

GENERAL RECORDS SCHEDULE 24

Information Technology Operations and Management Records

This schedule provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. As defined in the Information Technology Management Reform Act of 1996 (now the Clinger-Cohen Act), "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

This GRS does not cover all records relating to information technology operations and management. Offices with responsibility for IT operations also maintain administrative records covered by other GRS and records not in the GRS that must be scheduled by the agency. In addition, this GRS does not apply to system data or information content, which must be scheduled separately by submitting an SF 115, Request for Records Disposition Authority, to NARA.

The disposition instructions apply to records regardless of physical form or characteristics. Records may be maintained on paper, in microform, or electronically. Dispositions apply, however, only to records that are maintained as described in each item or subitem. If documents are part of a larger case file or recordkeeping system that contains records not covered in this GRS, agencies must separately schedule that file or system by submitting an SF 115 to NARA. If records covered by more than one item in this schedule are maintained together in one file or recordkeeping system, agencies must retain the records for the longest retention period authorized for those items.

Note that GRS 20, Electronic Records, remains in effect. GRS 20 covers certain temporary files associated with data base management. This new schedule supplements GRS 20 by providing disposal authority for temporary records relating to overall IT management, as opposed to the operation and use of specific systems. NARA is reviewing alternatives to GRS 20 and will develop revised requirements as it explores new approaches to managing electronic records.

1. Oversight and Compliance Files.

Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to compliance with IT policies, directives, and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities.

a. Performance measurements and benchmarks.

Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

b. All other oversight and compliance records, including

certification and accreditation of equipment, quality assurance reviews and reports, reports on implementation of plans, compliance reviews, and data measuring or estimating impact and compliance.

Destroy/delete when 3 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

[Note: See item 3b for performance files relating to systems.]

2. IT Facility, Site Management, and Equipment Support Services Records.

Records maintained by offices responsible for the control and operation of buildings and rooms where IT equipment, systems, and storage media are located, including files identifying IT facilities and sites, and files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence.

Destroy/delete when 3 years old, or when superseded or obsolete, whichever is longer.

3. IT Asset and Configuration Management Files.

a. 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.

Destroy/delete 1 year after completion of the next inventory.

b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems. Includes, but is not limited to:

(1) 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.

Destroy/delete 1 year after termination of system.

(2) 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.

Destroy/delete when 3 years old or 1 year after termination of system, whichever is sooner.

[Note: If any maintenance activities have a major impact on a system

or lead to a significant change, those records should be maintained as part of the item 3b(1).]

4. System Backups and Tape Library Records.

a. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

(1) Delete/destroy incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

(2) Delete/destroy full backup tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

[Note: See GRS 20, item 8, for backups of master files and databases.]

b. Tape library 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.

Destroy/delete when superseded or obsolete.

5. Files Related to Maintaining the Security of Systems and Data.

a. System Security Plans and Disaster Recovery Plans.

Destroy/delete 1 year after system is superseded.

b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data.

Destroy/delete 1 year after system is superseded.

6. User Identification, Profiles, Authorizations, and Password Files, EXCLUDING records relating to electronic signatures.

a. Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records.

Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

b. Routine systems, i.e., those not covered by item 6a.

See GRS 20, item 1c.

7. Computer Security Incident Handling, Reporting and Follow-up Records.

Destroy/delete 3 years after all necessary follow-up actions have been completed.

8. IT Operations Records.

a. Workload schedules, run reports, and schedules of maintenance and support activities.

Destroy/delete when 1 year old.

b. Problem reports and related decision documents relating to the software infrastructure of the network or system.

Destroy/delete 1 year after problem is resolved.

c. Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring; and management reports.

Destroy/delete when 3 years old.

9. Financing of IT Resources and Services.

[Note: Copies of records needed to support contracts should be in procurement files, which are scheduled under GRS 3.]

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.

Destroy/delete 3 years after agreement is superseded or terminated.

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.

Destroy/delete 3 years after control measures or procedures are superseded or terminated.

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, which are covered in GRS 8, items 6 and 7.

Destroy/delete records with no outstanding payment issues when 3 years old.

10. IT Customer Service Files.

a. Records related to providing help desk information to customers, including pamphlets, responses to "Frequently Asked Questions," and other documents prepared in advance to assist customers.

Destroy/delete 1 year after record is superseded or obsolete.

b. Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting.

Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.

11. IT Infrastructure Design and Implementation Files.

Records of individual projects designed to provide and support new agency IT infrastructure (see Note), systems, and services. Includes records documenting (1) requirements for and implementation of functions such as maintaining network servers, desktop computers, and other hardware, installing and upgrading network operating systems and shared applications, and providing data telecommunications; (2) infrastructure development and maintenance such as acceptance/accreditation of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with implementation, modification, and troubleshooting; (3) models, diagrams, schematics, and technical documentation; and (4) quality assurance reviews and test plans, data, and results.

a. Records for projects that are not implemented.

Destroy/delete 1 year after final decision is made.

b. Records for projects that are implemented.

Destroy/delete 5 years after project is terminated.

c. Installation and testing records.

Destroy/delete 3 years after final decision on acceptance is made.

[Note: IT Infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Components include hardware such as printers, desktop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems (e.g., Microsoft Windows and Novell NetWare) and shared applications (e.g., electronic mail, word processing, and database programs). The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency's IT infrastructure. However, records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of an SF 115 to NARA.]

12. Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this GRS 24

schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is completed.

GRS 24 Implementation Aid

GRS 24 Schedule Items

Examples of Types of Records

1. Oversight and Compliance Files

Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to compliance with IT policies, directives, and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities.

a. Performance measurements and benchmarks.

Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

b. All other oversight and compliance records, including certification and accreditation of equipment, quality assurance reviews and reports, reports on implementation of plans, compliance reviews, and data measuring or estimating impact and compliance.

Destroy/delete when 3 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

[Note: See item 3b for performance files relating to systems.]

Statistical

performance data for systems and networks;

System availability reports; Sample performance indicators

Target IT architecture reports; Systems development lifecycle handbooks; Network assessments; Contractor evaluation reports; Market analyses; Performance surveys; Cost-benefit analyses; Histograms; Corrective action reports

2. IT Facility, Site Management, and Equipment Support Services Records.

Records maintained by offices responsible for the control and

operation of buildings and rooms where IT equipment, systems, and storage media are located, including files identifying IT facilities and sites, and files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence.

Destroy/delete when 3 years old, or when superseded or obsolete, whichever is longer.

Listings of facilities;

Inspection reports

3. IT Asset and Configuration Management Files.

a. 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.

Destroy/delete 1 year after completion of the next inventory.

b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems. Includes, but is not limited to:

(1) 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.

Destroy/delete 1 year after termination of system.

(2) 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.

Destroy/delete when 3 years old or 1 year after termination of system, whichever is sooner.

NOTE: If any maintenance activities have a major impact on a system or lead to a significant change, those records should be maintained as part of the item 3b(1).

Maintenance IT assets:

Inventories of assets,

Equipment control systems; Databases of barcodes; Bar code reports;

Maintenance service histories;

Asset management guides,

Service; Requisitions for equipment maintenance; Change orders;

Purchase orders for maintenance; Property transfer control systems;

Flow reconfiguration requests;

Standardization requests and justifications.

4. System Backups and Tape Library Records.

a. Backup tapes maintained for potential system restoration in

the event of a system failure or other unintentional loss of data.

(1) Delete/destroy incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

(2) Delete/destroy full backup tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

[Note: See GRS 20, item 8, for backups of master files and databases.]

b. Tape library 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.

Destroy/delete when superseded or obsolete.

Backup tapes;
Backups of system software

Location vault lists;
Offsite storage facilities;
Bin location

5. Files Related to Maintaining the Security of Systems and Data.

a. System Security Plans and Disaster Recovery Plans.

Destroy/delete 1 year after system is superseded.

b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data.

Destroy/delete 1 year after system is superseded.

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

Risk management analyses; Security directives; Security policy analysis; Virus handbooks; Vulnerability analyses

6. User Identification, Profiles, Authorizations, and Password Files

EXCLUDING records relating to electronic signatures.

a. Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records.

Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

b. Routine systems, i.e., those not covered by item 6a.

See GRS 20, item 1c.

User identification; User profiles;
User passwords
Profiles; User authorizations

7. Computer Security Incident Handling, Reporting and Follow-up Records

Destroy/delete 3 years after all necessary follow-up actions have been completed.

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

8. IT Operations Records

a. Workload schedules, run reports, and schedules of maintenance and support activities.

Destroy/delete when 1 year old.

b. Problem reports and related decision documents relating to the software infrastructure of the network or system.

Destroy/delete 1 year after problem is resolved.

c. Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring; and management reports.

Destroy/delete when 3 years old.

Cycle time reports; Maintenance schedules; Run reports; Workload schedules

Software problem reports

Benchmark measures; Operation reports; Performance monitoring

9. Financing of IT Resources and Services

[Note: Copies of records needed to support contracts should be in procurement files, which are scheduled under GRS 3.]

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.

Destroy/delete 3 years after agreement is superseded or terminated.

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.

Destroy/delete 3 years after control measures or procedures are superseded or terminated.

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, which are covered in GRS 8, items 6 and 7.

Destroy/delete records with no outstanding payment issues when 3 years old.

Acquisition; Contract award fees; Financial mgmt; Financial records; Payment for software and services; Performance agreements; Service level agreements; Service support levels; Third party agreements
10. IT Customer Service Files

a. Records related to providing help desk information to customers, including pamphlets, responses to ``Frequently Asked Questions,`` and other documents prepared in advance to assist customers.

Destroy/delete 1 year after record is superseded or obsolete.

b. Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting.

Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.

Customer queries; Customer service; End-user inquiries; Feedback records; FAQs; Help Desk logs; Pamphlets; Requests for assistance; Trend analysis; Trouble reports; User guides

11. IT Infrastructure Design and Implementation Files

Records of individual projects designed to provide and support new agency IT infrastructure (see Note), systems, and services. Includes records documenting (1) requirements for and implementation of functions such as maintaining network servers, desktop computers, and other hardware, installing and upgrading network operating systems and shared applications, and providing data telecommunications; (2) infrastructure development and maintenance such as acceptance/accreditation of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with implementation, modification, and troubleshooting; (3) models, diagrams, schematics, and technical documentation; and (4) quality assurance reviews and test plans, data, and results.

a. Records for projects that are not implemented.

Destroy/delete 1 year after final decision is made.

b. Records for projects that are implemented.

Destroy/delete 5 years after project is terminated.

c. Installation and testing records.

Destroy/delete 3 years after final decision on acceptance is made.

[Note: IT Infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Components include hardware such as printers, desktop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems (e.g., Microsoft Windows and Novell NetWare) and shared applications (e.g., electronic mail, word processing, and database programs). The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency's IT infrastructure. However, records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of an SF 115 to NARA.]

Acquisition; Implementation of new systems; Installation and testing; Installation reviews; New enterprise projects; Quality assurance plans; Requirements specifications; Technology refresh plans; Test plans

12. Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this GRS 24 schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is completed.

Copies of records in this GRS 24 created using electronic mail and word processing