Using Records Retention Schedules:
How Long Do Audit Trails Need to Be Kept?

Purpose: Provide retention guidance to state and local government agencies for information system audit trails.

Retention Requirements

Until no longer needed for agency business

DAN	Description of Records	Retention and Disposition Action	Designation
GS 14020 Rev. 2 / GS2010-003 Rev. 2	*Audit Trails and System Usage Monitoring* Records documenting the use of the agency's information technology and communication systems to ensure security and appropriate use. Includes, but is not limited to: • Audit trails; • Authorizations for and modifications to the configurations and settings of the agency's IT infrastructure (such as firewalls, routers, ports, network servers, etc.); • Log-in records, security logs and system usage files; • Internet activity logs (sites visited, downloads/uploads, video/audio streaming, etc.); • Fax and telephone logs. Excludes records covered by: • *Internet Browsing (DAN GS 50010/GS2016-006);* • *Security Incidents and Data/Privacy Breaches (DAN GS 25008/ GS2010-008)*	Retain until no longer needed for agency business *then* Destroy.	NON-ARCHIVAL NON-ESSENTIAL OFM

The *State Government General Records Retention Schedule* and *Local Government Common Records Retention Schedule (CORE)* are available from the Washington State Archives' website.

What Does This Mean?

This does not mean zero retention, or the default system/vendor's retention settings.

Agencies need to determine and document in their policies/procedures how long they need to retain audit trails to ensure security and appropriate use.

Agencies may also need to adopt strategies to capture and preserve audit trails if their business need is longer than the default system/vendor settings.

Additional advice regarding the management of public records is available from Washington State Archives:

www.sos.wa.gov/archives
recordsmanagement@sos.wa.gov