



Records Management Handbook and Retention Schedule

Adopted February 3, 2020

Amended October 14, 2026 [Proposed, Not Yet Adopted]

Introduction

This Handbook has been developed with reference to the State Records Management Program (Government Code ~~§ 14745~~ **§§ 12270–12279**), which governs records management practices for Executive Branch State agencies. While local governments, including special districts such as the Crescent City Harbor District (CCHD), are not required to follow the program, it nonetheless offers a useful framework for developing internal best practices. **The District’s authority to destroy or dispose of its records, and the categories of records that may not be destroyed, are governed by Government Code § 60201, which applies to special districts.**

While informed by these State-level standards, the guidelines in this Handbook have been deliberately simplified to establish a program that is manageable given CCHD’s limited resources. They are intended to offer structure and consistency to CCHD’s records management practices. Furthermore, this Handbook includes a records retention schedule to guide staff in determining how long specific types of records should be retained before they are eligible for disposition.

Definitions

- **Active Records** - Records that are referred to at least once a month per cubic foot of records.
- **Administrative Records** - Records commonly found in all offices and typically retained only for short time periods.
- **Archival Records** - Records with enduring value because they reflect significant historical events, document the history and development of an agency, or provide valuable research data.
- **Essential Records** - Information that is essential for the continuation or reconstruction of the organization during or immediately following a crisis.
- **Non-Records** - Material kept only for convenience or for reference in the preparation of actual records.
- **Permanent Records** - Records that are required in perpetuity, usually identified by statute or other written guidance.
- **Perpetual Records** - Records retained for an indefinite period of time and then stored or destroyed after some qualifying event takes place.
- **Program Records** - Records that relate to the primary function of the agency in response to its daily mission.
- **Protected Records** - Records that are explicitly prohibited from being destroyed, except under specific conditions identified by statute.
- **Records Retention Schedule** - An agency’s authority to retain and dispose of official records. It documents which records should be destroyed because they no longer have any administrative value.

Save Space, Time, and Money

Unless records are regularly disposed of, CCHD will run out of physical storage space or incur increased costs for record storage. Also, the more records an agency retains, the more time it takes staff to search for records that are actually needed in the course of daily business. CCHD should ensure only the records with a high reference status are retained.

While it may seem like electronic records have an endless storage capacity, there are repercussions for needlessly retaining a high volume of electronic records. Cloud storage, server space, Information Technology staff time, as well as the maintenance and security of—and access to—electronic documents all factor into the cost of storing electronic records. Staff time should not be spent digging through filing cabinets or shared drives that are stuffed to the brim with records that have far surpassed retention so that they can access the information they need to complete their daily work. Disposing of records improves workflow!

Except for perpetual records, most administrative records should only be kept two years or less. Transitory records are typically not retained at all, or kept only briefly before being discarded. An effective records management program doesn't cost—it pays. It pays by improving customer service, increasing staff efficiency, and better allocating scarce resources.

Questions to ask are: How serious would it be if a record were unavailable? Are the consequences serious enough to justify keeping a large volume of records for long periods of time at considerable cost? Don't accept the answer that "the records are used all the time and therefore must be kept permanently." "Permanent" retention is very expensive, rarely necessary, and usually must be justified by a specific written requirement such as a statute or Government Code.

In general, most agencies keep records well beyond the record's administrative value "just in case" the records may be desired for future purposes. That is one of the worst reasons to retain records because excess records overburden staff and slow response times to public records requests. Records Management's primary concern is the efficient, effective, and economical management of information. The guiding principle is to ensure that information is available when and where it is needed.

Electronic Records

There are two main categories of electronic records: born digital records and digitized records. Born digital records are those records created with a computer that require a computer to be readable by people, such as a Word document, PDF file, an online post, or even emails sent. A digitized record is one that is born analog (paper) and has been converted into a machine-readable format using a scanner or camera, such as a scanned version of a paper record. For the purposes of this Handbook, electronic records refers to both types.

