

# Standard Operating Procedure: Creating and Storing Electronic Records of Attested Written Wills

**Law Firm Name:** [Insert Firm Name]

**Effective Date:** January 1, 2026

**Last Revised:** [Date]

**Applies to:** North Carolina attested written wills under G.S. Chapter 31, Article 11

**Software Requirements:** Adobe Acrobat Pro, Adobe Sign subscription

---

## Purpose

This Standard Operating Procedure (SOP) establishes the firm's protocol for creating, signing, storing, and probating electronic records of attested written wills pursuant to Session Law 2025-33 and G.S. §§ 31-71 through 31-73. This procedure is designed to ensure the integrity and authenticity of electronically stored wills over their entire storage life.

---

## Scope

This SOP applies to all North Carolina attested written wills for which the client directs the firm to create an electronic record. It does not apply to:

- Holographic (handwritten) wills
  - Wills executed in other states (unless valid under NC law and client requests electronic storage)
  - Any will where the client does not provide express written authorization for electronic storage
- 

## Definitions

**Attested Written Will:** A will that meets the requirements of G.S. 31-3.3, signed by the testator and at least two witnesses.

**Electronic Record:** A digital file (typically PDF) of the attested written will, created at the testator's direction by a North Carolina-licensed attorney, accompanied by the attorney's certifying affidavit under G.S. 31-72.

**Certified Paper Copy:** A printed copy of the electronic record with a second certifying affidavit under G.S. 31-73, which can be offered for probate.

**SHA-256 Hash:** A cryptographic "fingerprint" of a digital file, used to verify the file has not been altered.

**Adobe Sign Certificate of Completion:** The audit trail and tamper-evident certificate automatically generated by Adobe Sign when a document is signed.

---

## **Roles and Responsibilities**

**Supervising Attorney:** The NC-licensed attorney who will sign the G.S. 31-72 affidavit. This attorney is responsible for verifying all steps are completed correctly.

**Paralegal/Legal Assistant:** May perform Steps 1-4 and Steps 9-11 under attorney supervision.

**IT/Records Manager:** Responsible for long-term storage, backup verification, and maintaining the Electronic Will Register.

---

## **Materials and Software Required**

- Original executed attested written will (paper document)
  - High-quality scanner (minimum 300 dpi, preferably 600 dpi)
  - Adobe Acrobat Pro (current version)
  - Adobe Sign subscription (active)
  - Access to firm document management system
  - Access to secure cloud backup (if different from DMS)
  - Windows PowerShell or Mac Terminal (for hash generation)
  - Electronic Will Register (spreadsheet or database - see Appendix A)
- 

## **Procedure**

### **PHASE 1: PREPARATION AND CLIENT AUTHORIZATION**

#### **Step 1: Confirm Client Authorization**

**WHO:** Supervising Attorney

**WHEN:** Before creating the electronic record

#### **Actions:**

1.1. Review the executed will to confirm it is a valid attested written will under G.S. 31-3.3 (signed by testator and at least two witnesses).

1.2. Discuss the electronic storage option with the client, including:

- The client will lose the ability to revoke the will by physical destruction (G.S. 31-72(b))
- The electronic record eliminates the presumption of revocation if the original will is lost
- The firm's storage and security practices
- No additional cost for this service [or state your fee policy]

1.3. Obtain the client's **written authorization** to create an electronic record. This can be documented by:

- A signed engagement letter provision, OR
- A separate authorization form signed by the client (see Appendix B for template)

1.4. Document the authorization in the client file and in the Electronic Will Register.

**QUALITY CHECK:** Do not proceed without written client authorization.

---

## **Step 2: Prepare the Attorney's First Affidavit (G.S. 31-72)**

**WHO:** Supervising Attorney

**WHEN:** Immediately after Step 1

### **Actions:**

2.1. Prepare the attorney's affidavit on firm letterhead using the template in Appendix C. The affidavit must state:

- That the electronic record is a complete, true, and accurate copy of the attested written will
- That the testator expressly authorized the attorney to create the electronic record
- That the testator has been advised that electronic storage eliminates the ability to revoke by physical act

2.2. Have the affidavit notarized. The supervising attorney must sign the affidavit in the presence of a notary.

2.3. Physically attach the notarized affidavit to the original executed will using a staple or permanent binding method. The affidavit becomes part of the physical document that will be scanned.

