Document Organization System

Draft Edition

First Final Draft
Version: 0.8.0

Tyler Morgan
DOS@tylermorgan.co
https://orcid.org/0009-0006-9819-6065

Updated: April 22nd, 2024

⚠ This document is currently undergoing drafting, and the information might change before publication. Please reference this document at your own risk.

Abstract

This document delineates methodologies for how individuals should file and organize digital and physical documents, informative information, folders/folios, booklets, cards, vaults, and other sensitive documentation. Although primarily designed for individuals in the United States, it can be modified to suit the needs of individuals in other countries.

The general populace deserves possession of their important documents on demand while securely storing their information using recommended practices. This specification delineates document organization security and consistency, ensuring easy access while minimizing physical and online threats.

Document Status

This document and helpful examples reside within the DOS GitHub repository. Feedback and comments on this specification are welcome and facilitated through GitHub issues. Access the most recent version of this document via GitHub, which links to the README.md file. Alternatively, locate the latest publication of this document at https://tylermorgan.co/DOS.

Publication location may change in future iterations of this document.

This version:
https://tylermorgan.co/docs/dos/0.8.0-20240422.pdf

Latest published version:
https://tylermorgan.co/DOS

Previous versions:
https://tylermorgan.co/docs/dos/FDHT-20231204.pdf

Table of Contents

1 - Document Classes

Each document in the standard will be considered and organized into a document class code. The first character identifies the document medium class (§ 1.1) and the second character identifies the document sensitivity class (§ 1.2), e.g., D4.

1.1 - Medium Classes

In this document, any references to the medium class code alone (eg., Class D) considers all sensitivity classes (1-5).

1.1.1 - Class P (Physical) Documents (P1-P5)

- Paper or material documents that were issued to the document owner (acquirer) at least once in the past or are expected to be issued to the document owner in the future.
- Documents that can be issued online but were also physically issued to the document owner will still be considered a physical document, e.g., U.S. Selective Service System Registration Acknowledgements.
- Scanned P-class documents will still be considered P-class.

1.1.2 - Class D (Digital) Documents (D1-D5)

- Natively digital documents that were never issued and will never be issued through a physical medium, e.g., online certificates.
- Documents created digitally for translational purposes will be considered a class D document, e.g., translated birth certificates.

1.1.3 - Class I (Informative) Documents (I1-I5)

- Informative numbers or other information that was never or will never be attached to a digitally or physically issued document.
    - For example: TSA PreCheck/Global Entry Known Traveler Numbers (KTN)
- If information was obtained from a class P5 or D5 document (§ 1.2) but the actual document file wasn't obtained. Do not consider the document as class I, consider them as their original medium class.

1.2 - Sensitivity Classes

In this document, any references to the sensitivity class code alone (e.g., Class 2-5) considers all medium classes (P, D, and I).

1.2.1 - Class 1 Documents (P1, D1, I1) – Completely confidential

- Credential Manager Logins
- Other High-Security Logins that Cannot be Saved in a Credential Manager

- Financial Records - One owner eyes only

1.2.2 - Class 2 Documents (P2, D2, I2) – Confidential outside household members and authority personnel

- Social Security Administration (SSA) Cards
- Passports/Passport Cards
- Certificates of Naturalization
- U.S. Permanent Resident Cards
- Financial Documents/Cards
- Other Documents that Reveal Full or Partial SSA Number
    - Any class 3-4 documents listed that contain an SSA number should be considered a class 2 document.
- Tax Documents

1.2.3 - Class 3 Documents (P3, D3, I3) – Confidential with exception

- Birth Certificates
- Marriage Licenses
- Vehicle and Estate Titles
- Immunization/Medical Records
- Selective Service System Registration Acknowledgements
- Other Somewhat Sensitive State-Issued Licenses
- Pet Adoption Certificates
- Pet Immunization/Medical Records

1.2.4 - Class 4 Documents (P4, D4, I4) – Tentatively shareable

- Educational Diplomas
- Important Receipts
- Important Letters
- TSA PreCheck Known Traveler Numbers
- Global Entry Cards
- Non-Sensitive Membership Documents/Cards
- Emotional Support Animal Letters
- Insurance Cards

1.2.5 - Class 5 Documents (P5, D5, I5) – All class 2-4 documents where there is no ownership within the household

- Class 5 documents should never be stored physically within the household unless requested by the owner and a proper POA is filed as stated under § 6.5 and § 7.13. In this case, if the owner wishes to follow the DOS, the document will no longer be considered class 5 and will fall between 2-4 classes depending on the document.

If a household individual would like to add a document that is not directly listed in § 1.2 of this standard, consider which classes the document belongs to and follow the standard outlined for those document classes.

For pet documents, document ownership belongs to the pet owner and receives exemptions for digital vaults (more in § 3.3) and document sorting (more in § 2.4).

Class 1 documents can only be shared with a properly notarized POA as defined by § 6.5 and § 7.13.

1.3 - Document Classification Table

	Class 1	Class 2	Class 3	Class 4	Class 5
Class P	P1	P2	P3	P4	P5
Class D	D1	D2	D3	D4	D5
Class I	I1	I2	I3	I4	I5

2 - Physical Locations

2.1 - Vaults

The terms safes, strongboxes, and vaults will be referred to as ("vaults"). In ideal situations, each person in the household should have access to their own personal vault to store class 1 documents. A large, shared vault will place all class 2-4 documents. The shared vault must be accessible to everyone residing in the household. Only vaults that have a keypad or biometric scanning may be used. Access to vaults secured by keypads should only be granted through randomly generated PINs, and not through familiar or known combinations (such as the last four digits of a Social Security Number, phone number, special dates, etc.). Repeat PINs are not allowed. In ideal cases, vaults will be bolted to the floor or wall using three or more mounting bolts. For renters, contact the management company/landlord for best practices and approval.