Electronic records are not considered a record series or category on their own. "Electronic" is simply a format. Electronic records should be organized based on the information they contain and the purpose they serve. For example, email systems should be organized so that email messages

can be placed in electronic folders and arranged in a consistent pattern reflecting the ways in which records are used and referenced.

Electronic/Digital Security

CCHD recognizes that electronic records and other information assets must be appropriately managed and protected according to their sensitivity and value. This section applies to CCHD information assets, including paper records, electronic records, transported data, stored data, hardware, and software.

CCHD will use its existing hardware, software, and other information technology resources to support electronic and digital security. The goal is to maintain appropriate oversight of CCHD information assets and strengthen the overall security of District information systems.

Asset, Change, and Configuration Management

CCHD will maintain an inventory of information technology assets to support effective cybersecurity management. Asset inventories should be reviewed and updated as appropriate. Changes to systems should be monitored, and hardware and software configurations should be managed in a manner that supports the security and reliability of CCHD information systems.

CCHD currently manages authorized devices connected to its network and performs ongoing network scans for unauthorized devices. Knowing what devices are connected to the CCHD network, where they are located physically and logically, their purpose, and who is responsible for them assists CCHD in identifying unauthorized or malicious devices and responding to security incidents.

Software and Secure Configuration Management

CCHD will monitor, maintain, and update approved software to help ensure that software is appropriately installed and maintained. The goal is to limit CCHD systems to authorized software in order to reduce the risk of malware, illicit or unwanted activity, and copyright violations.

CCHD will maintain secure and supportable base configurations for hardware and software and use available tools and techniques to identify changes that may create vulnerabilities or system support problems.

Threat and Vulnerability Management

CCHD will gather cybersecurity threat and vulnerability information from appropriate external sources, including government advisories, industry reports, and information provided by suppliers. CCHD will assess this information for relevance to District systems and operations and use applicable information to inform cybersecurity risk management and the prioritization of security measures.

CCHD will identify and catalog District information assets, including applicable hardware, software, and data. Tools and techniques such as vulnerability scanning, penetration testing, and manual assessments may be used to identify potential weaknesses. Identified vulnerabilities will be

evaluated based on their potential impact and likelihood so that remediation efforts may be prioritized according to risk.

Third-Party Cybersecurity Monitoring

CCHD will maintain processes for ongoing monitoring and reassessment of cybersecurity threats and vulnerabilities as systems, projects, and identified risks change. As appropriate, CCHD may contract with an outside firm to assist with monitoring cybersecurity threats and vulnerabilities affecting District digital systems and assets.

Transitory Records

Transitory records are created primarily for the communication of information as opposed to the perpetuation or formalization of institutional knowledge. Specific examples of transitory records include, but are not limited to: transmittal letters, acknowledgments, preliminary calculations, scheduling communications, non-substantive follow-up communications or reminders, and similar communications that provide information of a short-lived value. Additional specific examples of transitory records are: drafts, notes, instant messages, text messages, emails, records not kept in the ordinary course of business, and certain records not intended for public distribution. The value of these records is comparatively short-lived and these types of records may be discarded when they have fulfilled the brief, limited purpose for which they were created.

Typically, communications such as instant messages, text messages, and emails are considered presumptive draft materials for records management purposes. This is because they are generally transitory or ephemeral in nature, often composed with unrefined or preliminary language, not intended for public distribution, and not intended for long-term retention or formal reference. These communications are generally used for informal internal deliberations, preliminary discussions, or routine administrative matters and, as such, are not ordinarily retained in the normal course of business.

However, when such communications document or memorialize a formal substantive action, such as a policy directive or formal management decision, they must be retained. **Communications that document a Federal or State grant procurement, contractor selection, approval, expenditure, reimbursement request, matching contribution, material project decision, compliance determination, monitoring action, or other action supporting administration of a grant-funded activity are not transitory records and must be retained with the applicable grant file.** In such cases, the communication should be exported or converted into CCHD's designated archival format (searchable text file) and stored ~~on CCHD file servers~~ **in CCHD's server-based recordkeeping system.** These records should no longer be treated as transitory or draft material. Additional retention guidance for such records is provided in the retention schedule included in this Handbook.

