CHAPTER 13

Digital Data & Documents

New here? Ready, Set, Ready is a 10-minute starting point: an honest assessment, one gap closed for real, then a map for using the rest of this site. Once something's actually happened, Surviving picks up where this chapter leaves off, organized by chronology instead of category. Curious how Tier, Stage, and Phase relate? See the Glossary.

Why This Category Matters

A household that survives a disaster physically intact can still lose everything on paper (proof of identity, property ownership, insurance coverage, or years of financial and medical history) if the documents proving it exist only in one place. This chapter is about redundancy: making sure no single fire, flood, or hard-drive failure can erase who you are on paper.

The chapter follows the same 3-2-1 principle used by IT professionals for critical data (3 copies, on 2 different media types, with 1 stored off-site) applied to a household's actual life instead of a server room.

Tier 1: Short-to-Medium Term (Hours – 14 Days)

Goal: *Protect originals from immediate physical damage (fire, flood, water damage) and ensure copies are accessible for insurance claims and identification.*

Tier 1 is about getting ahead of the single most common failure mode: a fire, flood, or chaotic evacuation destroying or leaving behind the physical originals of documents that are difficult or slow to replace.

Skills to Build

- **Document Digitization:** Scan every vital record to PDF at a resolution that's actually readable (300 DPI minimum) and organize files with consistent, searchable names: a folder of 40 files named "scan001.pdf" through "scan040.pdf" defeats the purpose under stress. See the Document Go-Bag & Digital Backup skill guide for the full checklist.

- **3-2-1 Backup Strategy:** 3 copies of every vital file, on 2 different media types (e.g., an external drive and cloud storage), with 1 copy stored off-site: a copy on a second hard drive in the same house doesn't protect against a house fire. See the Document Go-Bag & Digital Backup skill guide for setting this up.
- **Insurance Documentation:** Create a video walkthrough of your home's contents, narrating what's visible, room by room. Most insurers accept this as claims evidence and it takes 15 minutes, far less effort than an itemized list, while capturing more.
- **Encryption:** Use a real tool, not an ad hoc method: VeraCrypt (free, cross-platform) for an encrypted container or drive, or your operating system's built-in full-disk encryption (BitLocker on Windows Pro, FileVault on macOS) for a laptop that might be lost or stolen. See the Document Go-Bag & Digital Backup skill guide for applying this to your vital-records backup.
- **Legal Continuity Documents:** A will, financial and healthcare power of attorney, and, if you have minor children, a guardianship designation are the actual legal documents this chapter's own Materials & Supplies table below assumes you already have. See the Wills, Power of Attorney & Guardianship skill guide for what each document does, when a DIY version is defensible versus when to get an attorney, and the witnessing rules that most often invalidate a DIY attempt.

▸ GO DEEPER

The **Digital Data & Documents Addendum** builds these into real, tested competency.

For the hands-on how-to:

Document Go-Bag & Digital Backup | Wills, Power of Attorney & Guardianship

Tech & Equipment

- **Fireproof/Waterproof Safe:** UL-rated (e.g., SentrySafe, Honeywell), but check the specific rating class, not just "fireproof" on the box. UL 72 Class 350 protects paper (keeps interior below 350°F), while Class 125 protects electronic media (below 125°F and controlled humidity). A safe rated only for paper does not equally protect a hard drive stored inside it; if you're storing both, verify the safe is rated for both, or use separate rated containers.
- **Encrypted External Hard Drive:** 1TB+ for digital copies of all vital records, encrypted with one of the tools above. An unencrypted backup drive is a liability if it's ever lost or stolen.

- **Fireproof Document Bag:** A portable, silicone-coated fiberglass bag (SentrySafe and similar brands make these) for the go-bag: for documents that need to travel with you, not just sit in a home safe.
- **Scanner:** A flatbed or portable scanner for digitizing documents. A phone camera works in a pinch but produces lower, less consistent quality than even an inexpensive dedicated scanner.

Materials & Supplies

Item	Quantity / Spec	Notes
Original documents	Birth/marriage certificates, passports, SSN cards, deeds, insurance policies, wills/trusts	Store in the fire/water-rated safe; see the equipment note on matching the rating to what's stored.
Digital copies	Encrypted USB drive in emergency kit	The “grab and go” copy, separate from the home safe's drive.
Cloud backup	Secure account with automatic sync (e.g., Backblaze, iCloud, Google Drive)	Your off-site copy in the 3-2-1 strategy; verify it's actually syncing, not just installed.
Password manager emergency kit	Printed official export (not a handwritten list)	Use your password manager's own emergency-access feature (1Password's built-in “Emergency Kit” PDF or Bitwarden's “security readiness kit” template) rather than hand-copying passwords into a binder. Store the printed kit in the safe alongside other documents.
Cash reserve	$1,000+ in small bills, stored in the safe	A starter reserve for immediate liquidity; the full cash and financial strategy is covered in the Economic & Financial chapter.

