

Office of the Chief Information Officer

Online File Storage Guidance to Agencies to Develop Policies for Use

BACKGROUND

Online file storage services offer powerful and convenient methods to share files among collaborators, various computers, and mobile devices. In the absence of well-defined agency policies, education of employees, and the availability of approved alternatives for sharing files securely, some employees may overlook security and records management requirements in the interests of “getting the job done” via no or low-cost consumer level services.

Consumer-level online storage services can pose significant risks related to the security, privacy, copyright, and retention of public records (including “data”; see definition of “state records” below). These services are typically accessed via “click-through” agreements, which are binding contracts that often contain provisions that put state agencies and their records at significant risk. With these services, agencies have little or no visibility into or control over what records are stored there, or shared with other people or devices. Consequently agencies may be unable to search thoroughly when legal or business needs arise. The records stored in consumer-level services are associated with individual subscribers rather than organizations. Thus, if an agency employee who is a subscriber leaves the agency, the associated records are likely no longer accessible to the agency.

The increased use of online services, social media, mobile apps, personal devices for work, and online file storage can result in blurred lines between actions taken as a state employee and actions taken as a private individual. Employees who use online tools for both personal and agency purposes should understand that the way they handle information at home may not be the way they handle agency records at work.

INTRODUCTION

Agencies are responsible for maintaining and protecting state records as required by law. Agencies should educate employees on the best uses of online file storage services and provide enterprise-class alternatives that satisfy collaboration, productivity, and records management requirements. In short, make the right thing to do the easy thing to do.

These guidelines (1) offer a “refresher” on the overall guiding principles to manage state records of any type successfully and then, (2) provide information and tools related to online file storage to help agencies:

- Make a deliberate and informed decision on whether to authorize use of online file storage services for agency records based on the circumstances.
- Develop agency-specific policies or guidelines for using online file storage services that satisfy business productivity, legal, public disclosure, records management, and IT security concerns. Agencies can select from the recommended practices to suit their particular needs and establish additional guidelines or policies as necessary.
- Select enterprise-class solutions for online file storage services that meet agency needs for employee file sharing and collaboration and at the same time satisfy agency records management requirements.
- Educate employees to realize the benefits of using online file sharing services and avoid common mistakes that may lead to increased risk or financial loss.

DEFINITIONS

Online File Storage Service: A file hosting service, cloud storage service, or online file storage provider that hosts user files via the Internet. Users can upload files that can be accessed over the internet from other computers, tablets, smartphones or other networked devices, by the same user or other designated users.

State Records: For purposes of these guidelines, the term “state records” includes all public records. “Public record” is defined by statute and includes any paper, correspondence, completed form, bound record book, photograph, film, sound recording, map drawing, machine-readable material, compact disc meeting current industry ISO specifications, or other document, **regardless of its physical form or characteristics** (including copies of such records), that are made by or received by any agency of the state of Washington in connection with the transaction of public business. See RCW 40.14.010. As used in these guidelines, “agency records” and data also mean state records.

Mobile Devices: A small-sized computing device that may have a display screen, touch input or a keyboard, and/or data storage capability. Examples include laptops, smart phones, tablet PCs, accessible equipment, and portable data storage devices such as removable hard drives, and USB data storage devices.

Public Disclosure Request: A written request under chapter RCW 42.56 for the inspection and copying of a public record. An agency is prohibited from destroying or erasing a record, even if it is about to be lawfully destroyed under a retention schedule, if a public records request has been made for the record. Agencies are required to retain potentially responsive records until the public record request is resolved. Where notified of a public records request, employees must, *with regard to potentially responsive records, suspend the destruction of records, conduct a reasonable search for records, and gather or segregate records so they may be reviewed and, if necessary, produced.* Like other records, records created or stored with an online file storage service are subject to the requirements of public disclosure.

