*“Application Name”* **Acceptable Use Policy**

Contents

[Purpose 1](#_Toc58596954)

[Scope 1](#_Toc58596955)

[System Custodian Responsibilities 1](#_Toc58596956)

[Individual Rights and Responsibility 2](#_Toc58596957)

[1. Understanding. 2](#_Toc58596958)

[2. Revocability. 2](#_Toc58596959)

[Policy 2](#_Toc58596960)

[Privacy and Personal Rights 3](#_Toc58596961)

# Purpose

As a user of **“***Application Name”*you have access to valuable Department of Health information resources, it is important for you to act in a responsible, ethical and legal manner to protect these information assets.

In general, acceptable use means respecting the rights of other computer users, the integrity of the information resource, and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the Department of Health will take appropriate actions which includes the restriction and possible loss of system privileges. A serious violation could result in more serious consequences including punitive actions. Additional laws and policies may govern the use of information from federal, state, and local jurisdictions.

# Scope

This Acceptance Use Policy (AUP) applies to all users granted access to *“Application Name”* managed by the Department of Health and defines the system custodianship responsibilities. This further applies to all associated technology designed to support or use information retrieved from the system for further processing.

# System Administrator Responsibilities

1. Conduct periodic reviews of access logs and provide report to ISO on a quarterly basis.
2. Maintain appropriate security controls of the *“Application Name”* system to ensure the secure processing of information is maintained. (up to Category 4 data)
3. Comply with OCIO online file storage principles and guidelines (<https://ocio.wa.gov/online-file-storage-guidance>)
4. If users will be accessing *“Application Name”* Cat3+ environment multifactor authentication must be enabled.

# Individual Rights and Responsibility

* 1. Understanding. I understand that I have the primary responsibility to create or process appropriate information into *“Application Name”* according to authorized use, modification, disclosure, and destruction, as outline below.
	2. Revocability. Access to *“Application Name”* is a revocable privilege by the Department of Health and all information is subject to monitoring and auditing as established within the Information Governance Program.

# User Conditions

* 1. You may use only *“Application Name”* and information assets for which you have authorization.
	2. You may not use another individual's account or attempt to capture or guess other users' passwords.
	3. You are individually responsible for the appropriate information (content or data) captured or created, used, disclosed, or destroyed in the system. Information shared outside of the system external to the Department of Health, must utilize a data sharing agreement (DSA).
	4. The Department of Health is bound by its contractual and license agreements; you are expected to comply with all such agreements when using the system.
	5. You should make a reasonable effort to protect your passwords and to secure credentials against unauthorized use.
	6. External *“Application Name”* access requires multi factor authentication along with passwords to be a minimum of 8 characters long and contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
	7. You must not attempt to access restricted portions of the system or other connected applications that support the system without appropriate authorization by the system owner or administrator. All user actions are logged and monitored.
	8. You must comply with the policies and guidelines for any other information system you have been granted access connected to *“Application Name.”* When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
	9. You must only capture or create appropriate information within *“Application Name,”* according to defined business purposes. This system is only approved for processing transient (non-record) or duplicate information already stored in an approved DOH repository. It is unacceptable to place business records in this system that are defined as official records that require specific preservation requirements to protect their authenticity, reliability, and integrity.
	10. *“Application Name”* **is not** considered a system of record. You must transfer all official records, if they are created in the course of business activities within 30 days to an approved information repository. This system has limited ability to enforce retention as outlined in RCW 40.14, within the State General Government Retention Schedule or the DOH Unique Retention Schedule, or according to Information Governance information handling standards.
	11. The use of the “Application Name” application on state owned mobile devices or BYOD’s is not permitted at this time. (This capability is being considered for future deployment)

# Privacy and Personal Rights

* 1. All users of *“Application Name”* are expected to respect the privacy and personal rights of others.
	2. Be professional and respectful when using *“Application Name”* to communicate with others. All users should;
		1. Be as accurate as possible and take the same level of care as they would when creating other formal written communication representing DOH and the State of Washington,
		2. Not open any electronic message from a sender that is not known or having a reasonable suspicion of threat,

Not include information that is misleading, inaccurate, disparaging, fraudulent, harassing, embarrassing, explicit, profane, intimidating, defamatory, or anything else that may be considered inappropriate.

|  |  |  |
| --- | --- | --- |
| *“Application Name”* Acceptable Use Policy owner: Information Governance Officer: Jesse Hayes  |  | Date AUP Approved: 12/28/20 |
|  |  | Next AUP review: 01/01/21 |