**QUALITY CHECK:** The affidavit must be physically attached before scanning. Do not proceed to scanning without the attached, signed, and notarized affidavit.

---

## **PHASE 2: SCANNING AND FILE CREATION**

### **Step 3: Scan the Will and Attached Affidavit**

**WHO:** Paralegal/Legal Assistant or Supervising Attorney

**WHEN:** Immediately after Step 2

## **Actions:**

### 3.1. Prepare the scanner:

- Set resolution to **600 dpi** (minimum 300 dpi)
- Set color mode to **color** or **grayscale** (not black and white)
- Set file format to **PDF**

### 3.2. Scan the entire document in this order:

- All pages of the executed will
- All witness signature pages
- Self-proving affidavit (if present)
- Attorney's first affidavit (G.S. 31-72)
- Any exhibits or attachments

### 3.3. Review the scanned PDF on screen to ensure:

- All pages are present and in correct order
- All text is legible
- All signatures are clearly visible
- No pages are cut off or obscured
- File size is reasonable (typically 2-10 MB for a standard will)

### 3.4. Save the scanned PDF with the following naming convention:

[LastName][FirstName]\_Will\_Executed\_[YYYYMMDD]\_ORIGINAL.pdf

Example: SmithJohn\_Will\_Executed\_20260115\_ORIGINAL.pdf

### 3.5. Save this file to the client's matter folder in the document management system.

**QUALITY CHECK:** Open the PDF and visually confirm every page is legible before proceeding.

---

## **Step 4: Convert to PDF/A Format**

**WHO:** Paralegal/Legal Assistant or Supervising Attorney

**WHEN:** Immediately after Step 3

## **Actions:**

4.1. Open the scanned PDF in Adobe Acrobat Pro.

4.2. Convert to PDF/A using either Method A or Method B:

**Method A - Save As:**

- Go to **File > Save As Other > Archivable PDF (PDF/A)**
- Choose **PDF/A-2b** from the options
- Save the file with the naming convention:

[LastName][FirstName]\_Will\_Executed\_[YYYYMMDD]\_PDF/A.pdf

Example: `SmithJohn\_Will\_Executed\_20260115\_PDF/A.pdf`

**Method B - Preflight Tool:**

- Go to **Tools > Print Production > Preflight**
- In the Preflight dialog, search for "PDF/A"
- Select **"Convert to PDF/A-2b"**
- Click **Analyze and Fix**
- Save the file with the naming convention above

4.3. Verify PDF/A conversion:

- With the file still open in Acrobat, look for a blue banner at the top stating "This file complies with PDF/A standard"
- If you do not see this banner, repeat the conversion process

4.4. Close the ORIGINAL.pdf file. From this point forward, work only with the PDF/A.pdf file.

**QUALITY CHECK:** Confirm the PDF/A banner is visible before proceeding.

---

**PHASE 3: ELECTRONIC SIGNATURE USING ADOBE SIGN**

**Step 5: Prepare the Document for Adobe Sign**

**WHO:** Supervising Attorney or authorized staff

**WHEN:** Immediately after Step 4

**Actions:**

5.1. Open the PDF/A.pdf file in Adobe Acrobat Pro.

5.2. Go to **Tools > Prepare Form** or **Tools > Fill & Sign**.

5.3. Review the document one final time to ensure it is the correct, complete PDF/A file with all pages present.

5.4. Navigate to **Tools > Adobe Sign** or select **Fill & Sign > Work With Adobe Sign > Send for Signature**.

**Note:** Your firm's Adobe Acrobat Pro interface may vary slightly depending on version and Adobe Sign integration settings. Consult IT if the Adobe Sign option is not visible.