Quick Checklist

- [ ] All vital documents scanned at 300+ DPI with consistent, searchable file names
- [ ] 3-2-1 backup in place: 3 copies, 2 media types, 1 off-site
- [ ] Video home-contents walkthrough recorded and backed up
- [ ] Encryption tool (VeraCrypt, BitLocker, or FileVault) actually in use, not just installed

- [ ] Fire/water-rated safe checked against what's actually stored in it (paper vs. electronics rating)
- [ ] Fireproof document bag packed in the go-bag with paper copies of key documents
- [ ] Password manager's official emergency kit printed and stored securely, not a plaintext password list
- [ ] $1,000+ cash reserve in small bills in the safe
- [ ] Will, financial and healthcare power of attorney, and (if applicable) a named guardian for minor children, actually signed and properly witnessed, not just planned
- [ ] Practiced: located and opened every backup (safe, drive, cloud account) within the last 6 months to confirm access still works

Tier 2: Extended (2 Weeks – 3 Months)

Goal: Maintain access to critical data when cloud services are offline and physical infrastructure is damaged. Focus on offline redundancy and manual record-keeping.

Tier 2 assumes the cloud backup from Tier 1 may be unreachable for an extended period, and that new records (medical visits, financial transactions, important events) need to be tracked without the digital tools normally used for it.

Skills to Build

- **Offline Data Access:** Practice actually retrieving files from an encrypted drive without an internet connection before you need to do it under pressure. Password managers and some encryption tools behave differently offline than most people expect.
- **Manual Record-Keeping:** Maintain paper logs for financial transactions, medical events, and family records during the disruption; these become the source record to digitize later, not an afterthought.
- **Data Recovery Basics:** If a drive starts failing (clicking sounds, files disappearing, slow/unresponsive behavior), stop using it immediately and don't repeatedly power-cycle it: every additional read attempt on a failing drive risks further damage. The old advice to freeze a failing hard drive is a persistent myth and not a reliable recovery method; if the data is genuinely critical, the safest layperson step is to stop using the drive and consult a professional data recovery service rather than attempting DIY fixes.

- **Secure Storage:** Protect physical media from heat, moisture, and theft. A drive or paper archive stored in a hot attic or damp basement degrades quietly, with no warning until it's needed.

▸ GO DEEPER

The **Digital Data & Documents Addendum** builds these into real, tested competency.

For the hands-on how-to:

Document Go-Bag & Digital Backup | Wills, Power of Attorney & Guardianship

Tech & Equipment

- **Solar Power Station:** To power external drives and scanners for continued digitization; cross-reference the Energy & Heat chapter's Tier 2 sizing guidance.
- **Portable SSD:** Additional encrypted storage for rotating backups. SSDs have no moving parts and tolerate movement/vibration better than traditional hard drives for a go-bag or vehicle.
- **Paper-Based System:** Labeled binders and folders for manual record-keeping. Organize by category from the start rather than as a single growing pile.
- **Thermal Printer:** Useful for quick, ink-free printing of logs and receipts, but thermal paper fades significantly over months to a few years, especially with heat or light exposure. Treat thermal printouts as a short-term convenience, not an archival copy; anything that needs to last should be transcribed to standard paper or digitized.

Materials & Supplies

Item	Quantity / Spec	Notes
Off-site physical backup	Encrypted drive with an out-of-state relative	Pairs with the Communication chapter's out-of-state contact; the same person can often hold both roles.
Paper copies	Printed vital documents in the fireproof go-bag	The physical fallback if every digital copy is simultaneously unreachable.
Writing supplies	Pens, pencils, paper	For manual logs; inexpensive and easy to overlook until needed.
Disinfectant	For cleaning/preserving documents after water exposure	Mold sets in fast on wet paper; address exposure within 48 hours if at all possible.
Silica gel packets	For moisture/mold prevention	Replace or re-dry periodically; saturated silica gel stops absorbing and offers no protection.