Email Policies

When it comes to emails, records management often begins with subject lines, which can be critical for both the recipient and sender in identifying and filing messages. Subject lines should be unambiguous and as descriptive as possible so that records are more accessible and searchable.

Poor or Confusing Subject Lines:	Better, Descriptive Subject Lines:
"Helpful Info"	"Contact Info"
"Report"	"Quarterly Financial Report"
"News"	"January 2001 Board Minutes"
"Minutes"	"Revised Administrative Procedures"
"Important"	"New Agency Head Appointed"
"Contract Status"	"PO 12345 Delivery Status"

File Naming Conventions

A file name is the key identifier of a digital object and provides metadata for the record. Consistent and descriptive file names will provide a more organized and easily understood collection of records. How a file is named will have a large impact on finding the files at a later date and understanding their contents. The following should be considered when creating a file name, although ultimately file names should reflect the purpose and need of the record: project name, publication date, creation date, description of content, record series, version number, department, and name of creator.

When creating a file name, the following should also be considered:

- Create unique file names.
- File names should be easy to understand, and not overly complex.
- Do not use spaces but rather () or (-) to represent a space.
- Avoid using special characters such as \$ # @ & ^ % * ! and use only alpha-numeric characters.
- Limit file names to 25 characters or less.
- Use the three-character file extension with a period (e.g., .tif not .tiff) at the end of the name.
- Do not rely on the system to differentiate between upper and lower case and be consistent in what is used.
- If digits are included in the file name, include the appropriate number of leading zeros so that file names can be scalable.
- It is helpful to include metadata in the file name but consider using shortened versions of 1) a standardized date, 2) version number (only if this can/will vary), 3) creator's name, and 4) description/type of document/subject in the file name and in a logical order.

- Document whatever naming convention is chosen. Include the naming convention document any time records are transferred elsewhere.

Considerations Before Digitizing

Digitizing records can enhance accessibility, workflow, and productivity, but digital imaging projects can also be complex, time-consuming, and sometimes cost prohibitive. Before beginning any scanning or digitization project, the following are some of the questions that should be addressed:

- What are the goals for the digitization project?
- What is the desired end result?
 - A document management system?
 - Document preservation?
 - Online search capabilities to facilitate better access to records?
- What materials will be digitized?
 - Textual documents, photographs, or maps?
- How much material?
- What resources are readily available?
 - Will the records be scanned in-house? Do you need scanners? Software? Expertise?
- What file formats are most suitable for your records?
- What image quality is required?
 - Black and white? High resolution? What condition are the documents in?
- Is preparation required (e.g., removing staples and paperclips)?
- What different type(s) of digital storage media will be used?
- What metadata is necessary for each file?
 - Is the metadata readily available or is time needed to gather information?
- How will access be provided to the digital records?
 - Intranet or internet? Offline? DVD, CD, hard drive?
- How long will the digital files be retained?
- Will hard-copy documents be kept? What is considered the original?

Digitization Standards

During digitization, the spatial resolution and image dimensions determine the total number of pixels in an image file. For example, an 8" x 10" photograph scanned at 100 ppi produces an image that has 800 pixels by 1,000 pixels or a total of 800,000 pixels. Increasing resolution increases the total number of pixels, and results in a larger file size. Higher resolution will generally render more

fine detail of the original in the digital image, but not always. The actual rendition of fine detail is more dependent on the spatial frequency response of the scanner or digital camera, the image processing applied, and the characteristics of the item being scanned. Also, depending on the intended usage of the production master files, there may be a practical limit to how much fine detail is actually needed.

Records Retention Schedule

How long CCHD will maintain custody of records depends on the operational needs of the record. Maintenance of records can be just as costly and time consuming as creating the records in the first place. Retention periods are primarily based on the functional value of the records, rather than the format or media type. The primary administrative use for most records is exhausted when the transactions to which they relate have been completed. From that point on, the records begin to lose their administrative value, and disposition should be considered.

