SERIES: 2200 Information Management and Information Technology Operations

2200-IIS

Identity Information System (IIS): The IIS is a central repository composed of three sub-systems that provide an automated tool for human resources to track data and action to fill a position and for security officers to track the security screening action for hew hire. Systems users request access via IIS. IIS is also used to track a position announcement opening and closing, human resource activities, security officer's activities, revoke system access privileges, training, office and location data on employees and contractors. Information maintained include contact information, employee personal identification, office of assignment, office location, badge information, supervisor name, training taken, and information system access requests. Each BIA government employee and contractor has a record in the IIS eProfile system.

A. Source Records/Inputs

1. Source Records (Paper): The inputs to the system include: Data derived from Human Resource, Security, management, and employee activities.

Disposition Instructions: Apply disposition instructions approved for paper and microfilm records. (Reference Indian Affairs Record Schedule record series for specific program records)

2. Source Records (Electronic): Electronic files or records used to create or update a master file, including, but not limited to, work files, valid transaction files, and intermediate input/output records. **(GRS-20/1b)**

Disposition Instructions: TEMPORARY. Delete after information has been transferred to the master file and verified. Subject to Multiple Record Freezes and/or Litigation holds.

B. Master Data File

The master data files contain information on position announcement, position closing, date hired, date terminated, receiving of security screen packages, package status, screening activities, system access request and responses including approval and disapproval, employee name, social security number, mother's maiden name, types and dates of training, assigned office and location, badge information, supervisor, IIS system roles, system approval information and other security information collected.

Routine systems, i.e., those not covered by item 6a (Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records). **(GRS 24/6b)**

Disposition Instructions: TEMPORARY. (See GRS 20, item c) Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.

C. System Generated Documents/Outputs

1. System Generated Documents in Case Files: Case files specific queries, sorts, reports, tables, and related records and data compilation reports (e.g., management reports and plans) that are created for case files, studies, inquiries, inspections, and related program files.

Disposition Instructions: Apply disposition instructions approved for paper and microfilm records. (Reference Indian Affairs Record Schedule record series for specific program records)

2. Routine systems, i.e., those not covered by item 6a (Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records). **(GRS 24/6b)**

Disposition Instructions: TEMPORARY. (See GRS 20, item c) Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.

3. Data Verification Reports or Screen Prints, Data Verification – Non case/subject file specific screen prints, test reports, data validation reports and system diagnostics.

a. Electronic files or records created solely to test systems performance, as well as hard-copy printouts and related documentation for the electronic files/records. **(GRS-20/1a)**

Disposition Instructions: TEMPORARY. Delete/Destroy when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

b. Electronic files or records used to create or update a master file, including, but not limited to, work files, valid transaction files, and intermediate input/output records**. (GRS-20/1b)**

Disposition Instructions: TEMPORARY. Delete after information has been transferred to the master file and verified.

c. Electronic files and hard-copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use. **(GRS-20/1c)**

Disposition Instructions: TEMPORARY. Delete/Destroy when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

d. Records create 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: 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. **(GRS-24/3b1)**

Disposition Instructions: TEMPORARY. Destroy/delete 1 year after termination of system.

D. Documentation

1. Data Systems specifications, file specifications, code books, record layouts, user guides, output specifications, and final reports, regardless of medium, relating to a master file or data base. **(GRS 20/11a)**

Disposition Instructions: TEMPORARY. Destroy or delete when superseded or obsolete, or upon authorized deletion of the related master file or data base, or upon the destruction of the output of the system if the output is needed to protect legal rights, whichever is latest.

2. Copies of Records relating to system security, including records documenting periodic audits or reviews and re-certification of sensitive applications, disaster and continuity plans, and risk analysis, as described in OMB Circular No. A-130. **(GRS-20/11b)**

Disposition Instructions: TEMPORARY. Destroy or delete when superseded or obsolete.

E. Backups/Vital Record Backups. Backups are intended for making a copy of computer files for use if the original is lost, damaged or destroyed. The Backup process includes copying recorded information from internal storage to an external storage medium, such as magnetic tape, cartridges, CDs, and Optical disk. The Disposition of Backups is Temporary because they are intended to restore a system in case of failure. Backups do not meet NARA requirements for long term retention or preservation of permanent data. **(GRS-20/8a)**

Disposition Instructions: TEMPORARY. File identical to records scheduled for transfer to the National Archives: Delete when the identical records have been captured in a subsequent backup file or when the identical records have been transferred to the National Archives and successfully copied.