---

## **Step 6: Configure the Adobe Sign Request**

**WHO:** Supervising Attorney or authorized staff

**WHEN:** Continuation of Step 5

### **Actions:**

6.1. In the Adobe Sign interface, configure the signature request:

### **Recipients:**

- Add the supervising attorney's email address as the only signer
- Message to signer: "Electronic Record Certification - [Client Name] - G.S. 31-72 Affidavit"
- Set authentication: "Password" or "Identity Verification" if required by firm policy

### **Document Settings:**

- Document name: [[LastName]][FirstName]\_Will\_ElectronicRecord\_GS31-72
- Message field: "This electronic record is being signed pursuant to G.S. 31-72 to create an electronically stored will for [Client Name]. The attorney's first affidavit is included as part of this document."

### **Signature Placement:**

- Adobe Sign will prompt you to place signature fields on the document
- Place a signature field on the attorney's first affidavit page, in the space labeled for the attorney's signature
- **CRITICAL:** Even though the affidavit was already signed on paper, the electronic signature via Adobe Sign is what creates the tamper-evident seal and audit trail
- Add a date field next to the signature field

6.2. Review the document one more time in the Adobe Sign preview window.

6.3. Click **Send** to initiate the signing process.

**QUALITY CHECK:** Verify the correct attorney email is listed as signer and the signature field is placed correctly on the affidavit page.

---

### **Step 7: Attorney Signs the Document via Adobe Sign**

**WHO:** Supervising Attorney

**WHEN:** Same day as Step 6 (do not delay)

**Actions:**

7.1. The supervising attorney will receive an email from Adobe Sign with the subject line similar to: "Please sign [Client Name] Electronic Will Record."

7.2. Open the email and click "**Review and Sign**".

7.3. Adobe Sign will open in a browser window, displaying the PDF.

7.4. Review the entire document one final time to ensure:

- It is the correct client's will
- All pages are present
- The attorney's first affidavit (G.S. 31-72) is attached and complete
- You are comfortable certifying this as a complete, true, and accurate electronic record

7.5. Click in the signature field. Adobe Sign will prompt you to:

- Type your name, draw your signature, or upload a signature image
- Select your preferred signature style

7.6. Click "**Click to Sign**" to apply your electronic signature.

7.7. Review the completed document and click "**Finish**" or "**Click to Finish**".

7.8. Adobe Sign will process the document and send a confirmation email to you with the subject "Signed: [Document Name]."

**QUALITY CHECK:** Do not click "Finish" until you have reviewed the complete document and confirmed it is correct.

---

### **Step 8: Download and Store the Signed Electronic Record**

**WHO:** Paralegal/Legal Assistant or Supervising Attorney

**WHEN:** Within 1 hour of Step 7 completion

## Actions:

8.1. Open the confirmation email from Adobe Sign (sent to the supervising attorney).

8.2. Download two documents from the Adobe Sign confirmation email:

- The **signed PDF** (this is the electronically stored will)
- The **Certificate of Completion** (this is Adobe Sign's audit trail)

8.3. Rename the signed PDF using this naming convention:

[LastName][FirstName]\_Will\_Executed\_[YYYYMMDD]\_SIGNED.pdf

Example: SmithJohn\_Will\_Executed\_20260115\_SIGNED.pdf

8.4. Rename the Certificate of Completion using this naming convention:

[LastName][FirstName]\_Will\_AdobeSignCertificate\_[YYYYMMDD].pdf

Example: SmithJohn\_Will\_AdobeSignCertificate\_20260115.pdf

8.5. Verify the signed PDF:

- Open the file in Adobe Acrobat or Adobe Reader
- You should see a blue banner at the top stating "Signed and all signatures are valid" or similar language
- If you see a yellow or red warning, STOP and consult with IT or the supervising attorney