This Records Retention Schedule has been prepared with reference to the Local Government Records Management Guidelines published by the Secretary of State pursuant to Government Code § 12236 and is adopted by resolution of the Board of Harbor Commissioners as the District's record retention schedule pursuant to Government Code § 60201(b)(2). For that purpose, this Schedule classifies all records of the District, in any format, into the following categories, each of which is described in this Handbook: (1) transitory records, including communications exchanged through instant messaging and internal collaboration platforms, text messages, and emails that do not document a formal substantive action; (2) long-term retention records; (3) Federal award records; (4) protected records; and (5) general administrative records. Essential records are not a separate retention category; they are records within any of these categories that have been designated for the additional protections described in the Essential/Vital Records section of this Handbook. Where a record falls within more than one category, the longest applicable retention period controls.

General administrative records are all records of the District that do not fall within categories (1) through (4), including administrative records and program records not otherwise classified in this Handbook. General administrative records shall be retained for one year from their creation or receipt by the District, whichever is longer, or for such other longer period as may be required by applicable Federal or State law or regulation, the terms of a grant or contract, or another provision of this Handbook, and in all cases until they have served the administrative, fiscal, or legal purpose for which they were created or received. Thereafter, general administrative records may be destroyed in accordance with the standard destruction protocol set out in the Record Dispositioning and Protected Records section of this Handbook.

Instant Messages and Other Internal Messaging Platforms

There is a growing use of real-time messaging platforms designed for internal collaboration and productivity. These applications, commonly structured as team-based chat environments, are used to facilitate informal, iterative, and often spontaneous exchanges of information between staff.

Examples of such platforms include, but are not limited to, Microsoft Teams, Slack, or any application with comparable functionality.

Communications exchanged via these platforms typically fall into the category of transitory non-records. This is because these communications have the following characteristics:

- **Dynamic and modifiable:** Users may edit or delete content at any time, which may remove the content for all users. Messages may be revised multiple times before any definitive information is formally recorded elsewhere.
- **Not retained in the ordinary course of business:** These platforms are not used as the final or official repository for records. Instead, they serve as digital “whiteboards” or working notes for internal deliberation.
- **Not relied upon for agency decisions or policy:** Final decisions, directives, and approvals are captured in more permanent forms such as formal reports, memoranda, or meeting minutes.

Accordingly, message-type internal communications are considered non-substantive, transitory drafts and, unless a specific message is intentionally preserved in another format to document an agency decision or action, these communications are non-records that may be discarded at the discretion of the user once their temporary utility has expired. **This discretion is subject to the retention requirements for grant-related and other substantive communications set out in the Transitory Records and Record Dispositioning and Protected Records sections of this Handbook.**

Text Messages and Emails

While instant messages and internal collaboration tools typically represent the most ephemeral and transitory forms of electronic communication, text messages and emails can sometimes be considered less transient, requiring a greater degree of care and judgment when evaluating their retention value.

Text messages and emails that document or memorialize a formal substantive action, such as a policy directive or formal management decision, should be transferred to CCHD’s server-based recordkeeping system in ~~text file format~~ **CCHD’s designated archival format (searchable text file)**. Otherwise, text messages and emails can be retained at the discretion of the user, typically until it becomes clear that their administrative or informational value has expired. Users should regularly assess their stored messages to avoid unnecessary accumulation, preserving only what directly supports business needs.

Examples of substantive content that should be preserved:

- Confirmation of critical decisions or approvals.
- Instructions related to financial transactions.
- Discussions with external entities influencing District policy.

Routine operational texts and emails pertaining to short-lived informational exchanges may be deleted once their immediate utility ceases, at user discretion. **This discretion is likewise subject to**

the retention requirements for grant-related and other substantive communications set out in the Transitory Records and Record Dispositioning and Protected Records sections of this Handbook.

Long-Term Retention Records

Some records contain basic facts concerning CCHD's origin, policies, functions, and organization, and fall into the category of program records. These records should generally be preserved indefinitely to provide documentation of CCHD's operations in the past, present, and future.

