ADDENDUM K

Digital Data & Documents: Zero to Full Competency

Why This Addendum Exists

Chapter 11 tells you what to have and do at each tier of a disruption. It does not build the actual digital security and archival competency behind “encrypt it” or “store it acid-free,” the kind of understanding that lets you evaluate new tools and situations rather than just follow a fixed checklist. This addendum is a skill-building curriculum for exactly that, built from real, recognized certifications.

It’s organized by skill stage, not by disaster duration, following the same structure as the other addenda. Treat the self-check at the end of each stage as the actual gate.

Four stages: Foundations (basic safe practice), Applied Practice (hands-on competence), Self-Sufficiency (independent, resilient skill), and Mastery & Teaching (able to teach others and operate at community scale). Each stage covers two sub-skill tracks that run in parallel: digital security, and physical/archival records.

Stage 1: Foundations (Awareness)

Goal: understand the core digital security and archival concepts well enough to make sound decisions and evaluate whether a given tool or practice actually solves your problem. This stage is readable in a weekend.

Digital Security: Core Knowledge

The core concept at this stage is understanding what encryption actually protects against (a lost or stolen device) versus what it doesn’t (a compromised password, malware already on the unlocked device), and the 3-2-1 backup principle already covered in Chapter 11 well enough to explain why a second copy on the same physical device doesn’t count as real redundancy.

Archival: Core Knowledge

The core concept at this stage is understanding why digital and physical archival methods have opposite failure modes: digital media is convenient but fails suddenly and needs active migration, while acid-free paper degrades

slowly and predictably and needs no power at all. Chapter 11's Tier 3 guidance already covers this trade-off; Stage 1 is building genuine understanding of why, not just following the recommendation.

Stage 1 Learning Path

Resource	Cost / Format	Notes
FamilySearch Learning Center	Free, online, 140+ courses	familysearch.org/wiki/en/Classes_in_the_Learning_Center. Free video courses on genealogy and records research, taught by professional genealogists.
EFF (Electronic Frontier Foundation) Surveillance Self-Defense guide	Free, online	ssd.eff.org. A well-regarded, plain-language introduction to real digital security concepts, not just product recommendations.
CompTIA A+ Cyber overview	Free overview material available	comptia.org/en-us/certifications/a-cyber. A fast-track foundational overview if cybersecurity is a genuinely new subject.

Stage 1 Practice Exercises

- **Verify your actual 3-2-1 backup is real:** Physically confirm your 3 copies live on genuinely different media types and that the off-site copy is somewhere that wouldn't be destroyed in the same event as the other two. See the Document Go-Bag & Digital Backup skill guide for what actually belongs in that backup and how to keep a portable copy current.
- **Test your password manager's emergency access feature:** Actually walk through what a trusted person would need to do to access your accounts in an emergency, using the feature itself, not just assuming it would work.
- **Identify your household's most fragile physical document:** Find the single most damage-prone original document you own and decide, concretely, whether it needs archival-grade storage now.

Self-Check: Ready for Stage 2?

You should be able to explain what encryption does and doesn't protect against, why a true 3-2-1 backup requires genuinely different media and locations, and why digital and physical archives have opposite failure modes, all without looking it up.

Stage 2: Applied Practice (Competent)

Goal: move from knowing the concepts to having actually implemented and tested the real systems Chapter 11 describes.

Digital Security: Applied Practice

- **Actually implement full-disk encryption and test it:** Turn on BitLocker, FileVault, or VeraCrypt on your real devices (already covered in Chapter 11) and confirm you can still access your data afterward, including from a fresh reboot.
- **Set up and test a password manager properly:** Migrate your actual passwords into a real password manager, generate the official emergency kit, and store it per Chapter 11's guidance, rather than continuing to use browser-saved or reused passwords.
- **Practice offline data recovery under simulated pressure:** Time yourself actually retrieving a specific file from your encrypted backup without internet access, since Chapter 11's Tier 2 already flags that this behaves differently than people expect.