Each vault will have its own identification number (ID) (e.g., **V-497138-MP202308**):

- V- – Standing for *vault*. Followed by a hyphen.
- 000000- – Random unique number. Must be unused by ALL past and current identifiers for both folios and vaults. Followed by a hyphen.
- AA – The first letter of each last name that owns documents in that location. Sorted alphabetically. Different last names that have the same first letter will be condensed. Can be one or more letters.
- YYYYMM – The year the vault ID was created (four numbers). Followed by the month the vault ID was created (two numbers).

These codes will be stickered on each vault in plain sight and readable whether open or closed. Each document's digital copy will be labeled with the vault ID number the document is stored in. All new or replaced vaults must obtain a new unused ID number. If ownership of a document changes locations to where the last name ID section doesn't match, a new ID will need to be obtained and updated across all digital locations and documents. All IDs labeled on vaults must be printed in black Arial fourteen-point bolded font on a white or light-colored background.

2.2 - Folios

All vaults must have at least one folio organizer for each sensitivity class stored in the vault. I.e., personal vaults for class 1 documents should have at least one folio organizer. Vaults for class 2-4 documents should have at least three folio organizers, one for each sensitivity class. All folios, binders, and independent file folders will be referred to as *folio* or its plural term *folios*. All folios must be opaque along the outside casing of the folio. You should be able to see a document when the folio is closed. Some documents may require more than one folio if there is not enough space in one folio. This will be referred to as *folio groups*.

Each vault will have its own identification number (ID) (e.g., **F-019569-M202112**):

- F- – Standing for *folio*. Followed by a hyphen.

- 000000- – Random unique number. Must be unused by ALL past and current identifiers for both folios and vaults. Followed by a hyphen.
- A – The first letter of each last name that owns documents in that location. Sorted alphabetically. Different last names that have the same first letter will be condensed. Can be one or more letters.
- YYYYMM – The year the folio ID was created (four numbers). Followed by the month the folio ID was created (two numbers).

These codes will be stickered on each folio in plain sight and readable whether the folio is open or closed. Each document's digital copy will be labeled with the folio ID number the document is stored in. All new or replaced folios must obtain a new unused ID number. If the ownership of a document changes locations to where the last name ID section doesn't match, a new ID will need to be obtained and updated across all digital locations and documents. Print all IDs labeled on folios in black Arial fourteen-point bolded font on a white or light-colored background.

In ideal situations, folios should be completely lined with one layer of a Faraday cage and one layer of MuMetal® to protect against radio-frequency identification (RFID) attacks.

2.3 - Pages

All pages, page pockets, and file folders within folios will be numbered and referred to as ("page") or its plural term ("pages"). Mark number ranking in the following methods. Some documents may require more than one page if there is not enough space. This will be referred to as ("page groups").

- All pages will be numbered numerically in the following order that the pages appear in the folio.
- If there are multiple page pockets on a page, they will be ordered from left to right, followed by top to bottom.
- Folios that contain pre-inscribed numbers on their pages and other pages exist within those pre-inscribed numbers, page numbers with letters in alphabetical order can follow right after the page number. For example, the following can be sorted in sequence: **0a**, 1, 2, 3, **3a**, **3b**, 4…

All numbers must be printed and in plain sight on the corresponding page. Print all new page numbers (non-pre-inscribed) within folios in black Arial fourteen-point bolded font on a white or light-colored background.

2.4 - Document Sorting

Class 1 documents are sorted by owner's preference. Class 5 documents do not apply to this topic. Segment class 2-4 documents in the following order of priority:

1. Document Class – Personal vaults per owner for class 1 documents; shared vaults with different folios/folio groups for class 2-4 documents

2. Document Type – Different pages/page groups
3. Expired vs. Unexpired Documents & Document Owner Transferals (§ 5.1) – Different pages/page groups, but archived/expired documents follow on the very next page/page group
4. Document Ownership – Same page/page group; sorted alphabetically by last name
    a. If the document is for a pet, sort by pet name instead.
5. Documents under Different Organizations (e.g., Insurance cards or documents issued under different countries/states) – Same page/page group; sorted alphabetically by company name
6. Document Use Case (e.g., Lifetime Immunization Record and COVID-19 Vaccination Record Card) – Same page/page group; sorted from the smallest document in the front to the largest document in the back
7. Date of Issuance – Same page/page group; sorted reverse chronologically
8. Document Formats (e.g., Passport and Passport Card) – Same page; sorted from the smallest document in the front to the largest document in the back
9. Translated Documents – Same page/page group; sorted by the original document preceding the translated document

For priorities four through eight, a binder clip or paper clip is needed if more than one document exists within each priority. Binder and paper clips can be exempted if it deforms or damages the document.

2.5 - Immediate Documents

Immediate documents are defined as documentation that cannot be stored in a vault or folio due to their immediate need if requested by law enforcement or other officials, e.g., driver licenses, vehicle registrations, or tags on pet collars.

These types of documents do receive exception from § 2 based on the fluidity of the location of these documents. Digital labeling for immediate documents can be found in § 3.5.2.

3 - Digital Locations

3.1 - Overview

All class 2-5 documents should be scanned and stored digitally. All digitally stored class 2-5 documents must only be stored in an end-to-end encrypted credential manager account which is capable of storing and labeling any document type, which will be referred to as the *primary cloud provider* or *PCP*. Documents must only be stored longer-term in the primary cloud provider and the backup cloud storage provider listed under § 4. Exceptions include temporary downloads to edit the document or submit data to officials. Class 1 documents are exempt from this rule and are stored by the owner's preference. Class 5 documents will be digitally stored in the PCP but can also be digitally stored elsewhere according to owner preference if the owner does not follow the DOS.