Some examples of records that should be preserved indefinitely as archival records include:

- Agreements, including leases, titles, and contracts.
- Meeting minutes.
- Budgets, ledgers, allotments, payrolls, and vouchers.

Federal Award Records

Records related to Federal awards and grant-funded activities, including financial records, supporting documentation, procurement and contract records, invoices, reimbursement and match documentation, reports, and other records supporting the administration of a Federal award, shall be retained in accordance with applicable Federal requirements.

At a minimum, Federal award records shall be retained for three years after the date of submission of the final financial report for the applicable Federal award. Records relating to real property and equipment acquired with Federal funds shall be retained for three years after final disposition of the property or equipment. A longer retention period shall apply when required by the terms and conditions of the Federal award, applicable State or local law or regulation, or another provision of the District's Records Management Handbook and Retention Schedule, or when the District is notified in writing by the Federal awarding agency, pass-through entity, or cognizant or oversight agency for audit or indirect costs that the retention period has been extended.

Federal award records shall not be destroyed while an audit, monitoring or compliance review, litigation, claim, investigation, or other matter involving the records remains unresolved.

CCHD shall provide the applicable Federal awarding agency, pass-through entity, Federal Inspector General, Comptroller General of the United States, and their authorized representatives timely and reasonable access to Federal award records when required by 2 C.F.R. Part 200 or the applicable award, including access necessary for audits, examinations, excerpts, transcripts, monitoring, and compliance reviews. No provision of this Handbook authorizes destruction or withholding of a record during a period in which such access or preservation is required.

Essential/Vital Records

CCHD should identify records essential to the functioning of government in the event of a major disaster. Essential records (previously known as vital records) are the recorded information that is essential for the continuation or reconstruction of the organization during or immediately following a crisis. Some examples can include accounts receivable information, fire insurance policies, ~~research and development files,~~ and major contracts and agreements.

Such records are necessary to continue operations without delay under abnormal conditions, and these should be offered additional protections so that essential information is available in the event of a disaster or emergency where records may be unavailable for reference or lost during the event.

It is very important for CCHD staff to be particular and specific when they are identifying their essential records to ensure that they contain the correct information needed in the case of emergency where other agency records are unavailable. Essential records help the agency continue business processes to the public, or other entities they work with, as soon as the following day after an emergency or disaster has occurred. Essential records must remain accessible and usable while still being secure.

Essential records must be stored in one or more of the following ways:

- Cloud storage.
- Duplicate copy stored at least twenty miles from the main office.
- Fireproof safe located in the office.

There are two categories of essential records:

1. **Emergency Operating Records** - records that an organization needs to continue functioning or to reconstitute after an emergency. Examples include:
 - Emergency plans and directive(s) which specify how an agency will respond to an emergency.
 - Orders of succession.
 - Delegations of authority.
 - Staffing assignments.
 - Selected program records needed to continue the most critical agency operations under emergency conditions and to resume normal operations after an emergency.
2. **Financial Rights Records** - records needed to protect the financial rights of the ~~Government~~ **District** and of the individuals directly affected by its activities. Examples include:
 - Accounts receivable records.
 - Licenses and long-term permits.
 - Payroll records.

- Insurance records.
- Titles, deeds, and contracts.
- Retirement records.
- ~~Military service~~ **Personnel** and medical records.

The 3-2-1 Rule

One method for protecting essential records is the 3-2-1 rule. While the 3-2-1 rule is an ideal arrangement for storing essential records, it may not always be possible. Taking the time to duplicate a record into a second media type may be impractical for program staff who are busy creating and using the records. Best practices, however, still require three copies and some physical separation between those copies.

1. Keep **three** copies of any important file—a primary and two backups.
2. Keep the files on **two** different media types (such as paper and cloud storage) to protect against different types of hazards.
3. Keep **one** copy stored offsite.

