Effective Date: **9/1/2018**

Last Updated: Click or tap to enter a date.

POL 8530.02

Cancels: N/A

See Also:

National Institute of Standards and Technology 800-53

RCW 40.14 Preservation and Destruction of Public Records

RCW 42.56.010(3) Public Records Act

RCW 43.105.215 Security Standards and Policies

WAC 292-110-010

WAC 434-615 Custody of Public Records

WAC 434-662 Preservation of Electronic Records

OCIO Policy 101 Technology Policies and Standards

OCIO Policy 141.10 - Securing Information Technology Assets Standards

OCIO On-line File Storage Guidance

WDFW Policy 1005 Public Records Requests

WDFW Policy 1018 Separating Employees from WDFW

WDFW Policy 1020 Managing and Retaining WDFW Records

WDFW Policy 7008 Using State-Owned Computing Resources

POL 8000.01 Policy Governing IT Document Stacks

POL 8000.02 Technology Policy Waiver

PRO 8000.01 Document Stack Life-cycle Procedure

PRO 8000.02 Technology Policy Waiver

STD 8650.08 List of Sensitive Information

Approved by: /S/ Joe Stohr

POL 8530.02 ON-LINE FILE STORAGE

Applies to:

This policy applies to all WDFW employees and anyone working under contract for WDFW who use on-line file storage systems to create or manage WDFW public records. However, if policies or procedures are in conflict with or are modified by a bargaining unit agreement, the agreement language shall prevail.

Definitions:

Breach: For purposes of this section [policy], "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the Agency.

Category 3 Information: Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to;

(a) Personal information as defined in RCW 42.56.590 and RCW 19.255.10.

(b) Information about public employees as defined in RCW 42.56.250.

(c) Information about the infrastructure and security of computer and Telecommunication networks as defined in RCW 42.56.420.

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

(a) Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.

(b) Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Chief Information Officer (CIO): The Washington Department of Fish and Wildlife, Information Technology Services, Chief Information Officer (WDFW ITS CIO) is the senior-level manager within WDFW ITS responsible for the Information Technology strategy and the computer systems required to support the department’s technology objectives and goals.

Chief Information Security Officer (CISO): The Washington Department of Fish and Wildlife, Information Technology Services, Chief Information Security Officer (WDFW ITS CISO) is the senior-level manager within WDFW ITS responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Employee: Permanent, temporary, or volunteer worker.

Information Governance Unit (IGU): A division within Technology and Finance Management (TFM) responsible for records and data management, public records compliance, discovery and litigation hold requirements.

Information Governance Unit Manager (IGU Manager): The Washington Department of Fish and Wildlife, Information Governance Manager (WDFW IGU Manager) is responsible for the WDFW information governance program.

Information Technology Services (ITS): The Washington Department of Fish and Wildlife, Information Technology Services (WDFW ITS) is a division within Technology and Finance Management (TFM) responsible for enterprise-wide, ITS supported production systems and in establishing and maintaining the department's technology vision and strategy to ensure information assets and technologies are adequately protected.

Information Technology Steering Committee: A chartered committee of IT professionals from across the Agency, chaired by the WDFW ITS CIO responsible for reviewing proposed IT policies and procedures. This committee also reviews and recommends solutions to IT issues and works together to develop and implements a coordinated Agency-wide IT strategic plan.

Litigation Hold: A written communication issued as a result of current or reasonably anticipated litigation that instructs employees who are likely to have department records pertaining to the anticipated litigation to take immediate action to identify and preserve the records for future retrieval. A Litigation Hold Notice instructs employees to 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.

Notice of Security Breach: Pursuant to RCW 42.56.590, WDFW must provide notification to residents of this state whose personal information was, or is likely believed to have been acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of security is not reasonably likely to subject consumers to a risk of harm.

Office of the Chief Information Officer (OCIO): The Office of the Chief Information Officer (OCIO) sets information technology (IT) policy and direction for the State of Washington. The State CIO is a member of the Governor's Executive Cabinet and advisor to the Governor on technology issues.