3.2 - Choosing a Primary Cloud Provider

Primary cloud providers, aka PCPs, are cloud providers that offer the following services:

- Its applications are actively supported on the following operating systems and browsers:
  - Android 9 (Pie) or later[1] or Android-based operating system equivalent
  - iOS 16.4 or later[1]
  - iPadOS 16.4 or later[1]
  - macOS 10.15 or later[1]
  - Windows 10 (64-bit) or later[1]
  - Web application in Chrome 103 or later[1] or Chromium-based browser equivalent
  - Web application in Firefox 68 or later[1] or Gecko-based browser equivalent
  - Web application in Safari 16 or later[1] or WebKit-based browser equivalent
- Has the ability to label text from a document within the same vault item
- Files can be accessed by each member of a household/business using their account
- Offers up to at least 5GB of cloud storage (or more for some households)
- Stores all common file types (e.g., PDF, JPG, DOCX, etc.)
- Is fully end-to-end encrypted (E2EE) by default or enabled under a setting toggle
- Is reputably reliable and secure, using strong cryptographic methods
- Passes independent or collaborative audits regularly

Credential managers like 1Password, Bitwarden, and Dashlane offer these capabilities. It is recommended to use a credential manager such as these as the PCP for the DOS.

[1] The provider must support all versions of said software between the oldest acceptable version listed (e.g., Chrome 103), to the current latest stable version of said software. If a provider supports older versions of software than what's listed above and supports the latest stable version of the software, this is acceptable.

3.3 - Digital Vaults

Digital vaults are vaults in the PCP that specify the name of the documents' owner (or pet name if applicable) followed by *Docs*, *Stuff*, or *Files*, e.g., John's Docs. If a document is shared between more than one individual (e.g., Marriage Licenses), store the document by whose last name comes first alphabetically; if last names match, sort by first name alphabetically. All document owners must have access to shared documents. Duplicate shared document files/vault items can be created and stored in separate file vaults if needed but must be backed up in the same format as stated in § 4.3. All class 2-5 documents for each owner/pet will be stored in their respective vaults. No user other than the authorized editor and vault/document owner will be able to edit documents or vault management.

3.4 - File Naming

File naming will be in the order of the following properties:

1. [[Country/State of Origin] (if applicable), [Official Document Name], and [Document Format] (if applicable)]
    a. Example one: *U.S. Passport*
    b. Example two: *U.S. Passport Card*
2. [Vehicle [Year] and [Model] (if applicable)]
    a. Example one: *2021 Model 3*
    b. Example two: *2013 Crosstrek*
3. [Issue Year [YYYY]]
    a. Example: *2008*
    b. Add the most recent issue year to the filename if a document has multiple issue years. If the issue date is unknown, leave this property out of the filename.
    c. If multiple documents match filenames and have the same issue year but different dates, follow the issue year by month, and if necessary, by day in ISO 8601-1:2019/Amd.1:2022 extended format.
        i. Example: *2023-10* (Same issue year, different months)
        ii. Example: *2023-10-09* (Same issue year and month, different days)
    d. If multiple documents match filenames and have the issue date, place a hyphen after the date with an "N" and the number in which the document was received or identified on that specific date. Identification may be by preference but must remain static. The number after "N" does not need leading zeros.
        i. Example: *2023-08-03-N4* (The fourth document numbered on this date)
        ii. Example: *2023-10-23-N38* (The thirty-eighth document numbered on this date)
4. [*Front*, *Back*, or *pg*[Page Number] of a document (if applicable)]
    a. Example one: *Front*
    b. Example two: *pg402*
5. [*P*-[Pet First Name] (if applicable)]
    a. Example: *P-Duke*
6. [1st Person [FirstLast] Name]

   a. Example: *AmandaCrane* (Refrain from using shortened names, middle names, and/or nicknames.)
   b. Must be a document owner as defined by § 7.6.
   c. If more than one document owner needs to be added to the filename, sort alphabetically by first name followed by last name if needed.
      i. Example documents: Marriage licenses
7. [1st Person Birth Year [*B*-YYYY] (if first & last name matches another owner)]
   a. Example: *B-1985*
   b. If more than one document owner has the same first name, last name, and birth year, follow the birth year by month, and if necessary, by day in ISO 8601-1:2019/Amd.1:2022 extended format.
      i. Example one: *B-1985-04* (Same birth year, different months)
      ii. Example two: *B-1985-04-12* (Same birth year and month, different days)
   c. If multiple document owners have the first name, last name, and birth date, place a hyphen after the date with an "N" and the number in which the document owner is identified on that specific date. Identification may be by preference but must remain static. The number after "N" does not need leading zeros.
      i. Example one: *B-1985-04-12-N4* (The fourth document owner identified on this date)
      ii. Example two: *B-1998-12-01-N9* (The ninth document owner identified on this date)
8. [2nd Person [FirstLast] Name (if applicable)]
   a. Must be a document owner as defined by § 7.6.
9. [2nd Person Birth Year [*B*-YYYY] (if first & last name matches another owner)]
10. [3rd Person [FirstLast] Name (if applicable)]
    a. Must be a document owner as defined by § 7.6.
11. [3rd Person Birth Year [*B*-YYYY] (if first & last name matches another owner)]
12. [*OfficialCopy*, *UnofficialCopy*, or *Original* (if applicable)]
    a. This property is only applicable if multiple versions are scanned. For example, the original marriage license kept in a county office was scanned but the county office also issued an official copy to the document owner.
    b. Example document: Marriage licenses
13. [*Notarized*, *Signed*, or *Unsigned* (if applicable)]
    a. Example document 1: Agreements/Contracts
    b. Example document 2: Certain Tax Documents
14. [*Translated*[Language Name] (if applicable)]
    a. Example: *TranslatedEnglish* (if a document was translated to English).
15. .[File Format]
    a. Example one: *.pdf*
    b. Example two: *.jpg*

The following name properties will be imported into the following filename format:
[Property1] - [Property2] - [Property3] - […].[File Format]

The following characters are prohibited in document file naming:

–	—	/	\	|	[	]	{	}	,	<	>	#	@	%	^	~	`	$	°
&	*	(	)	:	;	‘	“	!	?	®	™	℠	©	+	=	¢	£	€	¿

Any other uncommon [ASCII7-bit], [ASCII-8bit], or non-ASCII characters with the exception of space (U+0020), period (U+002E), hyphen (U+2010), or underscore (U+005F) are prohibited in file naming. Please see *Wikipedia: Filename* for best practices and character prohibitions.