Quick Checklist

- [ ] Offline access to encrypted drives tested and confirmed working
- [ ] Paper log system set up and organized by category from the start
- [ ] Failing-drive protocol understood: stop use immediately, no DIY “fixes,” professional recovery for critical data
- [ ] Physical media stored away from heat/moisture extremes
- [ ] Off-site backup drive placed with an out-of-state relative or trusted contact
- [ ] Thermal-printed records understood as short-term only, not archival
- [ ] Silica gel packets fresh (not saturated) in document storage
- [ ] Practiced: a manual paper log actually maintained for at least one full week as a dry run

Tier 3: Permanent (Indefinite)

Goal: *Long-term preservation of family history, knowledge, and records without any digital infrastructure. Focus on physical durability and community knowledge sharing.*

Tier 3 assumes no reliable digital infrastructure for the foreseeable future. This shifts the core trade-off: digital media is convenient but degrades or fails suddenly and needs active migration to

new hardware every few years, while correctly stored acid-free paper and properly processed archival film degrade slowly and predictably, and can genuinely last a century or more without any power or maintenance at all.

Skills to Build

- **Archival Preservation:** Store paper documents in acid-free folders and boxes. Standard acidic paper and folders yellow and become brittle within decades; archival-grade materials are inexpensive by comparison and dramatically extend document life.
- **Microfilm / Film Photography:** Create long-term analog backups of important records. Properly processed silver-halide microfilm is the gold standard for multi-century document preservation used by professional archives, well beyond what any current digital format can promise.
- **Community Knowledge Base:** Organize and share vital information (skills, history, records) with trusted community members. Knowledge held by only one person is knowledge one bad season away from being lost, the same principle as other chapters' skill-redundancy guidance.
- **Data Migration:** Transfer data from failing or aging digital media to new storage proactively, on a schedule. Don't wait for failure. No digital medium is a "store once, forget forever" solution the way archival paper or film can be.

▸ GO DEEPER

The **Digital Data & Documents Addendum** builds these into real, tested competency.

For the hands-on how-to:

Document Go-Bag & Digital Backup | Wills, Power of Attorney & Guardianship

Tech & Equipment

- **Archival Storage:** Acid-free folders and boxes, plus climate-controlled storage where possible. Stable temperature and humidity matter more than any single container choice.
- **Film Camera & Darkroom:** For creating analog backups of documents and photos: a real, working skill set, not just nostalgia, in a scenario with no digital infrastructure.
- **Magnetic Tape Drive:** For long-term, air-gapped data storage if available. Worth noting this is genuinely enterprise-grade equipment, expensive and not easy to source for most households;

treat it as an if-available option, not a baseline expectation.

- **3D Printer:** For fabricating replacement tools or parts from digital files if the specific need arises.

Materials & Supplies

Item	Quantity / Spec	Notes
Archival paper	Acid-free, for long-term storage	The single highest-leverage, lowest-cost upgrade in this entire tier.
Microfilm rolls	For permanent analog backups	Pairs with the film camera/darkroom skill above.
Climate control	Dehumidifiers, silica gel, temperature monitoring	Consistency matters more than any single extreme; avoid large swings, not just avoiding heat or moisture individually.
Community archive	Physical library shared with trusted neighbors	Redundancy against losing any single household's collection to fire, flood, or loss.
Barter items	Digital storage devices, batteries, cables	High trade value in a community still running any digital equipment at all.

Northern Utah Note

Salt Lake City is home to one of the most extensive archival preservation operations in the world: FamilySearch's Granite Mountain Records Vault, built into a mountainside specifically for long-term, climate-controlled preservation of genealogical microfilm. It's not a resource available for personal storage, but the underlying model (climate-controlled, physically secure, redundant archival storage) is exactly the principle to scale down for a household or community archive, and FamilySearch's free genealogy resources are a genuinely useful tool for the "family history" half of this chapter's goal.

Quick Checklist

- [ ] Vital paper documents moved into acid-free folders/boxes
- [ ] Microfilm or archival film backups created for the most critical records

- [ ] Community knowledge base established with trusted neighbors
- [ ] Digital media migration schedule set (not waiting for failure)
- [ ] Climate-controlled or at least climate-stable storage arranged
- [ ] Community archive redundancy established across more than one household
- [ ] Practiced: successfully migrated data from one storage medium to another as a planned exercise

Tier 4: Sustainable Community

Goal: *Build a community-wide record-keeping and archival system so no single household's fire, flood, or loss erases records the whole community depends on.*

Beyond personal documents, a functioning community needs its own records (who owns what, what agreements were made, what happened and when), especially once formal government record-keeping may not be reliably available. Tier 4 extends this chapter's redundancy principle from individual households to the community's actual governance and history.

Name the real records a neighborhood actually needs, property boundaries, mutual aid agreements, resolved disputes, not every piece of paper every household owns. Then ask who's genuinely willing to steward them, and whether real equipment (scanners, archival supplies) exists to pool, before building a shared system around a need or a capacity that isn't actually there.

