Content Manager (CM) Guide

Security and Access

Content Manager (CM) is a DoD 5015.2 certified system. DoD (Department of Defense) 5015.2 is a federal government standard for electronic records management systems, which is also approved and recommended by NARA (National Archives and Records Administration). Among many other things, the standard describes the minimum setup for security and access to government records stored in an electronic records management system.

Content Manager (CM) is also compliant with CJIS (Criminal Justice Information Services) and HIPAA (Health Insurance Portability and Accountability Act) standards. All Content Manager administrators are also CJIS-certified.

What does this mean?

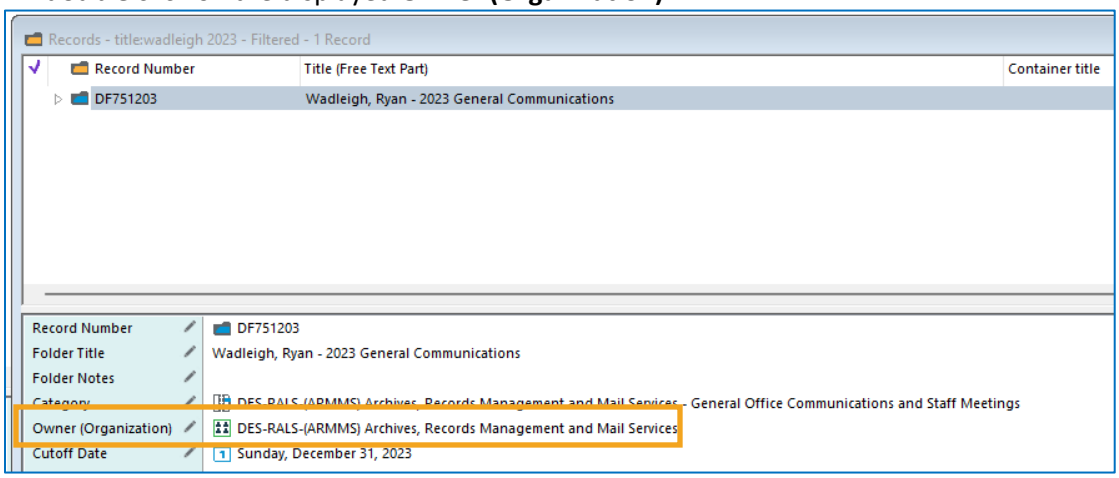
All records filed to Content Manager are stored according to the highest security standards for government agencies in the United States. Content Manager *can* be used to store sensitive information, including but not limited to PII (Personally Identifiable Information) and PHI (Protected health information) - *see definitions at the bottom of this document*.

Who can access records I file to Content Manager?

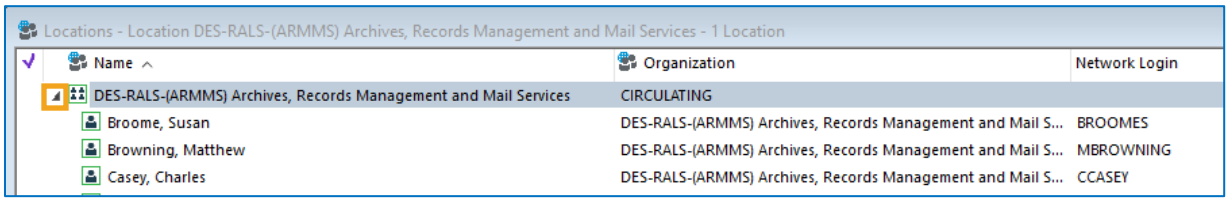
Any records you file to Content Manager are only accessible by other employees who are members of the **Owner (Organization)** where the records are filed. The Owner (Organization) setup varies across the county, but the most common setup is to have an Owner (Organization) for each **section** of the county's government. You can verify exactly who has access to a record in CM by performing these steps:

1 – locate a record in CM and navigate to the bottom details pane

2 – **double click** on the displayed **Owner (Organization)**



3 – In the next window, single **click** the **tiny triangle** to the left of the organization name to display the complete list of all staff with access



The exception to this is individual categories with "Restricted Access" (Modified Security) which are identified with **[Restricted Access]** as part of their category title. For these, you can verify who has access to records by double clicking on the **Category** from the record's bottom details pane. Then in the next window, navigate to **Access Control** in the bottom details pane to see a complete list of staff with access to that specific category.

The only *other* exceptions are the CJIS-certified Records Management Program staff who have access to *all* records in the system, as well Public Records Officers who have access to certain areas of the system under their purview in order to respond to public records requests.

How can I restrict access to certain records?

If any records need to be restricted to a smaller number of people, we can accomplish that by restricting individual categories. To accomplish that, email records.management@kingcounty.gov and include 1) which category(ies) needs to be restricted and 2) which employees need access to that category.

Note that if you decide to restrict access to certain categories, it is your responsibility to let us know who should be added to or removed from access to that category over time.

It is **not** possible to restrict access to individual records in CM.

What are my responsibilities?

As a county employee, you should be mindful about privacy whenever you create records. It is good practice to avoid creating records that have sensitive or private information, unless necessary for your job.

If you do have records with sensitive information, they should be managed with security in mind. If they do not have retention value, they should be deleted as transitory. But if they have retention value, they should be handled thoughtfully and securely. If you are filing records to Content Manager, be mindful about what you are filing and avoid filing records that others should not see.

Security and Access

Be mindful about which staff have access to different areas of Content Manager and inform Records Management when any staff need to be added or removed to any Owner (Organization) or Restricted Category in Content Manager.

Also remember that transparency is a benefit to the public we serve every day. Although certain records are sensitive and should be restricted from unlawful access, our public records should be as open and accessible as possible.

What records are sensitive or private?

Each of us has a unique role as part of King County government, and we maintain a large variety of records. Because of that, there is **not** a black-and-white answer to which of our records are sensitive or private. Below are some definitions that *can* apply to county records.

Personally Identifiable Information (PII) – "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." (NIST SP 800-122).

Protected health information (PHI) – "individually identifiable health information" regardless of its format; except for certain educational records and employment records held by an employer and records about a person (NIST SP 800-66 Rev. 1).

Essentially, this can include any records that have a **person's full name** in addition to certain bits of information, including **social security number**, **date and place of birth**, **mother's maiden name**, **medical/health information**, **financial information**, and **many more**.

Certain records might also be exempt from *public* disclosure under the Public Records Act. For information about records that might be exempt from public disclosure, reach out to your Public Records Officer.