Don't start or end the filename with a space, period, hyphen, or underline. Filenames should be no longer than 255 characters. Filenames should not be italicized, underlined, or bolded unless the operating system or application automatically formats the filename in such a manner.

When countries or organizations are part of the official document name and have common abbreviations. Prioritize using the abbreviation used for that country/organization separated by periods and a period on the end (excluding the end of the filename) (e.g., *The United States of America* as *U.S.*) or using the official abbreviation for the country/organization (e.g., *International Organization for Standardization* as *ISO*).

Here are some examples of filenames:

- United States of Mexico Birth Certificate - 2018 - KellySmith - TranslatedEnglish.pdf
- Utah Certificate of Title - 2018 Silverado - 2020 - DanielMonson.pdf
- State of Utah Marriage License and Certificate - 2023 - BillOfferman - FrankBartlett - OfficialCopy.pdf
- U.S. Passport Card - 2020 - Front - GraceBallinger.pdf
- Animal Hospital Visit Invoice - 2023-10 - P-Duke - DanielMonson.pdf

3.5 - File Labeling

All digitally scanned documents must be labeled to the best of their ability in the PCP. All important information on each document must be labeled. Sensitive information like Social Security Administration numbers will still be labeled but will be obfuscated until revealed intentionally. All class 2-4 documents must also include the vault ID, folio ID, and page number that the physical document is located in. All document information in the PCP must include the document file as well. For multiple households that share the same PCP family plan and follow the DOS, class 5 documents for outside households can be labeled in the 2-4 classes because they will need that information for categorizing documents according to the DOS.

3.5.1 - Standard Document Attribution Process

The following location and document attributes must be labeled on each document file in the PCP, followed by which document class the attribute is required on:

- Document owner name – Classes 2-5 (all medium classes)
- Document class code (e.g., D4) – Classes 2-5 (all medium classes)

- Vault ID – Classes P2-P4, D2-D4 (if printed), and I2-I4 (if printed)
- Folio ID – Classes P2-P4, D2-D4 (if printed), and I2-I4 (if printed)
- Page number – Classes P2-P4, D2-D4 (if printed), and I2-I4 (if printed)

For class 2-4 unobtainable documents (e.g., lost, stolen, or disposed of), do not include the Vault/Folio ID or the page number attributes.

3.5.2 - Immediate Document Attribution Process

Immediate documents as defined in § 2.5 do not need the Vault ID, Folio ID, or Page number label as they're not applicable. Each file, however, needs to be labeled by the following attributes:

- Document owner name – Classes 2-5 (all medium classes)
- Document class code (e.g., D4) – Classes 2-5 (all medium classes)
- Vehicle (if applicable) – Classes P2-P4, D2-D4 (if printed), and I2-I4 (if printed)
    - Vehicles must be labeled by color, year, and model of the vehicle.
        - Example: Black 2015 Cruze
- Alternate vehicle(s) (if applicable) – Classes P2-P4, D2-D4 (if printed), and I2-I4 (if printed)
    - Include any alternative vehicles if the document regularly moves between locations.
- Precise location – Classes P2-P4, D2-D4 (if printed), and I2-I4 (if printed)
    - Include a detailed description of where the document is stored. It must be detailed enough that one can find the document on the first attempt.
        - Example one: Stored in the passenger glove box in the small gray carrier.
        - Example two: Stored in the dark cherry-colored iPhone MagSafe wallet.
        - Example three: Stored on Dean's (pet name in this case) collar.

4 - Digital Backup

Creating another digital backup of important digital documents provides an additional layer of protection and redundancy, safeguarding against potential data loss due to unexpected events such as hardware failures, accidental/purposeful deletions, or data corruption. This extra step ensures that even if the primary digital backup is compromised or lost, you still have a secondary copy, reducing the risk of irreplaceable document loss and offering peace of mind in the face of unforeseen digital mishaps.

Backups must be created under cloud storage providers who do not share the same business entity as the PCP, meaning that the businesses and parent companies must share no relation.

4.1 - Choosing a Backup Cloud Provider

When choosing a backup cloud storage provider, aka BCP, the provider must follow the same requirements for picking the primary storage provider. Listed as the following:

- Offers up to at least 5GB of cloud storage (or more for some households)
- Stores all common file types (e.g., PDF, JPG, DOCX, etc.)
- Is fully end-to-end encrypted (E2EE) by default or enabled under a setting toggle
- Is reputably reliable and secure, using strong cryptographic methods
- Passes independent or collaborative audits regularly

Backup provider accounts must only be accessible under one individual in the household in the case of accidental or purposeful removal/corruption of documents. Multiple households that share the same primary cloud provider account and follow the DOS must create a separate backup for their household. Accounts must be protected under a strong unused random password.

A recommended backup cloud provider is Proton Drive if it's not already being used as the primary cloud provider.

4.2 - What to Backup

When backing up digital documents the following information is required in the backup:

- All class 2-5 document files
    - All document file names must follow § 3.4 of file naming and should have the same filename as the document stored in the primary cloud.
- Any vital information that cannot be found in its original document file (screenshots or other separated file types are acceptable)
    - All document file names must follow § 3.4 of file naming.
    - Examples include TSA PreCheck Known Traveler Numbers and any other vital information that does contain a filed document.
- The latest inventory list (as defined in § 6.3)
- Any audit dates, logs, and notes as stated in § 6.2

- Any class 5 document permission LOAs and POAs.
- Any other assets related to the DOS such as page label prints, used vault/folio IDs, latest DOS version, etc.

Any other information labeled in the PCP already on the document does not need to be backed up. Since the inventory list is included in the backup and document ownership is in the filenames; location, document class, and document ownership labels don't need to be backed up.