8.6. Save both files to the client's matter folder in the document management system.

**QUALITY CHECK:** Confirm the blue "valid signature" banner appears before proceeding.

---

## PHASE 4: HASH GENERATION AND DOCUMENTATION

### Step 9: Generate the SHA-256 Hash

**WHO:** Paralegal/Legal Assistant, Supervising Attorney, or IT

**WHEN:** Immediately after Step 8

## Actions:

9.1. Locate the signed PDF file (the \_SIGNED.pdf file from Step 8.3).

9.2. Generate the SHA-256 hash using the appropriate method for your computer:

## For Windows:

- Press the Windows key and type "PowerShell"
- Open Windows PowerShell
- Type the following command, replacing the path with the actual path to your file:

```
Get-FileHash "C:\Path\To\File\SmithJohn_Will_Executed_20260115_SIGNED.pdf" -Algorithm SHA256
```

- Press Enter
- The hash will appear on screen as a long string of letters and numbers (64 characters)
- Copy this hash string

**For Mac:**

- Open Terminal (Applications > Utilities > Terminal)
- Type the following command, replacing the path with the actual path to your file:

```
shasum -a 256 /Path/To/File/SmithJohn_Will_Executed_20260115_SIGNED.pdf
```

- Press Enter
- The hash will appear on screen
- Copy this hash string

9.3. Immediately document the hash by creating a Hash Verification Memo (see template in Appendix D). The memo should include:

- Client name
- Date will was executed
- Date electronic record was created
- SHA-256 hash (the full 64-character string)
- Statement: "This hash can be used to verify that the electronic record has not been altered since the date of creation."

9.4. The supervising attorney must sign and date the Hash Verification Memo.

9.5. Save the Hash Verification Memo using this naming convention:

```
[LastName][FirstName]_Will_HashVerification_[YYYYMMDD].pdf
```

Example: SmithJohn\_Will\_HashVerification\_20260115.pdf

9.6. Store the Hash Verification Memo in three places:

- In the document management system with the electronic will files
- Print a copy for the physical client file
- Email a copy to the supervising attorney (creating a dated email record)

**QUALITY CHECK:** Verify the hash string is 64 characters long and has been recorded accurately.

---

### **Step 10: Update the Electronic Will Register**

**WHO:** Paralegal/Legal Assistant or IT/Records Manager

**WHEN:** Same day as Step 9

#### **Actions:**

10.1. Open the firm's Electronic Will Register (spreadsheet or database).

10.2. Create a new entry with the following information:

- Client name
- Matter number
- Date will was executed
- Date electronic record was created
- Testator date of birth
- Supervising attorney name
- File location in DMS (exact path/folder)
- Backup location (if different)
- SHA-256 hash (full 64-character string)
- Adobe Sign transaction ID (found on Certificate of Completion)
- Next verification date (recommend: 1 year from creation)
- Status: "Active"
- Notes field (for any relevant information)

10.3. Save the Electronic Will Register.

10.4. If using a spreadsheet, ensure it is saved in a secure, backed-up location accessible only to authorized personnel.

**QUALITY CHECK:** Confirm the entry is complete and all information matches the source documents.

---

## PHASE 5: LONG-TERM STORAGE AND BACKUP

### Step 11: Store Files in Multiple Secure Locations

**WHO:** IT/Records Manager or Paralegal/Legal Assistant

**WHEN:** Same day as Step 10

#### Actions:

11.1. Ensure the following files are saved in the client's matter folder in the primary document management system:

- Original scanned PDF (the ORIGINAL.pdf file)
- PDF/A version (the \_PDFA.pdf file) - optional; can be deleted if desired
- Signed PDF (the \_SIGNED.pdf file) - **PRIMARY DOCUMENT**
- Adobe Sign Certificate of Completion
- Hash Verification Memo
- Client authorization form

11.2. Create a backup of the signed PDF in at least one additional location:

- Firm's secure cloud backup system (e.g., encrypted folder in Microsoft OneDrive, Dropbox, NetDocuments)
- OR secondary firm server
- OR secure external backup maintained by IT

11.3. Verify the backup was successful by navigating to the backup location and confirming the file is present and can be opened.