On-line File Storage: On-line file storage refers to the practice of storing electronic data with a third party service accessed via the Internet. It is an alternative to traditional local storage (such as disk or tape drives) and portable storage (such as optical media or flash drives). It can also be called "hosted storage," "Internet storage" or "cloud storage".

Public Disclosure Request (PDR) (also known as a Public Records Request): A written request under chapter RCW 42.56 for the inspection and/or copying of a public record per WDFW Policy 1005 Public Records Requests.

Public Record: Public record includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. "Writing" means handwriting, typewriting, printing, Photostatting, photographing, and every other means of recording any form of communication or representation –basically any information-recording medium, whether physical or digital.

Retention Requirements: The minimum amount of time to retain records according to requirements approved by the State Records Committee and as outlined in the Records Retention Schedules.

Secondary Services: Augmentation services provided in conjunction with on-line file storage services. User can communicate within the storage service by way of internal messaging or email.

Security Design Review: The Washington Office of Cyber Security (OCS) Security Design Review Process gives WDFW and WaTech the opportunity to review strategies for implementing new technology, or strategies for modifying existing services that interact with the following systems: The State Government Network (SGN), the Intergovernmental Network (IGN), state-wide systems, and the state's security infrastructure. The process analyses both internal and external system modifications. OCS then prepares a formal summary, which typically takes one to two weeks to research, prepare, and review with the customer. This summary is a valuable resource for customers to use in negotiations and discussions with business managers, third parties, and other government organizations. It also provides a formal record of the strategic and architectural intent of the project.

Policy Statement:

1. **The WDFW ITS CIO will be Responsible for Administering this Policy.**

2. **Employees Must Only Use Agency Approved Online File Storage Systems To Conduct Agency Business.**

3. **Employees Must Maintain Public Records Only on Approved Online File Services in Accordance with State Law, OCIO Security Policies, and WDFW Policy.**

4. **Employees Are Responsible for Searching, Retaining, and Providing Public Records Responsive to Public Disclosure Requests or Litigation Holds that Are Located on Online File Storage Services They Utilize.**

5. Employees may not Share Category 3 or Higher Information Outside of the Agency Without a Data Sharing Agreement, Signed Approval by the CIO, or unless Compelled by Law.

6. For the Agency to Meet Its Legal Notification Requirements of Security Breach and to Quickly Remediate Potential or Actual Cyber Security Issues, Employees Must Notify the WDFW ITS CISO and WDFW IGU Manager If There Is Suspicion of or an Actual Breach or Unauthorized Release of Category 3 or Higher Information Outside of the Agency.

7. The WDFW ITS CIO and WDFW IGU Manager Will Manage and Maintain the Process for Approving and Making Available a List of Approved Online File Storage Services.

8. The WDFW IT Steering Committee Will Review Requests for New Online File Storage Services and Evaluate Alignment with the Agency's IT Strategic Plan, Technology Portfolios and Investment, Public Records Management Plans, and with WDFW's Mission and Goals.

9. Approval of a New On-Line File Storage Service Must, at a Minimum, Consider:

9.1 Provisioning and removing user access.

9.2 Training and best practices materials for employees.

9.3 Passing a security design review.

9.4 Compliance with Agency litigation hold and public disclosure requests policies and procedures.

9.5 Budget approval.

9.6 Data Ownership & Stewardship, retention requirements and life-cycle.

10. The WDFW Information Governance Unit Will Develop and Maintain, as Necessary, any Standards, Processes, and Procedures, etc. to Support a Successful Adaptation, Implementation, and Governance of this Policy.

11. Employees may Submit a Technology Policy Waiver if they Believe Complying with This Policy Would Be Operationally or Technologically Detrimental to Their Organization.

11.1 Technology or policy requirements compelled by state WACs or RCWs cannot be waived.