4.3 - Folder Structure

The following backup structure should be created as follows:
Folder: *DOS Backup*

- Folder: *1 - Inventory List*
  - [Latest inventory list file]
- Folder: *2 - Audit Logs*
  - [Audit date] in YYYY-MM-DD format (e.g., *2024-01-30*)
    - [All applicable audit logs, notes, and date history files]
- Folder: *3 - Document Permissions*
  - Folder(s): [Approver FirstLast Name], e.g., *GregJohnson*
    - [All applicable class 5 document permission request/approval and POA files]
- Folder: *4 - Other DOS Assets*
  - [All applicable DOS assets such as used vault/folio IDs, page label prints, etc. Organized with or without folders by preference with legal characters under § 3.4.]
- Folder(s): [Digital Vault Name] Replace / with - if needed
  - Folder: *1 - Archived*
    - Folder(s): [Archived vault item] Replace / with - if needed
      - [All applicable document files]
  - Folder: *2 - Docs in Other Vaults* (Docs still must belong to the vault owner.)
    - Folder(s): [Digital Vault Name] Replace / with - if needed
      - Folder: *1 - Archived*
        - Folder(s): [Archived vault item] Replace / with - if needed
          - [All applicable document files]
      - Folder(s): [Vault item] Replace / with - if needed
        - [All applicable document files]
  - Folder(s): [Vault item] Replace / with - if needed
    - [All applicable document files]

4.4 - Backup Cadence

Anytime the following information listed in § 4.2 is changed, moved, removed, or added to the PCP, the backup information in the BCP must be updated within 48 hours afterward.

5 - Archives

In situations where document ownership has been transferred to another owner outside the household(s) (e.g., vehicle title transfers) or documents that expire (e.g., driver licenses or passports) the original document before shall be archived as the following.

5.1 - Physical Document Sorting

As stated under § 2.4, expired documents and documents where ownership is transferred shall be sorted directly behind the page/page group where the file was originally stored, e.g., expired passports should be sorted behind the page where active passports are currently being stored. Document owner transferals like historical vehicle titles will also follow this same rule.

5.2 - Primary Cloud Sorting

Expired documents and documents where ownership is transferred shall be marked as archived in their respective vaults within the PCP or an equivalent if an alternative service is being used. In the PCP, archived documents will only be viewable in the *Archive* tab or archive equivalent unless restored.

5.3 - Backup Cloud Sorting

Expired documents and documents where ownership is transferred shall be sorted into the *1 - Archived* folder in the respective vault folder as listed under § 4.3.

6 - Auditing

6.1 - Overview

Auditing is crucial to making sure that files are consistently organized, and the standard is followed/challenged. Following these guidelines will help ensure files are consistent, easy to find, and accounted for. Only class 2-5 documents need to be audited.

6.2 - Frequency

Document auditing should be conducted every 180 days. Every time an audit is finished, the current date (in ISO 8601-1:2019/Amd.1:2022 extended format [e.g., 2023-09-13]) should be marked to know when another audit must be conducted. All audit dates, durations, and notes should be logged.

6.3 - Inventory

An inventory of all stored class 2-4 documents needs to be recorded showing tiers of each location. The document name labeled should be the exact name of the filename excluding the file format. Folios will be sorted by document classes within the vault they're located in. Pages will be sorted alphanumerically within the folio they're located in. Documents will be sorted alphanumerically within the page they're located in.

Here's an example of a tiered inventory list:
555 Runaway Dr Houston, TX 77011
Stored Documents

- Vault: V-402985-CL201006
    - Folio Class 2: F-105992-CL201411
        - Page 0a
            - U.S. Passport - 2018 - KelonCampbell
            - U.S. Passport - 2018 - MichaelLarson
        - Page 1
            - U.S. Certificate of Naturalization - 2012 - MichaelLarson
        - Page 2
            - Social Security Administration Card - 2003 - KelonCampbell
            - Social Security Administration Card - 2006 - MichaelLarson
    - Folio Class 3: F-893056-CL201709
        - Page 1
            - United States of Mexico Birth Certificate - 2006 - MichaelLarson - TranslatedEnglish
            - State of Texas Certificate of Live Birth - 2013 - KelonCampbell
        - Page 1a
            - Texas Certificate of Title - 2013 Malibu - 2021 - KelonCampbell

                - Texas Certificate of Title - 2015 Soul - 2019 - MichaelLarson
            - Page 2
                - Marriage License and Certificate - 2020 - KelonCampbell - MichaelLarson - OfficialCopy
            - Page 3
                - State of Texas Lifetime Immunization Record - 2022 - KelonCampbell
                - United States of Mexico Lifetime Immunization Record - 2022 - MichaelLarson
        - Folio Class 4: F-281909-CL201006
            - Page 1
                - Emotional Support Animal Letter - 2020 - MichaelLarson
            - Page 2
                - Health Insurance Card - 2022 - KelonCampbell
                - Health Insurance Card - 2022 - MichaelLarson
            - Page 3
                - High School Diploma - 2013 - KelonCampbell
                - High School Diploma - 2013 - MichaelLarson

Immediate Documents

- Blue 2013 Malibu
    - State of Texas Vehicle Registration - 2013 Malibu - 2023 - KelonCampbell
        - In the passenger glove box.
- Red 2015 Soul
    - State of Texas Vehicle Registration - 2015 Soul - 2023 - MichaelLarson
        - In the passenger glove box in the biggest red carrier.
- Texas Driver License - 2018 - MichaelLarson
    - Stored in the golden brown colored FineWoven iPhone MagSafe wallet.
- Texas Driver License - 2019 - KelonCampbell
    - Stored in the black faux alligator skin clutch wallet.

6.4 - Questions to Ask

When auditing document storage and organization, here are a few questions to ask:

- Are all organizer IDs (vault IDs, folio IDs, and pages) properly implemented?
    - Do vault and folio IDs include the correct last names under § 2.1 and § 2.2 of the DOS?
    - Are page numbers in the correct sequence under § 2.3 of the DOS?
    - Are all IDs properly printed and visible when closed and open under § 2.1 and § 2.2 of the DOS?
- Are all physical documents properly stored?
    - Are folios separated by document class under § 2.4 of the DOS?
    - Are documents in their proper pages under § 2.4 of the DOS?
    - Are documents properly clipped under § 2.4 of the DOS?
    - Are all documents accounted for in the inventory list under § 6.3 of the DOS?