11.4. Document the backup location(s) in the Electronic Will Register.

11.5. Update the client's physical file to include:

- Printed copy of the Hash Verification Memo
- Note indicating the will has been electronically stored with file location(s)

**QUALITY CHECK:** Open the backed-up file from the backup location to confirm it is the correct, complete file.

---

### Step 12: Communicate with the Client

**WHO:** Supervising Attorney

**WHEN:** Within 3 business days of completing Step 11

**Actions:**

12.1. Send a letter or email to the client confirming:

- The electronic record has been created and stored
- The locations where the electronic record is stored
- The client can no longer revoke the will by physical destruction
- The client should notify the firm immediately if they wish to revoke or amend the will
- Instructions for how to contact the firm if they have questions

12.2. Include a copy of the Hash Verification Memo with the communication (optional but recommended).

12.3. File a copy of this communication in the client's matter folder.

---

## **PHASE 6: ONGOING MAINTENANCE AND VERIFICATION**

### **Step 13: Annual Verification Procedure**

**WHO:** IT/Records Manager or designated staff

**WHEN:** Annually, on or near the anniversary of the electronic record's creation

**Actions:**

13.1. Review the Electronic Will Register and identify all wills due for annual verification.

13.2. For each will requiring verification:

- Locate the signed PDF in the document management system
- Open the PDF in Adobe Acrobat or Adobe Reader
- Verify the Adobe Sign signature banner shows as valid (blue banner, no warnings)
- Regenerate the SHA-256 hash using the same method as Step 9
- Compare the newly generated hash to the hash recorded in the Hash Verification Memo and Electronic Will Register
- If the hashes match and the signature is valid, update the Electronic Will Register with "Verified [Date]" in the notes field
- If the hashes do NOT match or the signature shows as invalid, immediately notify the supervising attorney and follow the troubleshooting procedure in Appendix E

13.3. Document each verification in the Electronic Will Register.

13.4. Set the next verification date for one year from the current verification date.

**QUALITY CHECK:** Any discrepancy between the original hash and the newly generated hash must be immediately escalated to the supervising attorney.

---

## **PHASE 7: PROBATE PROCEDURE (AFTER TESTATOR'S DEATH)**

### **Step 14: Prepare the Certified Paper Copy for Probate**

**WHO:** Supervising Attorney (may be a different attorney than the one who created the electronic record)

**WHEN:** After notification of testator's death

#### **Actions:**

14.1. Locate the electronically stored will in the document management system using the Electronic Will Register.

14.2. Verify the file's integrity before printing:

- Open the signed PDF (the SIGNED.pdf file)
- Confirm the Adobe Sign signature shows as valid (blue banner)
- Regenerate the SHA-256 hash and compare to the hash recorded in the Hash Verification Memo and Electronic Will Register
- If either verification fails, STOP and consult with another attorney before proceeding

14.3. Print the signed PDF on standard 8.5" x 11" paper using a high-quality printer:

- Use the "actual size" setting (do not scale to fit)
- Print in color if the original was in color
- Use at least 24 lb paper (standard copy paper is acceptable)

14.4. Review the printed document page by page to ensure:

- All pages printed correctly
- All text and signatures are legible
- Page order is correct
- No pages are missing

14.5. Prepare the attorney's second affidavit (G.S. 31-73) using the template in Appendix F. This affidavit must state:

- That the printed paper copy is a complete, true, and accurate copy of the electronically stored will

- The attorney's name and NC bar number
- The date

14.6. Have the second affidavit notarized. The attorney must sign in the presence of a notary.

14.7. Attach the notarized second affidavit to the printed certified paper copy using a staple or binding.

14.8. The certified paper copy is now ready to be filed with the Clerk of Superior Court for probate in accordance with G.S. 28A-2A-8(a1).

