Guidelines for Organizing Electronic Records

In compliance with WAC 434-662-040, Military Department electronic records must be retained in electronic format and remain usable, searchable, retrievable, and authentic for the length of the designated retention period that fall under one of the following records retention schedules:

State Government General Records Retention Schedule

Military Department Records Retention Schedule

Public Schools (K-12) Records Retention Schedule (Youth Academy School Records)

The Military Department is required to protect data that is specifically protected from public disclosure in compliance with OCIO Standard No. 141.10, Securing Information Technology Assets that include the following four categories:

- **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.

- **Category 3 – Confidential 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) Lists of individuals for commercial purposes as defined in RCW 42.56.070 (8).
  d) Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

- **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:

  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.

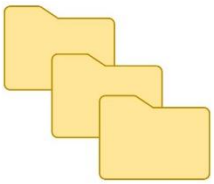
Procedure

1. Identify the location to store the records.

   The Military Department's Information Technology Division has approved the following platforms, software, and classifications for storing electronic records:

   - *SharePoint Online* – Approved for up to Category 3 data for internal, and up to Category 2 data external.
   - *On prem server shared drives* – On prem server shared drives can go to Category 4 but require additional provisions to store Category 4 data. If you plan on storing Category 4 data here, please notify IT first before proceeding.
   - *WISE* – The WISE is currently certified to go to Category 2 data.
   - *OneDrive* – approved for Category 3 and can only be utilized internal.
   - *Teams* – Approved for up to Category 3 internal, and Category 2 external.
   - *Email* – Approved up to Category 4 but will require encryption and certain provision done by IT for Category 4.
   - *Computer hard drive* – Up to Category 3 with encryption for temporary storage, not approved for long term data storage.

2. Create the folder for storing the records. The limit for creating hierarchies is three-folders deep.



3. The record name should be one that is short (under 255 characters) and easy for users to identify.

4. The following special characters already have specific tasks in an electronic environment and should not be used when naming a record:

   \ /: * ? " < > | [] & $, .

5. Use underscores between words or capitalize the first letter of each word.

   Example 1: file_naming_convention

   Example 2: FileNamingConvention