- Are all digital documents properly stored?
    - Are all documents in their respective digital vaults?
    - Are digital vaults properly named under § 3.3 of the DOS?
    - Do filenames follow § 3.4 of the DOS?
    - Is all important information labeled in the PCP under § 3.5 of the DOS?
    - Is all sensitive information obfuscated in the PCP under § 3.5 of the DOS?
    - Is the location of the physical document correctly labeled?
- Is the digital backup being followed correctly?
    - Does the backup provider still follow the standards set in § 4.1?
    - Are all document files backed up?
    - Do backed-up filenames and primary filenames match?
    - Is all other required information backed up as defined in § 4.2?
- Is data integrity being followed?
    - Are digital vaults only editable under authorized users under § 3.3 of the DOS?
    - Are class 5 documents explicitly approved for use under § 6.5 of the DOS?
    - Are class 5 document permissions saved and stored correctly under § 6.5 of the DOS?
- Is the audit fair and accurate?
    - Is the audit completion date stored for future use?
    - Are notes about the audit stored correctly?
    - Does the DOS need to be revised?

If all questions of the audit (besides the last question listed) can be answered as yes in high confidence. The audit is correctly completed.

6.5 - Document Permissions

All class 5 documents that are obtained must be under a letter of authorization (LOA) from the document owner. An example LOA for the DOS can be found in the DOS GitHub repository. All LOAs will be stored for future reference. New LOAs must be obtained every other audit (every 360 days). No class 5 documents can be submitted or used on behalf of the owner without a valid and properly notarized power of attorney (POA) being signed by the document owner.

The following actions of a class 5 document can be executed without a POA:

- Label adjustments, additions, or removals in the PCP and BCP
- Adjustments to the filename
- Cropping blank space out of a document scan
- Adjustments to the digital location of the document (only in accordance with the DOS)
- Rescans of the document
- Adjusting orientation and order of document pages
- Merging and unmerging of document pages
- Temporary downloads of documents to make non-destructive adjustments
- Any other actions that don't share/submit information to any unauthorized personnel nor modify information on the document scan

All these listed actions, however, still require initial written approval from the document owner as listed above in this section.

One may also not share/submit information about class 1-4 documents if they are not the document owner themselves. This also requires a POA signed by the document owner.

Written approval requests must outline the possible actions that may be done with the document and what cannot be done to the document without a POA. The written approval request must also list every document that will be obtained as well as every person who will be able to view, edit, and/or manage access to the documents (it would be best if the owner were to choose who has access to the documents). Here is a list of accepted written approval mediums:

- An email showing the sender's address, receipt address, and date
- A text message showing the sender number, receipt number, and date
- A letter, paper agreement, or digital agreement showing the requestor's signature, approver's signature, and date that the document was signed

POAs must be drafted alongside a lawyer to outline what actions will be taken with a class 5 document(s).

7 - Glossary

7.1 - Advanced Encryption Standard 256-bit (AES-256)

AES-256, short for Advanced Encryption Standard 256-bit, is a widely adopted encryption algorithm and one of the most secure encryption methods available today. It uses a symmetric key encryption process, where the same key is used for both encryption and decryption.

AES-256 employs a 256-bit key length, which means it uses a complex and lengthy key to encrypt data. This long key length contributes to its high level of security, making it extremely difficult and time-consuming for attackers to decipher encrypted information without the proper decryption key.

AES-256 is used in various applications, including data security, secure communications, and protecting sensitive information stored digitally. It is considered highly secure and is commonly used by organizations, government agencies, and security-conscious individuals to safeguard their data from unauthorized access or interception. Within the context of this standard, AES-256 is highlighted for its role in ensuring the security of digital documents and data stored in the PCP (if used) and other secure storage systems.

7.2 - Alphanumeric

Refers to the arrangement or sorting of items, such as documents or labels, based on a combination of letters (alphabetic characters) and numbers (numeric characters) in ascending or descending order. Alphanumeric sorting typically involves organizing items first by their alphabetical characters and then by their numerical characters, ensuring a systematic and logical order. This method of sorting is utilized in various aspects of document organization within this standard, such as the sorting of pages within folios and documents within vaults.

7.3 - Audit

An audit is a systematic examination and evaluation of documents, processes, or systems to ensure compliance with established standards, identify discrepancies, and maintain consistency. In the context of this standard, document auditing is performed regularly to verify that documents are organized, stored, and labeled correctly, following the prescribed guidelines. Auditing serves as a quality control mechanism, helping to maintain document integrity and adherence to the standard's requirements.

This term is vital in the standard as it outlines the process of inspecting and certifying document organization, which is essential for maintaining order, security, and accessibility of important documents in both physical and digital formats.

7.4 - Biometric

Refers to a method of securing access to personal vaults used for storing sensitive documents. Specifically, it pertains to the use of biometric scanning technology to control access to vaults. This means that individuals must provide a biometric identifier, such as a fingerprint or another unique physiological characteristic, to access their personal vault or shared vaults where sensitive documents are stored.

7.5 - Document class

Refers to a predefined category or group into which documents are classified based on their characteristics, importance, and sharing permissions. Document classes help organize documents into distinct tiers, each with its own set of rules and permissions regarding access and sharing. In the context of this standard, document classes are identified as 1, 2, 3, 4, and 5 in tandem with P, D, and I, with each class representing a specific level of sensitivity, shareability, and medium. This classification system guides the proper filing and organization of documents, ensuring that they are managed and protected according to their respective class code. Example class code: P3.

7.6 - Document ownership

Document ownership refers to the legal or rightful possession and responsibility for a specific document or set of documents. It signifies the individual or entity that has the authority to access, manage, and make decisions regarding the document's use, storage, and dissemination. Document ownership is a critical aspect of document organization, as it determines who is accountable for maintaining the document's accuracy, security, and compliance with relevant standards and regulations.