The Importance of Managing Essential Records

If essential records are managed properly, CCHD is protected. In the event of an emergency or disaster, those records have been protected properly, so it will be ~~clear~~ **easy** for agency staff to find them when needed either before, during, or after the event has occurred.

If essential records are not managed properly, CCHD may be exposed to risks such as noncompliance, loss of asset value, and high costs associated with restoration and duplication of essential information that has been lost.

While essential records may be stored for lengthy periods of time, records should be classified as essential only so long as they support critical business processes. When records lose their essential status, they should be reclassified. Alternatively, if an essential record has been updated with current information, it is incredibly important to ensure that staff are cycling (or replacing the outdated essential record copy with the updated copy) these records.

Storing Confidential Information

When discussing records security and storage, it's important to consider whether the records contain confidential information, including personal information, tax information, or medical information. If so, this sensitive information may require additional protection. Once confidential information has been communicated to the intended recipient, it may be advisable to destroy the record to avoid the risk of unauthorized disclosure.

Record Dispositioning and Protected Records

A record may be dispositioned when it has reached the end of its useful value to CCHD and it is not considered a “protected record.” Various categories of protected records are described below, along with any applicable retention periods required by statute.

Protected records include:

- Records related to the formation or reorganization of the District, as well as adopted ordinances, are all considered permanent records. While ordinances that have been repealed, invalidated, or rendered unenforceable may be destroyed, this can only occur five years after they became inactive.
- Official minutes from any meeting of the Board of Harbor Commissioners are also considered permanent records and must be preserved indefinitely.
- Records connected to any active claim, pending litigation, or a settlement concluded within the past two years must be retained.
- Records that are the subject of a pending Public Records Act (PRA) request cannot be destroyed until the request has either been fulfilled or at least two years have passed since the District formally denied the request in writing.
- Records related to pending construction projects, unresolved stop notices, or projects not yet completed and accepted by the District must also be preserved during the pendency of the activity. Likewise, documents tied to outstanding financial obligations, real property interests, or active contracts are not eligible for destruction.
- Unaccepted bids or proposals for construction work that are less than two years old.
- Records showing payments to District employees, officers, or independent contractors—including those related to expense reimbursements, travel payments, or use of District-issued credit cards—must be retained for at least seven years from the date of payment before they can be destroyed.

More generally, no record should be disposed of if it has not yet served the administrative, legal, or financial purpose for which it was created.

Disposition of records may entail destroying paper or electronic records, and confidentially shredding records. While there may be some reluctance to destroy records, CCHD would be overwhelmed with records that are no longer useful to conduct business. Records may be destroyed by in-house recycling, shredding, confidential destruction, or through a contracted vendor.

The following standard protocol applies to the destruction of District records. Before a record is destroyed, it shall be confirmed that (1) the retention period applicable to the record’s category under this Handbook has expired and (2) the record is not a protected record and is not subject to a pending claim, litigation, litigation hold, audit, investigation, Public Records Act request, or Federal award retention or access requirement. Records containing confidential information shall be destroyed by shredding or another method that renders the information unreadable.

The authority to determine whether a record is no longer required for retention depends in part on the nature of the communication. For team collaboration and real-time internal messaging platforms (e.g., Microsoft Teams, Slack), messages are generally considered transitory and non-record material unless a user affirmatively preserves a message, such as by exporting or integrating it into a report, directive or other formal record. ~~These platforms are not designed for long term recordkeeping, and users may freely delete, revise, or purge such messages unless a specific communication has been identified for retention.~~ they document a substantive District action or otherwise fall within a retention category in this Handbook. Users may not delete, revise, or purge a communication that documents a grant procurement, approval, expenditure, reimbursement or match, material project decision, compliance action, audit or monitoring matter, litigation hold, or other record required to be retained by law, an applicable funding agreement, or District policy. Such communications must be preserved in the District's server-based recordkeeping system.

The decision on retention of other types of communications may be made by any of the following: Division Manager, Deputy Harbormaster, CEO/Harbormaster, or the Board of Harbor Commissioners, taking into consideration the principles and guidance outlined in this Handbook.