Legal Hold: A legal hold is a communication issued as a result of current or reasonably anticipated litigation, audit, government investigation or other such matter that suspends the normal disposition or processing of records. Legal holds may encompass procedures affecting data that is accessible as well as data that is not reasonably accessible. The specific notice to agencies may also be called a “hold,” “preservation order,” “suspension order,” “freeze notice,” “hold order,” or “hold notice.” Where notified of a Legal Hold, employees must, *with regard to potentially responsive records, suspend the destruction of records, conduct a reasonable search for records, and gather or segregate records so they may be reviewed and, if necessary, produced.*

GUIDING PRINCIPLES FOR STATE RECORDS MANAGEMENT

For all state records, including those stored on online file storage services, agency management and employees should apply these guiding principles:

Agency

The agency, not employees, own agency records

- The agency establishes approved storage services and devices
- The agency assigns one or more officials to manage its various types of records

Online File Storage
Guidance to Agencies to Develop Policies for Use

- Designated agency officials are authorized to make decisions on data collection, storage methods, use, modification, sharing, protection and disposal of state records
- The agency classifies data and records into categories 1 – 4 based on sensitivity

Employee

Employees are custodians of agency records, and should:

- Store records only on agency-approved storage services or devices
- Minimize the number of copies and storage locations
- Be accountable to use, store, share, and protect agency records according to agency direction and applicable statutes, policies, contracts, and data classification
- Keep the records as long as required to meet records retention schedules, then delete them as directed by the agency unless they are subject to public disclosure or legal hold

Records management requirements are listed in the Related Laws and Resources Section.

GUIDELINES

Guidelines for agency and employee use of online file services follow below:

Agency Guidelines

Q1: How does an agency initiate use of an online file storage service?

A1.1: Use of online file storage services should be expressly authorized by appropriate agency action.

A1.2: Following authorization agencies should select and approve, according to state procurement policies, one or more online file services for agency use.

A1.3: The agency should communicate the approved storage services (and, if applicable, mobile devices) to employees who are authorized to use them.

A1.4: Agencies are encouraged to include in the selection criteria the items in Appendix A on security, agency administration, and Terms of Service (TOS), ensuring that enterprise-grade and not consumer-grade online file storage services are approved.

Q2: What are the contractual considerations?

A2.1: Prior to authorizing the execution of a “click-through” agreement, if used for such services, agencies should review the applicable Terms of Service, which constitute a binding contract between the service provider and the agency.

A2.2: Agencies are encouraged to consult their assistant attorney general before executing such an agreement. Certain terms may preclude an agency from using a particular service.

A2.3: Agencies should assess Terms of Service for risk, for critical terms that may be missing, and for unacceptable terms in light of the intended use and type of records to be stored.

Q3: How should agencies treat original records vs. copies?

A3.1: Agencies should ensure that online file storage services are used as temporary storage to share copies of records for collaboration and access by other computers and mobile devices. In summary, use approved services as “systems of engagement” rather than “systems of record”.

A3.2: Original or official records should be stored on agency or state computer systems serving as systems of record.

A3.3: If a record has been modified in the collaboration process, the agency should sync interim versions with the system of record if the service allows, because the modified record is no longer a “copy”. In any case, the agency must ensure that the final version is stored back on the system of record.

A3.4: Unneeded copies and outdated versions of records on the online file storage system, the system of engagement, should be deleted in accordance with records management policies. Agencies are required to provide originals and all copies of relevant records in response to public disclosure requests and legal holds. Keeping too many records that are scheduled for destruction, as well as keeping multiple unneeded copies of records, significantly increases agency costs and administrative burdens for complying with public records requests or legal hold notices.

A3.5: Whether or not they are considered copies, records potentially responsive to a public disclosure request or legal hold must be preserved and not deleted until the hold is lifted with regard to those records.

Q4: Is central administration of an online file storage service necessary? Who does it and what do they do?

A4.1: Agencies should centrally administer the online file service similar to the way they administer agency-operated computing and storage services.

A4.2: At a minimum, administrators should create and de-activate employee accounts using existing agency approvals and processes, assist employees with use as needed, and access, search, and manage all records as needed across employee accounts belonging to the agency on the service.

A4.3: Agencies are expected to ensure that online storage of state records is expressly authorized and is in compliance with these guidelines. Agencies may want to determine which types of data are authorized for storage in online file services or mobile devices, regardless of data category. Online storage may not be appropriate even for some category 1 or 2 records.

A4.4: Agencies should use periodic audits, training, data loss prevention tools, etc., to detect and prevent the misconfiguration or misuse of approved services. One example is storing unapproved data or confidential category 3 and above data in online file storage services approved only for category 1 and 2 data.

Q5: How should agencies educate employees to use online file storage services?