In the context of the Document Organization System (DOS), document ownership plays a key role in defining access rights for all documents and ensuring that documents are appropriately labeled and stored according to the standard's guidelines. Properly identifying document ownership contributes to document security, organization, and accountability within the document management system.

7.7 - Document type

Denotes the category or classification of a document based on its purpose, content, or characteristics. Document types help distinguish different kinds of documents, making it easier to organize and categorize them according to their specific attributes. Within the context of this standard, document types are used as one of the criteria for sorting and organizing documents, ensuring that documents of similar types are grouped for efficient management and retrieval, (e.g., Passports, Social Security Administration Cards, or Driver Licenses).

7.8 - End-to-end encryption (E2EE)

End-to-end encryption (E2EE) is a security protocol that ensures data remains encrypted and unreadable to unauthorized parties throughout its entire journey, from the sender to the recipient. In an E2EE system, only the sender and the intended recipient possess the necessary keys to decrypt and access the data.

E2EE provides a high level of data privacy and security, as it prevents intermediaries, service providers, and potential eavesdroppers from accessing or intercepting the content of the encrypted communication. Even the service provider that facilitates the communication cannot decipher the data passing through its servers.

Within the context of this standard, E2EE is highlighted to emphasize the secure storage of digital documents and the protection of sensitive information when using digital vaults and storage solutions in the PCP and BCP. E2EE ensures that documents remain confidential and secure even when stored in digital form.

7.9 - Household

A household refers to a single unit or group of individuals, whether related by blood, marriage, partnership, adoption, or other legal arrangements, who live together in a common dwelling and typically share responsibilities and resources. In the context of this standard, a household is significant when determining document organization, accessibility, and sharing permissions. Documents related to a household may pertain to shared expenses, property ownership, family records, and other cohabitational matters. Recognizing the nuances and dynamics of a household is essential to ensure that documents are categorized, stored, and accessed in a manner that respects both collective and individual rights and responsibilities.

In the context of this specification. Households can and may refer to business entities and departments/teams within a company.

7.10 - Obfuscation

Obfuscation refers to the deliberate act of concealing or making information unclear, typically for security or privacy reasons. In the context of this standard, obfuscation is used to protect sensitive information, such as Social Security Administration numbers, within digital documents stored in the PCP. Obfuscated information remains hidden until intentionally revealed, enhancing data security and privacy.

This term is important in ensuring that sensitive data remains confidential when stored in digital format, aligning with the standard's emphasis on document organization and security.

7.11 - Personal identification number (PIN)

A numeric code is used to authenticate a secured vault, particularly in cases where keypad access is utilized. The PIN serves as a safeguard to ensure that only authorized individuals with knowledge of the correct code can unlock and access the vault's contents. This standard emphasizes using random and secure PINs to enhance security and protect sensitive documents. Easily guessable or common numbers, such as portions of Social Security Numbers or phone numbers, are discouraged for use as PINs within this standard.

7.12 - Post-quantum cryptography (PQC)

Post-quantum cryptography (PQC) refers to cryptographic techniques and algorithms designed to resist attacks from quantum computers. Quantum computers have the potential to solve certain mathematical problems, such as integer factorization and discrete logarithms, much faster than classical computers. These problems form the basis of many widely used encryption schemes, such as RSA and ECC (Elliptic Curve Cryptography).

PQC aims to develop encryption and cryptographic algorithms that remain secure even in the presence of powerful quantum computers. This is crucial because the advent of quantum computers could potentially break existing encryption methods, posing a significant security risk to sensitive data and communications.

Within the context of this standard, PQC is mentioned to highlight the use of AES-256 encryption, which is considered one of the highest standards of non-PQC encryption and offers strong security for storing and protecting digital documents.

7.13 - Power of attorney (POA)

A power of attorney (POA) is a legal document that grants one person, known as the *agent* or *attorney-in-fact*, the authority to act on behalf of another person, known as the *principal*, in legal, financial, or personal matters. This authorization can be general, granting broad powers, or specific, conferring limited authority for particular actions or decisions. In the context of this standard, a valid and properly notarized power of attorney is required for the submission or use of class 5 documents on behalf of the document owner. The POA ensures that individuals authorized to handle important documents have the legal right to do so, protecting the interests and privacy of the principal.

7.14 - Pre-inscribe

Refers to documents, forms, or labels that have been printed in advance with certain information, text, or identifiers, typically using a standard template. In the context of this standard, *pre-inscribed* may relate to elements like identification codes, labels, or organized layouts on physical storage items such as vaults, folios, or pages. Pre-inscribed materials can help maintain consistency and clarity in document organization and identification processes.

7.15 - Reverse chronological

Refers to the arrangement or sorting of items, such as documents or events, in a chronological order that proceeds backward in time from the most recent to the oldest. In a reverse chronological order, the latest or most recent items appear at the top or beginning of the sequence, while older items follow in descending order. This method of sorting is utilized in various aspects of document organization within this standard, such as organizing documents by their date of issuance in a reverse chronological order, ensuring that the newest documents are readily accessible and identifiable.

7.16 - Radio-frequency identification (RFID)

RFID refers to a technology that uses electromagnetic fields to automatically identify and track tags attached to objects. These tags contain electronically stored information. In the context of this standard, RFID may be used in document organization systems to facilitate quicker identification, tracking, or retrieval of physical documents or items. It can also help in ensuring document security by restricting access based on RFID-enabled badges or cards.

7.17 - Security model

A security model is a structured framework that defines the principles, strategies, and technical mechanisms used to protect information systems from security threats. It encompasses security policies, access control, encryption, authentication, authorization, audit trails, and threat assessment. A security model serves as a blueprint for safeguarding data and maintaining system integrity.

In the context of this standard, the term *security model* refers to the specific security framework and practices employed by the primary cloud provider to ensure the confidentiality and protection of user accounts and data stored within the platform.