Archival: Applied Practice

- **Digitize a real batch of documents to spec:** Actually scan a meaningful batch of vital documents at 300+ DPI with consistent, searchable file names, not just the one or two documents used to test the process. The Document Go-Bag & Digital Backup skill guide covers which documents actually belong in that batch.
- **Move your most fragile document into archival storage:** Act on your Stage 1 assessment: actually rehouse your most damage-prone document in an acid-free folder or box.
- **Take a genealogy research course:** Complete at least one full FamilySearch Learning Center course relevant to your own family history research, applying real research methodology rather than casual searching.
- **Put your household's actual legal documents in place:** A will, financial power of attorney, healthcare power of attorney, and a guardianship designation for any minor children are the specific legal documents Chapter 11's archival guidance exists to protect once they're created; if your household doesn't have them yet, creating them is a real Stage 2 task, not a someday item. See the Wills, Power of Attorney & Guardianship skill guide for what each document actually does, DIY versus an attorney, and the witnessing rules that most often invalidate a DIY attempt.

Stage 2 Learning Path

Resource	Cost / Format	Notes
A password manager with an emergency-access feature (1Password, Bitwarden)	$0–$60/year depending on tier	Already cited in Chapter 11; actually implement it, not just know it exists.
Archival-grade folders and boxes	$20–$60 for a starter set	The single highest-leverage, lowest-cost archival upgrade, per Chapter 11's Tier 3 guidance.
A flatbed or portable scanner	$80–$250	Already cited in Chapter 11; a phone camera works in a pinch but produces meaningfully lower quality.

Self-Check: Ready for Stage 3?

You should have actually implemented full-disk encryption and a real password manager with tested emergency access, digitized a real batch of documents to spec, and rehoused at least one fragile document in archival storage. Owning the tools without having configured and tested them is still Stage 1 competency.

Stage 3: Self-Sufficiency (Proficient)

Goal: genuine independent digital security judgment and real archival/research skill, the actual level Chapter 11's Tier 2 and Tier 3 assume a household has.

Digital Security: Self-Sufficiency

- **Begin CompTIA Security+ study:** Security+ is the recognized entry-level professional cybersecurity credential, covering network security fundamentals, cryptography basics, threat detection, and risk management; even partial study builds real judgment beyond following a checklist. CompTIA's own A+ Cyber track is a genuine on-ramp if Network+ (Security+'s formal prerequisite) feels like too large a first step.
- **Understand real threat modeling for your own household:** Move beyond generic advice to actually reasoning through your specific household's realistic threats (device theft, a compromised account, a lost backup drive) and whether your current setup actually addresses each one.
- **Practice a real data-recovery scenario:** Simulate a failed or lost primary device and actually walk through full recovery from your backups, timing how long real restoration takes versus how long you assumed it would.

Archival: Self-Sufficiency

- **Build real genealogical research skill:** Move beyond a single FamilySearch course to sustained, real research on your own family history, applying proper source citation and evidence-evaluation practices, the actual skill professional genealogists are certified on.
- **Understand notarization and its practical role:** Learn how notarization actually works and why it matters for certain documents (property, legal agreements), since Utah's own notary process is a real, accessible credential covered in Stage 4.
- **Build a genuinely resilient community-relevant archive:** Begin identifying which of your records (property boundaries, community agreements, if applicable) might matter beyond your own household, laying groundwork for Chapter 11's Tier 4 community records concept.

Stage 3 Learning Path

Resource	Cost / Format	Notes
CompTIA Security+ study material / exam voucher	Study material varies; exam ~$400	comptia.org/en-us/certifications/security. The recognized entry-level professional cybersecurity credential.
FamilySearch Learning Center (sustained research)	Free	Continue building on Stage 2's introductory course into real, sustained research practice.
Salt Lake City Family History Library	Free to visit and use	The world's largest genealogical library, operated by FamilySearch; a genuinely major regional resource worth visiting in person.

Northern Utah Note

The Family History Library in downtown Salt Lake City is free, open to the public regardless of religious affiliation, and staffed by knowledgeable volunteers; it's a substantially deeper resource than the online FamilySearch platform alone, and worth an in-person visit while building real Stage 3 research skill.

Self-Check: Ready for Stage 4?

You should be actively studying toward or have completed Security+, be able to reason through your household's real threat model rather than following a generic checklist, and have conducted sustained, properly sourced genealogical research rather than casual searching.

