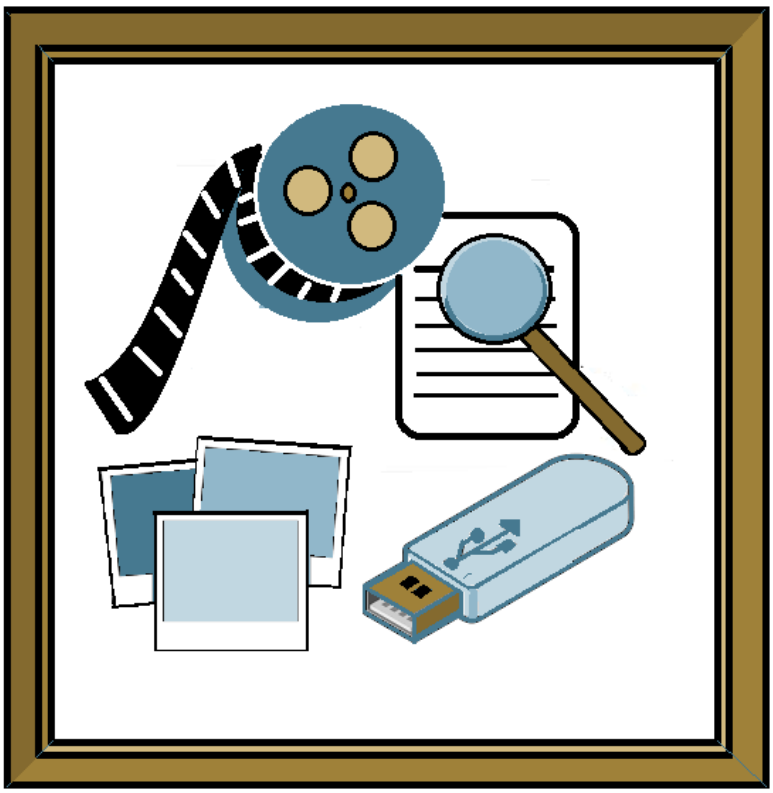

Section 2 – Essential Records and IT Systems

Description of topic

Essential records are the documents or data management systems that must be accessible during a continuity event so personnel can conduct essential functions, manage reconstitution activities, and maintain important and time-sensitive legal and accounting procedures. Your essential records may include hard or electronic documents, records, databases, photos, sound or video recordings, microfilm/fiche, software, etc.

To ensure essential records are available at time of need it is important to meticulously analyze ahead of time exactly what will be needed to conduct each important task. The lists can then be combined into a complete inventory of your essential records. This inventory can be kept as a separate document, or designation can be made within the overall inventory.

The Records Manager and IT Data Manager/IT Disaster Recovery Manager should be included in the identification of essential records, and in strategizing storage, backup and recovery options. This will help them understand why they need to prioritize access to these items. Also, their expertise is necessary to determine the organization's current recovery time (often several weeks) and strategies for storage and backup that will reduce these times to meet the recovery time objective (RTO) for continuity.

Personnel must be trained to establish secure, remote access to essential records via your servers, backup data center servers, cloud storage, data recovery tapes or other media, and to securely interface with other entities as needed. Also, developing reliable naming, storage and maps to essential electronic records makes it easier to find and recover what is needed when data has to be recovered.

printing spacer page

Component 1 – Management and Inventory

Location –

Essential Records section

- Identification of records manager and IT data recovery manager.
- Description of essential records

Essential Records appendix

- Essential records inventory (or reference the location).

Summary

A record is essential if it might be needed to conduct essential functions or reconstitution activities, or to maintain critical legal and accounting processes. This includes all hard and electronic copies of:

- Data
- Records
- Software
- Photos
- Videos
- Microfilm/fiche

To simplify the Records Manager's responsibilities referencing essential records within the master records inventory, rather than in a separate document, eliminates redundancy and the time required to maintain and cross-reference separate lists.

A plan should be developed for how each of these types of essential records will be maintained and backed up to minimize the chance of damage or loss. Some strategies to decrease these risks might include:

- Backing up to a redundant, offsite data center
- Backing up to an offsite server at a geographically separate branch of the organization, alternate facility partner or other secure location
- Backing up to a second server within the facility
- Using continuity computers, discs or encrypted flash drives to store data offsite (at the continuity facility, managers homes or other locations in accordance with acceptable levels of security determined by your leadership)
- Scanning hard copies to maintain an electronic backup
- Storing files in fire and waterproof cabinets or containers

A recovery plan should be evaluated and described, including providers and the time and expense required to return damaged records to service. *(A comparison should be made of the of cost to recover versus the cost to protect and backup records for consideration in the multi-year budgeting and acquisition section)*.

