STANDARD 9 ENSURING SOUND TRANSACTIONS

G. Recordkeeping

- 2. Keep originals of all documents essential to the defense of each real property transaction in a secure manner and protected from damage or loss

- Accreditation indicator elements located at www.landtrustaccreditation.org

IMPORTANCE OF PROTECTING ORIGINAL DOCUMENTS

Land trusts should prepare and maintain complete written documentation of all real property transactions. Because land trusts are in the business of perpetuity, they need to keep originals of key documents essential to the defense of each transaction safe from damage, tampering or inadvertent destruction. At a minimum, land trusts need to have two sets of documents:

1. Documents that are safely stored in a way that ensures that they will last and be acceptable evidence in the event of a court proceeding (permanent files).
2. Copies of all documents essential to the defense of each real property transaction. See Practice 9G3 for more information about duplicate documents, including working files.

PERMANENT FILES: ORIGINAL DOCUMENTS

The permanent file includes those documents and records that constitute the essential and irreplaceable record of a transaction and any subsequent activity related to that project. This includes easement monitoring, approval and enforcement data, as well as data related to the initial transaction.

In its permanent files, the land trust should have the following irreplaceable documents essential to the defense of each conservation easement and fee property still owned by the organization, including:

- Legal documents and agreements, including deeds, conservation easements, amendments and leases.
- Critical correspondence, including correspondence with the landowner related to project goals, tax and legal matters, notifications, approvals, enforcement and other key matters the land trust determines essential to the defense of the transaction.
- Baseline documentation reports for conservation easements.
- Title insurance policies or evidence of title investigation.
- Surveys, if any.
- Full appraisals (or summary appraisals if full appraisals are not available) used to substantiate the purchase price or used by the landowner to substantiate the tax deduction.
- Forms 8283 for projects where the landowner claimed a federal tax deduction. The land trust's "original" can be a copy of the landowner's signed original.
- Conservation easement monitoring reports.
- Fee property inspection records essential to the stewardship and defense of the property.
- Contracts and leases relative to long-term land management activities. The original may be retained only for as long as it and the applicable statute of limitations are in effect.

For accreditation, a land trust must retain originals of:

- Legal agreements, deeds, conservation easements, amendments
- Critical correspondence, including those related to project goals, tax and legal matters, enforcement and other matters essential to the project
- Baseline documentation reports
- Title insurance policies or evidence of title investigation
- Surveys (if any)
- Appraisals used to substantiate the purchase price or used by the landowner to substantiate the value on the Form 8283
- Conservation easement monitoring reports
- Fee inspection property reports
- Contracts and leases in effect for land management activities
- Conservation easement stewardship records, including substantive notices, approvals, denials, interpretations and exercise of reserved rights

A land trust is also expected to have the documentation requested in the application and the project documentation checklist; however, unless identified in the list above, the organization does not need to meet the storage and duplication requirements for these documents.

PERMANENT FILES: SAFE STORAGE

Original documents must be protected from daily use and reasonably secure from fire, flood and tampering by individuals. When determining where to store original files, land trusts need to ask themselves a number of key questions. What are the risks of loss, destruction or unauthorized access, and what are the consequences? Fire? Theft? Flood? Malicious mischief? Other? What can we do to limit the likelihood of loss? What will happen if we lose certain data? The list of threats may seem endless, but for each land trust, some will be more likely than others. For example, a land trust using a storage facility with lots of sprinklers may be more concerned about water damage than fire. An urban office may have a greater risk of unauthorized entry, and additional physical security may be necessary.

A land trust's records policy (Practice 9G1) will guide overall records retention and storage, including which documents a land trust considers part of the permanent record for a transaction. Land trusts use several approaches for safe storage of records, including:

- *Fireproof file cabinet or safe in another location*. Some land trusts keep their permanent files in a fireproof cabinet or safe in a separate location, such as an attorney's office or town hall. If originals are stored in another location, the land trust must have control over the retention of these documents. If they are stored in a private home (such as of a board member of a small, all-volunteer land trust) the land trust should secure a written agreement with the homeowner that guarantees that other representatives of the organization (such as officers or key employees) can access the records.
- *Safe deposit box*. Other land trusts choose to keep their files in a bank safe deposit box.
- *Formal archive facility*. Several land trusts choose the convenience and safety of a formal archival facility.
- *Registry of deeds*. Originals of property deeds, conservation easements, surveys and sometimes baseline documentation, may be kept at the county or municipal register.
- *Digital systems*. Land trusts increasingly digitize information and documents. They also use a variety of systems to protect that data, including off-site storage of discs or backup data and online backup systems.

At a minimum, these locations must protect the originals from daily use and be reasonably secure from fire, floods or other foreseeable hazards.

For accreditation, a land trust must keep originals secure (such as in a locked cabinet with limited access or in an archive facility with permission needed for access) and protected from damage or loss (such as in a fireproof safe, bank vault or archive facility with sprinklers).

A land trust must store copies in locations that could not be destroyed in a single calamity (such as paper originals and duplicates stored in separate locations or electronic duplicates backed up on a remote server or on the cloud).