Stage 4: Mastery & Teaching (Expert)

Goal: professional-level credentials, the ability to teach others, and real capacity to build or maintain community-scale records infrastructure. This is the stage Chapter 11's Tier 4 (distributed community archive, records registry) actually depends on.

Teaching & Certification

- **Complete CompTIA Security+ certification:** The full credential (exam fee approximately $400) is a genuine, globally recognized professional standard, and is one of the certifications the U.S. Department of Defense accepts as an information assurance baseline; appropriate if digital security work is becoming a real vocation.
- **Become a commissioned Utah Notary Public:** A real, accessible state credential: pass Utah's notary exam ($95 fee), pass a background check, secure a $5,000 surety bond, and file an Oath of Office through the Office of the Lieutenant Governor; the 4-year commission is a genuinely useful community skill for legal document authentication, especially valuable during Chapter 15's post-disaster recovery period when professional services may be scarce.
- **Pursue Board for Certification of Genealogists credentialing if research has become a real skill:** The Certified Genealogist (CG) credential requires a portfolio-based evaluation by multiple independent reviewers against professional research, analysis, and writing standards; a serious, multi-year pursuit appropriate only if genealogical research has become genuinely important to you, not a general expectation.

Community-Scale Practice

- **Build the distributed community archive described in Chapter 11's Tier 4:** Chapter 11 calls for multiple physical archive locations and a maintained records registry so no single fire or flood erases community records; Stage 4 is where you help design and maintain that system, not just list it as a goal.
- **Teach digital security basics to your neighborhood:** A short, practiced walkthrough of encryption, password managers, and real 3-2-1 backups, taught to several households at once, meaningfully raises a whole neighborhood's baseline security.
- **Offer notarization as a real community service:** If commissioned as a notary, actually make that service known and available to neighbors, particularly useful during Chapter 15's post-disaster insurance and legal document period.

Stage 4 Learning Path

Resource	Cost / Format	Notes
CompTIA Security+ certification exam	~$400 exam fee	comptia.org. The full, globally recognized credential.
Utah Notary Public commission	$100–$225 total (exam, bond, supplies)	notary.utah.gov. A 4-year commission through the Office of the Lieutenant Governor.
Board for Certification of Genealogists (BCG)	Application and portfolio fees apply	bcgcertification.org. A serious, multi-year professional credential for genealogical research.

Self-Check: Have You Actually Arrived?

The real test of Stage 4 isn't the certification stack; it's whether you've actually taught digital security basics to another household that has since implemented real encryption and backups because of you, and whether your community has an actual distributed archive or records registry you helped build, not just a plan on paper.

A Suggested Learning Sequence

The two tracks (digital security, archival) don't have to move at the same pace. As a rough guide, not a requirement:

- **Weeks 1–2:** Stage 1: verify your real 3-2-1 backup, test password manager emergency access, identify your most fragile document.
- **1–3 months:** Stage 2: implement and test full-disk encryption, digitize a real document batch, rehouse your most fragile document in archival storage.
- **6–18 months:** Stage 3: begin Security+ study, build real household threat-modeling judgment, conduct sustained genealogical research.
- **Ongoing:** Stage 4: complete Security+ certification if digital security is becoming a real vocation, consider becoming a notary, and start teaching digital security basics to neighbors.

At a Glance: Digital Data & Documents Deep Dive

A single-page reference for planning purposes. This does not replace the detailed guidance above; use it to see how the four stages scale, and cross-reference against Chapter 11's tiers, which describe what a household needs

to have and do rather than how skilled it needs to be.

Stage	Focus	Key Milestone	Primary Resource
Stage 1: Foundations	Encryption and archival trade-off concepts, no implementation yet	Can explain 3-2-1 backup logic and digital vs. physical archive failure modes	EFF Surveillance Self-Defense guide
Stage 2: Applied Practice	Real, tested implementation of Chapter 11's systems	Full-disk encryption and password manager implemented and tested; a fragile document archived	Password manager, archival supplies
Stage 3: Self-Sufficiency	Real threat-modeling judgment and sustained research skill	Studying toward Security+; conducting sourced genealogical research	CompTIA Security+ study material
Stage 4: Mastery & Teaching	Professional credentials, community records infrastructure	Taught digital security to a neighbor; helped build a community archive	CompTIA Security+, Utah Notary Public