**QUALITY CHECK:** Before filing for probate, verify both the digital signature validity and the hash match. If either fails, consult with another attorney and consider whether the paper original can still be located.

---

### **Step 15: Retain Records After Probate**

**WHO:** IT/Records Manager

**WHEN:** After probate is complete

#### **Actions:**

15.1. After the will has been admitted to probate, update the Electronic Will Register:

- Change status from "Active" to "Probated"
- Record the date of death
- Record the date probate was granted
- Record the county where probate occurred
- Record the file number

15.2. Retain all electronic files in accordance with the firm's document retention policy and North Carolina rules of professional conduct.

15.3. Do not delete the electronic record or related files unless and until the firm's retention period has expired AND all estate administration is complete AND all potential claims periods have expired.

**Recommended Retention Period:** Indefinitely, or at minimum 10 years after estate administration is closed.

---

### **Troubleshooting**

**Issue:** Adobe Sign signature shows as invalid

#### **Possible Causes:**

- File was modified after signing

- Adobe Sign certificate has expired
- File corruption during storage or transfer

**Actions:**

1. Regenerate the SHA-256 hash and compare to the original hash
  2. If hashes match, the file content is unchanged; the signature issue may be technical (certificate expiration, software update)
  3. If hashes do NOT match, the file has been altered
  4. Retrieve the Adobe Sign Certificate of Completion and review the audit trail
  5. Check backup copies of the file
  6. Consult with IT and the supervising attorney
  7. Consider whether the paper original is still available
- 

**Issue: Hash does not match**

**Possible Causes:**

- File was modified (intentionally or inadvertently)
- File was corrupted
- Wrong file was verified
- Hash was recorded incorrectly initially

**Actions:**

1. Verify you are checking the correct file (confirm file name and location)
2. Check backup copies of the file and regenerate their hashes
3. Review Adobe Sign Certificate of Completion to see if any modifications were logged
4. If all backup copies show the same new hash, the Hash Verification Memo may have been recorded incorrectly initially (unlikely but possible)
5. If backup copies have different hashes from each other, file corruption or tampering is likely
6. Consult with the supervising attorney immediately
7. Document all findings

**CRITICAL:** Never proceed to probate if the hash does not match without a full investigation and attorney approval.

---

## **Issue: File cannot be located**

### **Possible Causes:**

- File was moved or renamed
- Storage system failure
- Accidental deletion

### **Actions:**

1. Search the document management system using client name, matter number, and all known file name variations
  2. Check backup locations listed in the Electronic Will Register
  3. Check Adobe Sign account history to re-download the signed document
  4. Contact IT to search backup systems
  5. If file cannot be located, determine whether the paper original will is still available
  6. Document all efforts to locate the file
- 

## **Record Keeping Requirements**

The following records must be retained for each electronically stored will:

### **Digital Files:**

- Signed PDF (the \_SIGNED.pdf file) - PRIMARY DOCUMENT
- Adobe Sign Certificate of Completion
- Hash Verification Memo

### **Physical Files:**

- Original executed will (paper) - should be retained unless client specifically requests return
- Printed Hash Verification Memo
- Client authorization for electronic storage
- Attorney's notarized first affidavit (original - if not returned to client with paper will)

### **Electronic Will Register:**

- Complete entry for each electronically stored will

**Retention Period:** See Step 15 above.

---

## Training and Competency

All personnel involved in this procedure must:

- Complete training on this SOP before performing any steps
- Demonstrate competency in using Adobe Acrobat Pro and Adobe Sign
- Understand the legal requirements of G.S. Chapter 31, Article 11
- Know when to escalate issues to the supervising attorney

