authorized by NARA for Destruction in an Agency Specific Records Schedule—Hard Copy Printouts Created for Short Term Administrative Purposes Support Administrative housekeeping functions	<u>TEMPORARY:</u> Destroy when the agency determines that they are no longer needed for administrative, legal, audit or other operational purposes.	GRS 20, Item 3(b)(3)
	ITOM – 31 *	Data Files Consisting of Summarized Information Correspondence and Reports	<u>TEMPORARY:</u> Delete when business use ceases.	GRS 4.3, Item 031
	ITOM – 32 *	Records Consisting of Extracted Information Correspondence and Reports	<u>TEMPORARY:</u>	GRS 4.3, Item 031

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
			Destroy when business use ceases.	
	ITOM – 33 ✦	Backups of File for Permanent Records Correspondence, Reports and Backups	<u>TEMPORARY:</u> Destroy immediately after identical records have been captured in a subsequent backup file or at any time after the transfer request has been signed by the National Archives.	GRS 3.2, Item 050
	ITOM – 34 ✦	Backups of Files for Temporary Records Correspondence, Reports and Backups	<u>TEMPORARY:</u> Destroy immediately after the identical records have been deleted or replaced by a subsequent backup file.	GRS 3.2, Item 051
	ITOM – 36 ✦	Documentation Necessary for Preservation of Permanent Electronic Records Correspondence and Reports	<u>TEMPORARY:</u> Transfer to the National Archives with the permanent electronic records to which the documentation relates.	GRS 3.1, Item 050
	ITOM – 37 ✦	Downloaded and Copies Data Derived from Existing Agency Data Correspondence and Reports	<u>TEMPORARY:</u> Destroy when business use ceases.	GRS 4.3, Item 030
	ITOM – 40	(ERS Records) Website Records – Internet		
	ITOM – 41	(ERS Records) Website Records – Intranet		
	ITOM – 42	Security		
	ITOM – 43	Software Development		
	ITOM – 44 ✦	Public Key Infrastructure (PKI) Administrative Records Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction	<u>TEMPORARY:</u> Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA.	GRS 3.2, Items 060 and 061

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
		<p>process. Included are policies and procedures planning records; stand-up configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records. Policies and procedures planning records relate to defining and establishing PKI systems. Records relate to such activities as determining that a PKI should be established; creating project implementation plans; creating the certificate policy (CP), certification practice statement (CPS), and other key operating documents; developing procedures in accordance with the CP and CPS; conducting risk analyses; developing records management policies (including migration strategies); and selecting the entity that will serve as registration authority (RA). Stand-up configuration and validation records relate to installing and validating both the Certification Authority (CA) and Registration Authority (RA), obtaining final approval or rejection from the agency's oversight or authorizing body, creating and generating a CA signature key, testing security procedures for the CA and RA, validating certification revocation procedures, and establishing back-up and storage for the PKI system. Operation records relate to the certification application ; certificate issuance and key generation (including key pair generation and private key loading and storage of private keys and components of private keys); certificate acceptance, validation, revocation, suspension, replacement, and renewal; creating and maintaining an event log; and installing and validating software updates. Audit and monitor records relate to conducting periodic internal and external reviews of auditable events specified in the Federal Bridge Certification Authority (FBCA) X.509 Certificate Policy and other Entity CA policies, monitoring compliance with security requirements specified in the CPS and other operating procedures, investigating internal fraud or misconduct, and conducting internal and external audits of software and systems security.</p> <p>Termination, consolidation, or reorganization records relate to terminating, consolidating, or reorganizing a PKI; notifying subscribers of decisions, transferring inactive keys and revocation certificate lists to storage repositories, transferring inactive keys and revocation certificate lists to storage repositories, transferring consenting subscribers' and certificates and relating material to a new Certificate Authority, destroying sensitive records involving privacy (in accordance with an authorized records schedule), and shutting down and disposing of RA hardware and CA software.</p>		

OLD CODE	NEW (USDA) CODE	TITLE/DESCRIPTION	DISPOSITION	DISPOSITION AUTHORITY
	ITOM – 45 ✦	<p>PKI Transaction-Specific Records</p> <p>Records relate to transaction-specific records that are generated for each transaction using PKI digital signature technology. Records are embedded or referenced within the transaction stream and may be appended to the transaction content or information record. Along with PKI administrative and other administrative records, transaction-specific records are part of the PKI trust documentation set that establish or support the trustworthiness of a transaction. They may vary from transaction-to-transaction and agency-to-agency. When retained to support the authentication of an electronic transaction content record (information record), PKI digital signature transaction records are program records.</p>	<p><u>TEMPORARY:</u></p> <p>Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and /or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.</p>	GRS 3.2, Item 062