

OFFICE OF THE GOVERNOR  
OFFICE OF INFORMATION TECHNOLOGY SERVICES  
ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE

Program Records Retention and Disposition Schedule

The Program Records Retention and Disposition Schedule and retention periods governing the records series listed herein are hereby approved. In accordance with the provisions of Chapters 121 and 132 of the General Statutes of North Carolina, it is agreed that the records of the

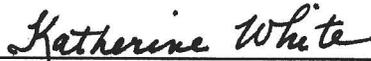
**ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE**

do not and will not have further official use or value for administrative, research, or reference purposes after the respective retention periods specified herein. The N.C. Department of Cultural Resources consents to the destruction or other disposition of these records in accordance with the retention and disposition instructions specified in this schedule. However, records subject to audit or those legally required for ongoing official proceedings must be retained until released from such audits or official proceedings, notwithstanding the instructions of this schedule. **Public records including electronic records not listed in this schedule or in the *General Schedule for State Agency Records* are not authorized to be destroyed. The**

**ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE**

agrees to destroy, transfer or dispose of records in the manner and at the times specified herein. This schedule is to remain in effect until superseded.

**APPROVAL RECOMMENDED**



Katherine White, Chief Records Officer  
Office of Information Technology Services



Ann Garrett, State Chief Information  
Security Officer  
Enterprise Security and Risk Management Office



David Brook, Director JPL  
Division of Historical Resources

**APPROVED**



George Bakolia, State Chief Information Officer  
Office of Information Technology Services



Lisbeth C. Evans, Secretary  
Department of Cultural Resources

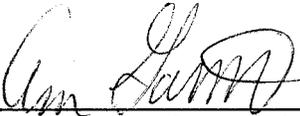
PROGRAM RECORDS RETENTION AND DISPOSITION SCHEDULE AMENDMENT

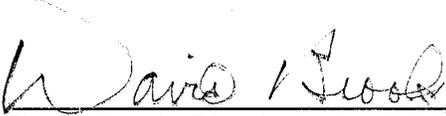
**OFFICE OF THE GOVERNOR  
OFFICE OF INFORMATION TECHNOLOGY  
Enterprise Security and Risk Management Office**

Amend the program records retention and disposition schedule approved February 22, 2008 and by amending items 47329 and 47332 and as shown on the included schedule. No other items on this schedule have been amended, added, or removed.

**APPROVAL RECOMMENDED**

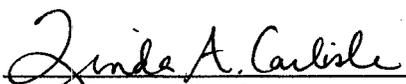
  
\_\_\_\_\_  
Danny Lineberry, Acting Chief Records Officer  
Office of Information Technology Services

  
\_\_\_\_\_  
Ann Garrett, State Chief Information  
Security Officer  
Enterprise Security and Risk Management Office

  
\_\_\_\_\_  
David Brook, Director  
Division of Historical Resources

**APPROVED**

  
\_\_\_\_\_  
George Bakolia, State Chief Information Officer  
Office of Information Technology Services

  
\_\_\_\_\_  
Linda A. Carlisle, Secretary  
Department of Cultural Resources

**OFFICE OF THE GOVERNOR  
OFFICE OF INFORMATION TECHNOLOGY SERVICES  
ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE**

**ITEM 47321. PROJECT (ELECTRONIC) FILE.**

Records in electronic format for projects of the Chief Information Security Officer concerning the security of information technology resources belonging to state agencies. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding security features of public information technology systems.

DISPOSITION INSTRUCTIONS: Destroy in office when administrative value ends.

**ITEM 47323. CHIEF INFORMATION SECURITY OFFICER'S CORRESPONDENCE FILE.**

Records in paper and electronic formats concerning correspondence generated by the Chief Information Security Officer. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding security features of public information technology systems.

DISPOSITION INSTRUCTIONS: Transfer paper and electronic records when administrative value ends to the State Records Center (electronic records will be held by the Information Technology Branch, Department of Cultural Resources). Paper and electronic records will be held for agency for 3 additional years and then transferred to the custody of the Archives. Electronic records must include information relating to the format and arrangement of the records as part of the accompanying metadata. (Contact the Government Records Branch, Electronic Records Unit prior to the transfer of electronic records.)

**ITEM 47324. INTERNAL AUDIT (ELECTRONIC) FILE.**

Records in electronic format concerning the security, risk management and internal audit of information technology resources of state agencies. File includes detailed and summary reports. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding security features of public information technology systems.

DISPOSITION INSTRUCTIONS: Destroy in office when superseded or obsolete.

**ITEM 47325. CORRESPONDENCE TO AGENCIES (ELECTRONIC) FILE.**

Records in electronic format comprised of routine correspondence with other agencies concerning the security, risk management and internal audits of information technology resources and the appointment of security liaisons. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding security features of public information technology systems.

DISPOSITION INSTRUCTIONS: Destroy in office when administrative value ends.

**ITEM 47326. AGENCY CAPITAL EXPENDITURE SHEETS (ELECTRONIC) FILE.**

Records in electronic format concerning expenditures made by state agencies for information technology security needs. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding security features of public information technology systems.

DISPOSITION INSTRUCTIONS: Destroy in office when superseded or obsolete.

**OFFICE OF THE GOVERNOR  
OFFICE OF INFORMATION TECHNOLOGY SERVICES  
ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE**

**ITEM 47327. NON-DISCLOSURE AGREEMENTS FILE.**

File contains signed non-disclosure agreements for each agency's security liaison.

DISPOSITION INSTRUCTIONS: Destroy in office 3 years after an employee is no longer a security liaison if no litigation, claim, audit, or other official action involving the records has been initiated. If official action has been initiated, destroy in office after completion of action and resolution of issues involved.

**ITEM 47328. BACKGROUND CHECK FORMS FILE..**

Completed background checks for employees acting as security liaisons. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding security features of public information technology systems.

DISPOSITION INSTRUCTIONS: Destroy in office 3 years after an employee is no longer a security liaison if no litigation, claim, audit, or other official action involving the records has been initiated. If official action has been initiated, destroy in office after completion of action and resolution of issues involved.

**ITEM 47329. SECURE PORTAL (ELECTRONIC) FILE.**

A secure portal and related records and data that informs state agencies of possible risks to their information technology resources. File includes announcements of computer viruses, articles of interest for those charged with information security and other related records. (Comply with confidentiality restrictions of G.S. 132-6.1 (c) regarding records with sensitive public security information.)

DISPOSITION INSTRUCTIONS: Update in office routinely. Destroy in office when administrative value ends.

**ITEM 47330. ACCESS DOCUMENTS FOR SECURE PORTAL FILE.**

Forms in paper and electronic formats used to regulate access to Secure Portal File (Item

DISPOSITION INSTRUCTIONS: Destroy in office paper and electronic records when superseded or obsolete.

**ITEM 47332. RISK ASSESSMENT DATABASE (ELECTRONIC) FILE.**

Records concerning incidents involving unauthorized attempted entry probes and/or attacks on agency electronic data processing systems, information technology systems, telecommunications networks, and electronic security systems, including associated software and hardware. File includes reports, logs, extracts and compilations of data, and other related records. (Comply with applicable provisions of G.S. 132-1.7 regarding sensitive public security

DISPOSITION INSTRUCTIONS: Item discontinued. Superseded by the General Schedule for State Agency Records.

**ITEM 47365. AUDIT FILE.**

Records in paper and electronic formats include internal audits, audits of other agencies, IRS audits and other related records.

DISPOSITION INSTRUCTIONS: Retain in office paper and electronic records permanently. Destroy paper and electronic reference copies of audits when administrative value ends.