Choosing an Approach

Three real models exist, and they fit different circumstances.

Approach	What it is	Fits when
Informal shared memory	Verbal agreements and a loosely kept group memory of who agreed to what, no formal records	A small, already-trusted group, or genuinely low real dispute risk
Documented shared ledger	A written, distributed community record of agreements and disputes, no notary involved	Real recurring need for written records, a willing steward, but no one pursuing notary commission
Formal notarized record-keeping	A commissioned notary in the community handling genuinely binding documents	Sustained need, and someone pursuing the notary credential below

A Community Ledger Isn't a Substitute for Formal Recording

A community's own written ledger is real and useful for settling a dispute informally, but it isn't a substitute for actual legal recording once that becomes available again, a county recorder still has to receive a deed or a court still has to see a judgment for it to carry full legal weight. Treat the informal record as a bridge that holds things together until formal systems come back, not a permanent replacement for them, and get anything that genuinely matters properly filed the moment that's possible again.

Skills to Build

- **Community Record-Keeping:** Maintain formal, shared records of property boundaries, mutual aid agreements, trades, and disputes resolved. Informal community agreements need a real record once formal legal/government systems can't be relied on to arbitrate disagreements.
- **Becoming a Notary:** Most states let a resident become a commissioned notary public through a fairly short, well-defined process: typically a state exam or short course, a background check, and a surety bond, together usually costing a few hundred dollars all in, followed by filing an oath of office through the relevant state office. Commissions typically run around four years before renewal; check your own state's exact fee, bond amount, and process directly. A notary's real value here isn't everyday convenience, it's what happens after a disaster, when insurance claims, legal paperwork, and property transactions all still require notarization, right when the normal local supply of notaries can become scarce. Difficulty: Medium. Training: a state exam or short course, a background check. Cost: $$-$$$.

- **Distributed Archival Skills:** Train more than one person in the community in archival preservation and digitization, the same redundancy principle used for medical, radio, and caregiving skills in earlier chapters.
- **Shared Digitization Projects:** Organize community-wide digitization efforts (shared history, collective skills, local knowledge) rather than leaving it to individual households working in isolation.
- **Succession Planning for Records:** Explicitly plan who takes over a household or community record archive if its original keeper is lost. An archive with no successor is a single point of failure no matter how well it's maintained.

▸ GO DEEPER

The **Digital Data & Documents Addendum** builds these into real, tested competency.

For the hands-on how-to:

Document Go-Bag & Digital Backup | Wills, Power of Attorney & Guardianship

Tech & Equipment

- **Shared Digitization Equipment:** Community-level scanners, cameras, and archival supplies, reducing the cost burden on any single household.
- **Distributed Archive Sites:** Multiple physical archive locations across different households or a shared community building; no single fire or flood should be able to erase the community's records.
- **Community Records Registry:** A maintained, accessible index of what records exist and where. An archive no one can find is barely better than no archive at all.

Materials & Supplies

Item	Quantity / Spec	Notes
Community records archive	Property, agreements, trade, dispute records	The community's actual functioning legal/governance memory in the absence of formal systems.
Shared archival supplies	Acid-free materials, film, digitization equipment	Pooled community resource rather than duplicated per household.
Distributed backup network	Copies held across multiple households	Same redundancy principle as every other chapter's shared reserve; no single point of failure.

Quick Checklist

- [ ] Community record-keeping system established for property, agreements, and disputes
- [ ] Multiple people trained in archival/digitization skills community-wide
- [ ] Records physically distributed across more than one location/household
- [ ] Community records registry maintained so records can actually be found
- [ ] Succession plan in place for who maintains records if the current keeper is lost
- [ ] Notary commission considered as a community credential, if sustained formal record-keeping need exists
- [ ] Practiced: a community records audit completed to confirm everything is where the registry says it is

At a Glance: Digital Data & Documents Across All Tiers

A single-page reference for planning purposes. This does not replace the detailed guidance above; use it to see how the plan scales, not as a standalone checklist.

Tier	Duration	Storage Method	Access Strategy
Tier 1	Hours – 14 days	Fireproof safe, encrypted drive, cloud backup	3-2-1 backup, password manager emergency kit
Tier 2	2 weeks – 3 months	Off-site backup, paper logs	Offline drive access, manual record-keeping
Tier 3	Indefinite	Acid-free archival paper, microfilm	Community knowledge base, scheduled data migration
Tier 4	Sustainable community	Distributed community archive	Shared records registry, succession planning