**Initial Training:** Required before first use

**Refresher Training:** Annually, or when this SOP is updated

---

## Revision History

Version	Date	Description of Changes	Approved By
1.0	[Date]	Initial SOP created	[Name]

---

## Appendices

### Appendix A: Electronic Will Register Template

The Electronic Will Register should be maintained as a secure spreadsheet or database with the following columns:

Column Name	Data Type	Description	Example
Client Name	Text	Last, First	Smith, John
Matter Number	Text	Firm's matter numbering system	2026-0015
Testator DOB	Date		01/15/1965
Will Execution Date	Date	Date will was signed	01/15/2026
Electronic Record Created Date	Date	Date electronic record was created	01/17/2026
Supervising Attorney	Text	Attorney who signed G.S. 31-72 affidavit	Jane Doe
File Location	Text	Full path in DMS	Clients/Smith_John/Estate_Planning/Wills/
Backup Location	Text	Secondary storage location	Azure_Backup/Wills/
SHA-256 Hash	Text	Full 64-character hash	abc123def456...
Adobe Sign Transaction ID	Text	From Certificate of Completion	ABCD-1234-EFGH-5678
Status	Dropdown	Active / Probated / Revoked	Active
Last Verified Date	Date	Date of most recent verification	01/17/2027
Next Verification Date	Date		01/17/2028
Date of Death	Date	If applicable	
Probate Date	Date	If applicable	
Probate County	Text	If applicable	Wake County
Probate File Number	Text	If applicable	26-E-0123
Notes	Text	Any relevant information	Client relocated to Florida 2027

**Access Control:** Limit access to supervising attorneys, IT/Records Manager, and authorized staff only.

**Backup:** Back up the Electronic Will Register at least weekly.



ATTORNEY'S AFFIDAVIT FOR ELECTRONIC STORAGE OF WILL

(Pursuant to N.C. Gen. Stat. § 31-72)

STATE OF NORTH CAROLINA

COUNTY OF [COUNTY NAME]

I, [ATTORNEY NAME], being duly sworn, depose and state as follows:

1. I am an attorney licensed to practice law in the State of North Carolina. My North Carolina State Bar number is [NUMBER].

2. I am a member in good standing of the North Carolina State Bar.

3. I have created an electronic record of the attested written will of [TESTATOR NAME] ("Testator"), which will was executed on [DATE OF EXECUTION].

4. The electronic record that I have created is a complete, true, and accurate copy of the Testator's attested written will, including all pages, signatures, and attachments.

5. The Testator expressly authorized me to create an electronic record of the Testator's attested written will.

6. I have advised the Testator that the creation of an electronic record of the Testator's attested written will eliminates the Testator's ability to revoke the attested written will by physical act pursuant to N.C. Gen. Stat. § 31-5.1(2).

7. This affidavit is made for the purpose of establishing the authenticity and accuracy of the electronic record of the Testator's will in accordance with N.C. Gen. Stat. § 31-72.

\_\_\_\_\_  
[ATTORNEY NAME]

\_\_\_\_\_  
Date

Attorney for Testator

NC State Bar No. [NUMBER]

Sworn to and subscribed before me

this \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_.

\_\_\_\_\_  
Notary Public

My Commission Expires: \_\_\_\_\_

[NOTARY SEAL]

## Appendix D: Hash Verification Memo Template

[LAW FIRM LETTERHEAD]

### HASH VERIFICATION MEMORANDUM

Date: [DATE]

Re: Electronic Storage of Will – [CLIENT NAME]

Matter: [MATTER NUMBER]

This memorandum documents the cryptographic hash of the electronic record created for the above-referenced matter.

#### WILL INFORMATION:

- Testator: [CLIENT NAME]
- Date of Birth: [DOB]
- Will Execution Date: [DATE]
- Electronic Record Creation Date: [DATE]

#### FILE INFORMATION:

- Filename: [Exact filename]
- File Location: [Full path in DMS]
- Backup Location: [Secondary location]

#### HASH VERIFICATION:

The SHA-256 cryptographic hash of the signed electronic record as of [DATE] is:

[INSERT FULL 64-CHARACTER HASH HERE]

This hash serves as a unique digital fingerprint of the electronic record. It can be used at any future date to verify that the file has not been altered, corrupted, or tampered with since the date it was created.