A5: Agencies should educate employees on appropriate use of online file services, addressing the following points at a minimum:

- The benefits and opportunities of using online file storage services
- The services approved for agency use
- The types of agency records that can and cannot be stored on the service
- The agency official(s) that direct the use of each type of agency record
- The employee's role and responsibilities as custodian of agency records, and how this may differ from how they handle information as private individuals
- Recommended ways to configure and use the service to obtain expected benefits, locate or produce agency records when requested, and avoid risks from unauthorized data access, change, or disclosure
- Avoiding the co-mingling of agency records and personal data on online storage services, mobile devices, personal email systems, home computers, etc.
- The risks to the state for misuse or misconfiguration of online storage services

Employee Guidelines

Employees can make good use of online file storage services by applying the guidelines below:

Q6: Can employees use online file storage services to share agency records?

A6: As approved by the agency, employees may use online file storage services to share agency records.

Q7: What type of records can be shared?

A7.1: Employees may share data and records classified as Category 1 or 2 as defined below, subject to additional direction from the agency:

Category 1 – Public Information: Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2 – Sensitive Information: Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

A7.2: Employees may share copies of Category 1 or 2 agency records using an approved service for temporary storage to share files among collaborators, various computers, and mobile devices. This is using the service as a “system of engagement” rather than a “system of record”. Original records must be stored on agency operated systems. Other policies and standards may apply as directed by the agency.

Q8: What type of records must not be shared?

A8: Employees must not share records classified as Category 3 or 4, as defined below, unless an online file service is expressly approved by the agency for such use. As an alternative however, when approved by the agency, employees may share Category 1 – 4

records using the Secure Email service that is available today as part of the CTS Shared Email service.

Category 3 – Confidential Information: Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

- Personal information about individuals, regardless of how that information is obtained.
- Information concerning employee personnel records.
- Information regarding IT infrastructure and security of computer and telecommunications systems.

Other examples include, but are not limited to:

- HIPAA Information – Any health related information including diagnosis, dates of service, doctor visits, treatments, provider information, etc.
- FERPA Information – Student records, grades, class enrollment, etc.
- Payment Card Industry Information – Credit card numbers, PINS, verification codes, etc.

Category 4 – Confidential Information Requiring Special Handling: Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

- Especially strict handling requirements are dictated, such as by statute, regulation, or agreement.
- Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Also, please note that employees must not store category 3 or higher data on mobile devices unless it is authorized by the agency and encrypted on the device.

Q9: Can employees use personal storage accounts to share state records?

A9.1: Employees must only use agency-approved online file storage services, and agency-provided accounts on those services, to share state records or access them from other computers and mobile devices. Employees are not permitted to use personal accounts, even on approved services, for state business. Likewise, employees must not use personal email accounts to transfer or share state records. This enables the employee and agency to manage state records according to state law and agency policy.

A9.2: Employees that store agency records in personal accounts may make those accounts discoverable. The same could apply to personal devices based on the circumstances.

A9.3: Employees must not click to accept click-through agreements when acting as a state employee, unless specifically authorized by the agency, because this may bind the agency to a contract that has not been evaluated or approved. Some click-through agreements on consumer services allow the service to access and use data stored there or delete it.

A9.4: Employees must promptly move any state records stored on personal accounts or unapproved services to agency-owned file storage or to an approved service / employee account, and completely dispose of any copies of state records in the unapproved service / account. The same principles apply to state records stored on unapproved mobile devices, and to personal devices as directed by the agency.

Q10: How can I avoid losing track of original state records and copies that I am responsible for?

A10.1: Use the fewest number of online storage services needed to meet agency needs. This reduces the complexity and effort of managing and locating state records, and reduces the risk of missing records subject to public disclosure or legal hold. (This principle also applies to mobile devices and home computers).

A10.2: Establish automatic expiration periods for files at the time they are stored on the online service. Files should not remain online, on mobile devices, or home computers for longer than necessary. Delete online files no longer used or no longer subject to records retention requirements. **This does not apply to files subject to a public records request or legal hold.**

A10.3: Establish procedures to (1) turn off automatic expiration periods for files subject to a public records request or legal hold, (2) preserve such files in their existing state and (3) preserve any relevant files later created.