Resources, tools and templates to guide planning

Internal

- Personnel who routinely conduct the essential functions
- Records manager
- IT server/data manager and internet security manager
- Accounting manager
- Purchasing

External

Example: Records inventory in the retention schedule
Retention schedule section 5.1 - General

RSIN	Essential for COOP	Record Series Title	Description	Total Retention	Archival	Vital	Remarks
5.1.001		**Contracts and Leases** Specific COOP documents or sub-categories	Contracts, leases, and agreements include general obligation, land lease, utilities, and construction except for buildings. Documents include specifications, affidavits of publication of calls for bids, performance bonds, contracts, purchase orders, inspection reports, and correspondence. May also include other applicable documentation in the master contract file per Texas Comptroller of Public Accounts Contract Management Guide. a) Executed, renewed, or amended on or after September 1, 2015. b) Executed, renewed, or amended on or before August 31, 2015.	AC + 7 AC + 4		X	AC = Expiration or termination of the instrument according to its terms. SEE related item numbers 3.1.035 Performance Bonds and 5.3.007 Bid Documentation. SEE item number 5.2.028 for building construction contracts and item number 5.1.017 for contract logs. Government Code, 441.1855

Component 2 – Storage, Backup and Recovery

Location –

Essential Records section

- Plans and procedures and resources to store, backup and protect essential records (offsite backup strategies encouraged)
- Summary of recovery strategies and service providers

Essential Records appendix

- List of locations within the building, offsite, and on specific servers or drives where had copy and electronic essential records are stored. *It may be beneficial to migrate essential records to specific servers so it is easier and cheaper to back up and protect everything that is needed during continuity operations.*
- MOAs/MOUs for data backup and recovery service providers
- MOAs/MOUs for hard copy recovery service providers

Summary

Having access to the programs necessary to conduct essential functions, and the data, records, contracts, and other documents may be the single most important resource requirement to continue your work. Once you have determined which tasks are essential to preserve the services and reputation of your organization you must next determine every record you need and then plan on how you can ensure these are available within the RTO when an event occurs.

Recovery of electronic documents can take weeks, and may include:

- Ordering and waiting for delivery of new servers,
- Loading operating systems, security software, all other necessary software
- Re-writing customized code to make software function as your organization requires
- Recovering terabytes of data
- Recovering email

Most organizations have essential functions they need to resume within at most 30 days, so this delay could be the point of failure for continuity. Creating offsite storage to backup data and programming can significantly improve recovery time.

When hard copy records are damaged it is a very expensive and time-consuming process to recover them, and regardless of the expertise of recovery professionals it may be impossible to salvage everything. When documents are lost (as might happen in flooding or high wind disasters) there is no way to re-claim them.

Although it is becoming commonplace to convert and maintain all records in an electronic format, most entities still have hard copies they must be able to access, and hard copies can be valuable as backups when servers are unreachable or electricity unavailable. Hard copy documents can be protected using water or fireproof storage, but if damage renders the building inaccessible the records cannot be accessed.

Backing up hard copy records at the State Library, or at a contract document storage facility provides a second opportunity to quickly access and use these documents.

Resources, tools and templates to guide planning

Internal

- Personnel who routinely conduct the essential functions
- Records manager
- IT server/data manager and internet security manager
- Purchasing

External

- Department of Information Resources vendor list.
- Data backup and disaster recovery contract providers
- Document recovery providers

Worksheet ER-2-A: Storage, backup and recovery

Identify the records, their primary and backup locations, and any instructions that will help the Continuity and Reconstitution Teams access these files from a location other than the normal workplace. *(This might include remote access such as VPN, Citrix MyDesktop, cloud accounts, alternate log in procedures).*

Record (or record category)	Retention schedule ID	Primary storage location							Backup storage location(s) (preferably off-site)							Recovery strategy/ service provider	MOA or MOU in place?
		Hard copy	Electronic	Recording	Photo	Microfilm/fiche	Database	Software	Hard copy	Electronic	Recording	Photo	Microfilm/fiche	Database	Software		

Component 3 – Remote Data Access

Location –

Essential Records section

- Description of how hard copy records should be accessed from the alternate facility or remote/telework locations.
- Description of procedures to access electronic records from the alternate facility or remote/telework locations, including alterations to cover if servers are accessible, and if they are not.

Essential Records appendix

- MOA/MOU with external electronic data backup and recovery provider.
- Access instructions and passwords for external data center.
- Procedures for requesting records from the State Library or other document storage provider.
- *You may wish to complete a work flow process to provide step-by-step instructions for these procedures.*

Summary

The ability to quickly access records, particularly electronic versions, requires forethought. Records must be accessed, but servers (your own and other's) must be protected from the introduction of malware which is heightened when using less protected internet lines.

To protect the security of their servers, host entities may not allow your organization to piggyback on their network connection. If access is available their system may, or may not, meet the security standards you wish to maintain for your own data, or that others require to interface with their servers.

If they prohibit use their lines to protect their data, or your IT department prohibits that use to protect your security, you may have to find another solution such as:

- Install additional internet lines in the alternate facility, including high speed switches and other hardware necessary to ensure that the volume of data you need to process can be handled at an acceptable rate of speed.
- Procure wireless routers 'hot spots' with enough user capability to handle your Continuity Team.
- Obtain satellite internet capabilities.