To verify the file's integrity at a future date, regenerate the SHA-256 hash using the same file and compare it to the hash recorded above. If the hashes match exactly, the file is unchanged.

#### VERIFICATION INSTRUCTIONS:

Windows: Get-FileHash "[filepath]" -Algorithm SHA256

Mac: shasum -a 256 [filepath]

Prepared by: [NAME]

Supervising Attorney: [ATTORNEY NAME]

[ATTORNEY SIGNATURE]

Date

---

## Appendix E: File Integrity Investigation Checklist

Use this checklist if a hash mismatch or signature validation failure is discovered:

- Verify the correct file is being checked (confirm filename and location)
- Verify the hash was copied correctly from the original memo
- Check all backup copies and regenerate their hashes
- Document the hash of each backup copy
- Compare all hashes to each other and to the original recorded hash
- Review Adobe Sign Certificate of Completion for any logged modifications or access
- Check DMS audit logs for file access and modification history
- Interview staff who had access to the file
- Determine when the file was last verified successfully
- Determine if any software updates, migrations, or system changes occurred
- Document all findings in writing
- Consult with supervising attorney before any further action
- Consider whether paper original is still available
- Consider consulting with IT forensics specialist if intentional tampering suspected

---

## Appendix F: Attorney's Second Affidavit Template (G.S. 31-73)

[LAW FIRM LETTERHEAD OR NOTARY FORMAT]

ATTORNEY'S CERTIFICATION OF PAPER COPY OF ELECTRONICALLY STORED WILL

(Pursuant to N.C. Gen. Stat. § 31-73)

STATE OF NORTH CAROLINA

COUNTY OF [COUNTY NAME]

I, [ATTORNEY NAME], being duly sworn, depose and state as follows:

1. I am an attorney licensed to practice law in the State of North Carolina. My North Carolina State Bar number is [NUMBER].

2. I am a member in good standing of the North Carolina State Bar.

3. The decedent, [TESTATOR NAME], died on [DATE OF DEATH].

4. The attached document is a paper copy of an attested written will of [TESTATOR NAME] that was stored as an electronic record pursuant to N.C. Gen. Stat. § 31-72.

5. I certify that the attached paper copy is a complete, true, and accurate copy of the attested written will of [TESTATOR NAME] that was stored as an electronic record, including the certifying affidavit of the attorney who created the electronic record.

6. [OPTIONAL: The electronic signature on the certifying affidavit was verified as valid on [DATE], and the SHA-256 hash of the electronic record matched the hash recorded at the time of creation, confirming the file has not been altered.]

7. This certification is made for the purpose of offering the attached certified paper copy for probate in accordance with N.C. Gen. Stat. §§ 31-73 and 28A-2A-8(a1).

\_\_\_\_\_  
[ATTORNEY NAME]

\_\_\_\_\_  
Date

NC State Bar No. [NUMBER]

Sworn to and subscribed before me

this \_\_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
Notary Public

My Commission Expires: \_\_\_\_\_

[NOTARY SEAL]

---

## Questions or Issues

If you have questions about this SOP or encounter issues not addressed in the troubleshooting section, contact:

**Primary Contact:** [Name, Title]

**Email:** [Email]

**Phone:** [Phone]

**For technical/IT issues:** [IT Contact]

**For legal questions:** [Managing Partner or Ethics Committee]

---

*This SOP is based on North Carolina Session Law 2025-33 and G.S. Chapter 31, Article 11. It should be reviewed and updated as needed to reflect changes in law, technology, or firm practice. Attorneys should exercise independent professional judgment in implementing this procedure.*

*Last Updated: [Date]*