7.18 - Temporary

Temporary or temporarily, as used in the LOA document, refers to a limited and specific duration during which designated individuals are granted temporary privileges or permissions solely for the purpose of facilitating document storage and/or accessibility within the framework of the Document Organization System (DOS) specified in the agreement. Temporary actions may include, but are not limited to, editing, managing personnel access, or other actions necessary to ensure the proper organization, storage, and retrieval of digital documents. The temporary nature of these permissions implies that they are time-bound and revocable, ceasing once the specified actions are completed or when the document owner decides to revoke such privileges. The scope of temporary permissions is strictly confined to actions directly related to the efficient functioning of the Document Organization System and does not extend to sharing, submitting, or modifying information for purposes other than document storage and accessibility.

8 - Other Information

8.1 - Copyright

8.2 - Trademark Use

This document acknowledges the ownership of various trademarks, registered trademarks, service marks, icons, and logos (collectively referred to as "Intellectual Property") by their respective owners. It includes these Intellectual Properties solely for informational and educational purposes, without implying any endorsement or affiliation by the respective owners.

This document refrains from claiming ownership of the Intellectual Properties, using them solely to provide information about documentation organization. Any references to Intellectual Properties aim to benefit the respective owners in good faith.

If you, as an owner of Intellectual Property, believe that your rights have been violated or your property has been used in a manner that might constitute infringement, please contact copyright@tylermorgan.co promptly for immediate resolution.

8.3 - Environmental Impact

Consider using eco-friendly or recycled products to store bulk documents. Minimize paper and physical resources, including audits, whenever possible.

Please read this document as a PDF instead of printing it. If printing is necessary, print double-sided to conserve paper. Note that when referencing this document in print, some information such as URL links and uncommon ASCII characters may be unavailable.

8.4 - Accessibility

Individuals with disabilities may require accessibility assistance for certain processes. Consider incorporating applicable accessibility aids like braille, sign language, and audio/visual aids.

8.5 - Legal Compliance

In rare cases where legal compliance contradicts the standard of this document, prioritize and follow the legal standard set by your jurisdiction and report contradictions as needed.

Please note that this specification assumes no liability for any legal action taken against someone adhering to or not adhering to the DOS. This specification only serves as currently recommended practices for document organization.

8.6 - Recommended Items

Folio | Medium – Click here
Folio | Large – Click here

9 - Normative References

AgileBits Inc. *Password Manager for Families, Businesses, Teams*. 1Password Service. URL: https://1password.com

[ASCII7-bit]
ISO/IEC JTC1/SC2. *Information technology – ISO 7-bit coded character set for information interchange*. 16 December 1991. International Standard: ISO/IEC 646:1991(E) Third Edition. URL: https://www.iso.org/standard/4777.html

[ASCII8-bit]
ISO/IEC JTC1/SC2. *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*. 16 April 1998. International Standard: ISO/IEC 8859-1:1998(E) First Edition. URL: https://www.iso.org/standard/28245.html

ISO/TC 154. *Date and time – Representations for information interchange – Part 1: Basic rules*. 25 October 2022. International Standard: ISO 8601-1:2019/Amd.1:2022(E) First Edition: Amendment 1. URL: https://www.iso.org/standard/81801.html

Tyler Morgan. *Document Organization System*. 15 December 2023. GitHub Repository. URL: https://github.com/TylerJMorg/DOS

Wikipedia Contributors. *End-To-End Encryption*. 12 December 2019. URL: https://en.wikipedia.org/wiki/End-to-end_encryption

Wikipedia Contributors. *Filename*. 29 September 2020. URL: https://en.wikipedia.org/wiki/Filename

10 - Informative References

AgileBits Inc. *About the 1Password Security Model*. 19 July 2023. Published Security Model. URL: https://support.1password.com/1password-security/

Apple Inc. *Use Advanced Data Protection for your iCloud data*. Apple Support Guide. URL: https://support.apple.com/guide/iphone/use-advanced-data-protection-iph584ea27f5/ios

Proton AG. *Proton Drive: Free Secure Cloud Storage*. Proton Service. URL: https://proton.me/drive

Savor Goods, LLC. *Document Organizer Folio*. Recommended Product. URL: https://savor.us/collections/teachers-co-workers-wfh-team/products/the-folio-document-organizer

Savor Goods, LLC. *Family Command Center Vault Organizer Box*. Recommended Product. URL: https://savor.us/collections/teachers-co-workers-wfh-team/products/family-command-center

11 - Standard Status & Revisions

11.1 - Standard Progress – In Hard Testing/Finalization Stage

Stage Name	Status – Start/Completion Date
Conception	Completed – August 31, 2023
Drafting	Completed – September 8, 2023
Soft Testing	Completed – December 2, 2023
Revision	Completed – December 3, 2023
Hard Testing	In Progress
Finalization	In Progress
Full-Scale Beta	Expected Start Date: TBD
Final Draft Approved	Expected Date: TBD
Implemented	Expected Date: TBD

11.2 - Errata

No revisions can be approved or noted until the standard is finalized and published.

11.3 - Review Frequency

Every two years or as needed (whichever arrives first), this standard will be under review for 30 days to test real-world examples and provide the most up-to-date information with ever-growing technology as well as the growing online and physical threats one faces.

Last Reviewed: N/A

11.4 - Dates & Times

All recorded dates and times in this document are in accordance with *Tango* Military Time/Mountain Standard Time (UTC−07:00) from the first Sunday in November to the second Sunday in March or *Sierra* Military Time/Mountain Daylight Time (UTC−06:00) from the second Sunday in March to the first Sunday in November.

Individuals are in no way required to follow these time zones in their practices. These are just time zones to obtain more information about updates, reviews, and progress dates/times on this document.

About the Author

Tyler Morgan *(Pronouns: he/him or they/them)* is a freelance cybersecurity researcher and classical bassist residing in Utah, United States. He currently works as a Synergy Department Client Manager at Conservice®. Socials and website links are listed below:

Website:
https://tylermorgan.co

ORCID iD:
https://orcid.org/0009-0006-9819-6065

GitHub:
https://github.com/TylerJMorg

Email:
DOS@tylermorgan.co