Telework from home or from public buildings makes it even harder to ensure secure and dependable internet access. Policies and procedures need to be put in place and required hard and software identified to allow safe work from all locations. Training needs to be done, and testing conducted, to ensure that workers from the alternate facility or from home or other locations can access and use the identified systems and procedures.

Once you have developed a list of requirements to meet your own needs and security, have conversations with the IT teams of any other entity you would need to be able to access, or with whom you would interface, so that you can plan how you can conduct work that passes through their systems. *(Example: filing emergency payments through the Comptroller's database).*

Resources, tools and templates to guide planning

Internal

- IT Security Manager
- IT team

External

- Partner's IT teams
- DIR preferred provider list
- Internet service providers

Worksheet ER-3-A: Access strategies

Provide instructions to help the Continuity and Reconstitution Teams access files from a location other than the normal workplace. This might include instructions for:

- Remote server access services such as VPN or Citrix MyDesktop
- Accessing cloud accounts,
- Logging into backup servers at a data storage and recovery facility

Issues	Explanation and instructions
Hardware requirements and limitations	
Remote access security protocols from alternate facility	
Remote access security protocols from home or remote location	
Procedures for remote access of oeganization's servers	
Procedures for remote access of data center backup servers	
Protocols for accessing other entities servers	*Ex: Accessing Comptroller to make emergency payments*

Component 4 – Naming and Mapping Conventions

Location –

Essential Records section

- Overview of the organization's rules and best practices for naming files and folders, and mapping storage so that documents are easy to retrieve.

Essential Records appendix

- Step by step guide or example that shows how documents and folders should be handled.

Summary

If users store essential records on their desktop there is significant risk of loss. Servers are usually either fully backed-up at offsite locations, or cyclically backed up to other in-house servers, tape or other media. This means that a version of the record is recoverable. If the desktop crashes there may be no way to re-claim what is lost.

In the Windows' environment it is easy to create layer upon layer of folders that help segregate stored files into discrete bundles. However, if a server crashes the desktop icon for the parent folder will no longer lead to the intended destination. If the user doesn't remember each sub-folder along the path to the file they need IT will have a more difficult time locating the needle it in the giant, jumbled haystack of recovered documents. If the user keeps a personal map (hard copy) of where they store their essential records, or if there are organizational conventions for how files and folders are created and named, the task becomes easier.

EX 1: Post crash IT begins efforts to rapidly recover first the essential records needed for continuity, then all other records to allow resumption of full operations.
IT: "Where did you store the records you need to recover for continuity?"
User: "Right here on my screen." (points to upper left corner of blank screen)
IT: "What was the name of the folder?"
User: "My stuff"
IT: Do you remember where that folder led?"
User: "The common drive."
IT: "Which folders on the common drive?"
User: "I don't know! I just picked what I needed from each folder as they opened!"

Some important things to remember in naming files and folders are to:

- Use key words that will clearly identify the specific record or folder.
- Avoid blank spaces between words and symbols other than a dash (–) or an underline (_). Symbols other than these either:
    - Aren't recognized, which means that during a search, the name will cut off at just before the unrecognized character and anything beyond that point which may have helped narrow the search will be inaccessible.
    - Have meanings that could mis-direct the system.

Adding the retention expiration dates to the name where applicable, and where there is room, also make it easier to know when outdated files can be deleted. This minimizes the data the organization is paying to retain and simplifies the jobs of both the Legal Division and the Records Manager.
EX. 2: P:\bond_payment_record_ret-2-19 (file retention ends by the last day of February, 2019 and after that date can be submitted to the Records Manager for permission to destroy).

To further aid recovery avoid overlong names. While it is good to include enough detail to ensure a record is searchable, Windows 10 will truncate a search at 256 characters. That count includes all letters, characters, punctuation and spaces in the directory route to get there.

Additionally, if the 256-character limit is surpassed the file or folder that exceeds the character barrier will be locked and cannot be deleted or changed. One of the parent folders will need to be renamed with a shorter name that brings the characters back under the limit. Then the file can be edited or deleted and the parent folder name changed back.
EX 3: (=127 characters) P:\division_name\section_name\topic-folder\case-folder\individual_record-folder\individual_record_name-user_name-retention-date

EX 4: The user is unable to delete the file 'House_Bill_1232_edits_2017-12-30' from the following location (268 characters):

P:\Legal_Services_Division\Legal_Assistant_follow_up\specific_Legal_Aid_Name\Legislative_issues_to_track_2019\Legislative_session_notes_2019\House_of_Representatives_bills_and_statutes\proposed_changes_to_standing_documents\House_Bills\House_Bill_1232_edits_2017-12-30
By changing the name of the parent folder 'House_of_Representatives_bills_and_statutes' to 'House_bills_and_statutes' they reduced the characters from 268 to 250. Now they can delete the file.

Your IT team can help outline the best system for your organization's needs and create steps to begin steering personnel to these new, better habits. Some may be difficult to implement, but will be well worth the time and effort when a directed search is needed in a hurry.

Resources, tools and templates to guide planning

Internal

- Server/Data Manager
- Records Manager
- IT team

External

- External data storage provider
- Cloud service provider