A10.4: Ensure that synchronizing features of the online storage service only access the intended files and folders. This avoids storing records on the online service that belong only on the internal systems of record.

A10.5: Ensure that files stored online remain usable, searchable, retrievable, and authentic for their designated retention period as required by WAC 434-662-040.

A10.6: When leaving the agency, the employee must ensure all employee managed records are transferred to an appropriate custodian and shared folder owners and appropriate agency officials are notified.

Q11: How can I protect the confidentiality of records I store on an online file service?

A11.1: Ensure that sharing records with the public at large complies with the OCIO Public Records Privacy Protection Policy and other applicable statutes or regulations.

A11.2: Use shared folders, not public folders, authorizing access to specifically identified individuals or groups.

A11.3: Frequently review usage events and shared folder membership. Update permissions and make other changes as needed.

RELATED LAWS AND RESOURCES

Agencies are required to create, retain, manage, and dispose of public records according to:

- Chapter 40.14 RCW (Preservation and destruction of public records)
- Chapter 42.56 RCW (Public disclosure)
- WAC 434-662 (Preservation of electronic public records)
- State IT Security Standards 141.10 - Securing Information Technology Assets
<http://ofm.wa.gov/ocio/policies/documents/141.10.pdf>
- Definition and Classification of Public Records
<http://apps.leg.wa.gov/RCW/default.aspx?cite=40.14.010>
- Public Records Act - Definitions
<http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.010>
- Records Management and Retention Schedules
http://www.sos.wa.gov/archives/RecordsManagement/records_state.aspx

- Unique Agency Schedules
- Use of State Resources: WAC 292-110-010
- Preservation of Electronic Public Records: WAC 434-662-040
- Ethical Obligations: RCW 42.52.050

APPENDIX A

Criteria for agency selection of online file storage services

At a minimum, agencies should include the following criteria when selecting online file services:

Security

- Ensure that the security controls in place in the solution comply with OCIO 141.10
- Records should be encrypted in transit and at rest with a minimum strength of 128 bit encryption
- Least privilege concepts and role based access controls can be enforced to ensure users only have access to authorized files
- Ensure automated enforcement of strong passwords per OCIO security standards
- Ensure that logging and monitoring tracks all add, change, delete, copy/sync activity for each file. Agency administrators should be able to review these logs.
- Provide high availability infrastructure, all within the United States

Central Administration

- Agency central account creation and de-activation
- Administration interface to manage file and folder structures and access
- Administrators can search for and access records across all agency/employee accounts
- Retention, logging, and archiving must support agency requirements for e-discovery and investigations
- Usage monitoring and the ability to view file storing, sharing, and modification activity over time
- Mobile application user settings / options management
- Recovery of items that have been inadvertently deleted
- Manual and automated expiration for files
- Forced deletion of objects that are past their records retention storage date
- Remote administration capabilities, including the ability to remotely wipe devices or synchronized files from those devices
- Ability to monitor and add additional storage
- Secure methods to ensure User Authentication and Controlled Access
- Integration with Active Directory

Terms of Service

“Click-through” terms of service, which cannot be negotiated, frequently include provisions that create legal or risk issues for state agencies. Also, agencies may not have authority to

Online File Storage
Guidance to Agencies to Develop Policies for Use

agree to some provisions contained in these terms. At a minimum, consider the following issues:

- Do the terms indicate whether state records will be stored only in the United States?
- Is the service provider expressly prohibited from using state records for any purpose other than providing services to the agency, such as “data mining”?
- Do the terms provide for state records to be downloaded or destroyed in a manner acceptable to the agency when services are terminated?
- Do the terms provide that the agency agrees to waive its right to a jury trial? Agencies are encouraged to discuss this circumstance with their AAG.
- Do the terms state that the agency agrees to indemnify the service provider? Agencies are encouraged to discuss this circumstance with their AAG.
- Do the terms provide for jurisdiction and venue in, or applying the laws of, another state? Agencies are encouraged to discuss this circumstance with their AAG.
- The privacy policy for online file storage services should be consistent with federal and state privacy obligations, including implications for personal information required from employees.

Agencies and their AAGs will vary in their risk tolerance on these points.

Whether to agree to a particular term or set of terms is for the agency to decide, as long as it has conducted a thorough review of the Terms of Service before accepting them via “click through”.