PAPER VERSUS ELECTRONIC FILES

Many land trusts now use both paper files and electronic systems to manage and maintain project data; each has its own advantages and disadvantages.

Computer-based systems provide for relatively easy access (even from remote locations) and can easily accommodate changing or updating files and data. They also require consistent, rigid protocols for greatest efficiencies and credibility. What is easily created can also be easily lost. While creating an entire system can seem overwhelming and expensive, there are relatively inexpensive off-the-shelf products available. Keep in mind that if the land trust stores its originals in an electronic format, the originals must meet the requirements of applicable federal and state law with respect to rules of evidence regarding electronic originals. They must also be replicas of signed originals and include all exhibits and attachments in a format that cannot be altered. Some land trusts maintain their electronic originals in a PDF format that is more difficult to alter than those stored as word processing documents. Safeguards for ensuring the originals do not get erased or written over include using non-rewritable discs and limiting access to cloud-based original records as read only or only to those with permission. The approach a land trust uses should be based on managing the risk of the land trust not having the documentation needed to steward and enforce its conservation easements and properties. If electronic originals are stored on portable devices (discs or external hard drives), they should be maintained separate from duplicates, protected from daily use and reasonably secure from fire, flood and tampering by individuals.

Tips for Cloud-Based Storage

Choosing a vendor to work with to store documents in the cloud is not unlike choosing a vendor to store paper documents.[1] Considerations such as security controls, access and contracting all carry through into the virtual world. Storing documents in the cloud does present some additional benefits, such as ease of access, protection against physical damage and integration into online or searchable database systems. While storing documents in the cloud carries many benefits, it does add some additional concerns and complexity.

1. Choose a cloud-based storage service or provider with care. Things to look for:

    a. Choose a vendor with a good service level agreement (SLA). The SLA describes the performance of the system and what you should expect as a customer. If the service is down frequently, it won't be useful to you.

    b. Choose a well-established vendor. If your vendor goes out of business or can't invest in good cloud infrastructure, your files are at risk.

    c. Understand what type or format of files the vendor uses to store files. The most common is PDF for scanned or saved documents. PDF documents should be in the PDF/A format, which includes some additional benefits for long-term archiving of digital content.

    d. Decide how to organize documents. There are several different ways to store and manage data. Some systems are organized in a traditional file and folder structure. Other cloud-based storage systems may have additional features, such as tags so that a document could be assigned multiple attributes. If you need to switch vendors, it is important to understand how you can remove your data from a system. Is there a way to export all your files easily in the event you need to move your files to an alternate storage solution?

    e. A service should provide encryption "at rest" (when the files are stored on the cloud service servers) and "in transit" (when you are uploading or downloading the files to your local computer). Even if documents are in the public record, ensuring the correct method of access is important.

[1] Thanks to CommunityIT Innovators for providing guidance on cloud-based storage.

2. Limit access to your cloud-based storage files. A good storage service will provide granular security settings. Restrict access to the degree you can without compromising operations. Only give access to personnel that need it and limit that access to "read only" when that will suffice. Require complex passwords and consider setting up multifactor authentication (to login, user must provide several separate pieces of evidence that is authenticated by the system).

3. Employ a third-party backup solution for your cloud-based storage. A good cloud storage service provider will perform regular backups of their customer's data to protect their own liability, but you should have your own backups in place independent of that. That third-party backup solution could be a backup to local on-premise storage or to an alternate cloud solution. Having a separate backup repository of data is an extra layer of protection against the loss of data through a crypto attack, vendor disruption or intentional or unintentional data destruction by staff.

4. Check the status of your cloud-based storage service and third-party backup service regularly. Are credit card autopayments working properly? Are there customer notifications regarding service interruptions or concerns?

Tips for Paper Storage

Paper, however, is still a trusted and essential part of almost all land trusts' recordkeeping systems. It is still the most common format in which to create most documents and records. In fact, paper documents are required to complete most real estate transactions. Paper files and filing systems are often easier to change or expand than computer systems and may be less expensive to create and maintain than sophisticated databases. However, paper takes up a lot of space and, if not properly selected and stored, can be damaged by water, mildew, pests and time itself.

The Library of Congress provides very detailed specifications for paper they will accept for their archive, which is summarized below.

- *Fiber*. The stock must be made from rag or other high alpha-cellulose content pulp, minimum of 87 percent. It must not contain any post-consumer waste-recycled pulp.

- *Lignin*. The stock must not contain lignin.

- *Impurities.* The stock must be free of metal particles, waxes, plasticizers, residual bleach, peroxide, sulfur and other components that could lead to the degradation of the paper sheet itself. Iron must not exceed 150 ppm and copper shall not exceed 6 ppm.

- *Optical brighteners*. The stock must be free of optical brightening agents.
- *pH*. The stock must have a pH value within a range of 8.0 - 9.5
- *Alkaline reserve.* The stock must contain an alkaline reserve with a minimum of 2 percent and a maximum of 5 percent.

If you choose not to store your photos digitally, you may want to check with a local museum as to what type of paper they use or will accept. At a minimum, print photographs on acid-free photographic paper.

Most land trusts inevitably use a combination of recordkeeping processes. Your land trust should decide what approach best meets your informational needs.