PRACTITIONER RESOURCE

The Litigation Counsel ESI Preservation and Spoliation Defense Protocol

Coordinate legal authority, custodians, devices and cloud records for matters in Florida state courts and federal court, with the questions counsel and the preservation team answer together.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/preservation/

A preservation notice is the start of the record. Proving that the right systems were covered, that deletion stopped and that every collection can be explained takes the technical follow through this protocol lays out. It connects counsel's instructions to named technical owners, identifiable sources and documented verification, for matters in Florida state courts and in federal court. GDF examiners work alongside legal counsel, internal auditors and corporate IT security teams to preserve the evidence and document exactly what the record holds.

The time bands below organize the urgent work of the first forty eight hours; move faster wherever a source is about to expire. Counsel sets the preservation duty, the forum and the authorized scope, and the preservation record documents the actions taken, the sources retained and the questions counsel needs to address.

1. First Two Hours: Establish Authority and Stop Unrecorded Changes

Name the lawyer directing preservation, the business owner responsible for execution and the technical lead who can reach the relevant systems. Record the known dispute, the events that prompted action, the sources at immediate risk and the time each instruction was received. Give IT a specific instruction to pause relevant device reuse, account deletion, mailbox conversion and scheduled disposal while scope is settled. Keep the instruction targeted so the business keeps operating. The useful record identifies what was stopped, who stopped it, when the change became effective and which processes continue to run.

Require each owner to acknowledge the instruction and identify exceptions. A complete response that a mailbox is retained names the account identity, covered locations, applicable configuration and evidence that the control is active. Mark any source an administrator has yet to confirm as unresolved and assign an escalation time. Treat preservation as complete once every source is confirmed.

2. Define the Disputed Facts Before Narrowing the Sources

Translate the matter into the questions the evidence must answer. Identify the people, relevant period, business systems, transactions and communications involved. Include shared mailboxes, delegated accounts, collaboration spaces, mobile applications, shared drives and systems operated by outside providers when they may hold relevant records. Distinguish data the organization controls from material it can only request. Once counsel sets the legal boundaries, the technical team maps them to actual account identifiers and storage locations.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Write down the initial assumptions behind any date or keyword restriction. A narrow search that misses aliases, attachments, linked documents or a shared workspace can leave a misleading impression of completeness. Broader preservation and narrower review may be appropriate where authorized and proportionate. Record why a source was included or excluded and set a time to revisit the decision as facts develop.

3. Separate Federal and Florida Preservation Analysis

In federal court, Rule 37(e) of the Federal Rules of Civil Procedure governs electronically stored information that should have been preserved, was lost because a party failed to take reasonable steps and cannot be restored or replaced through additional discovery. Florida state courts apply the same structure under Fla. R. Civ. P. 1.380(f) in the October 1, 2026 edition of the Florida Rules of Civil Procedure. On a finding of prejudice the court may order measures no greater than necessary to cure it, and only on a finding that a party acted with intent to deprive may it presume the lost information was unfavorable, instruct the jury on that presumption, or dismiss the action or enter a default judgment. [1] [2]

Florida discovery rules put the source register to work early. Initial discovery disclosures under Fla. R. Civ. P. 1.280(a) include a copy, or a description by category and location, of the electronically stored information a party may use to support its claims or defenses, due within 60 days after service of the complaint or joinder unless the court sets a different time. Under Fla. R. Civ. P. 1.280(e), a party may object to discovery of ESI from sources it identifies as not reasonably accessible because of burden or cost, and Fla. R. Civ. P. 1.350(b)(8) lets the requesting party specify the form of production. A preservation record that shows reasonable steps, source by source, is the evidence that answers a motion under either court's rules. [2]

4. Hours Two Through Six: Convert the Hold Into Executable Instructions

Send each system owner a source specific instruction identifying the custodian, account or workspace, the relevant period and the action required. Address retention settings, device refresh schedules, backup expiration, collaboration history, mailbox rules and any pending employee departure. Require the owner to retain the original configuration record before making a necessary change, document the replacement configuration and explain the expected effect. Preserve the instructions and responses alongside the technical evidence rather than relying on recollection.

The execution record should distinguish notice sent, acknowledgment received, control configured and control verified. Those are different events. If a scheduled purge may occur before a hold is effective, escalate the timing immediately and agree on a lawful interim preservation method. Show that deletion was prevented with the active configuration record.

5. Preserve Microsoft 365 Content and Activity Separately

Have an authorized administrator identify the relevant Exchange mailboxes, OneDrive accounts, SharePoint sites and Teams associated locations. Use the appropriate preservation controls for those locations and verify licensing, scope, deployment status and errors. Microsoft states that a new eDiscovery hold can take up to 24 hours to take effect. Treat that interval as an operational issue requiring an explicit plan for expiring material. Preserve the hold definition, location identifiers, status records and later changes. Tenant activity logs need a preservation step of their own, because a content hold covers content. [3]

© 2026 Global Digital Forensics, Inc. All rights reserved.

Assign a separate owner to preserve available audit, identity and security records. Record the actual coverage, earliest available time, export method and any failures. Microsoft audit retention depends on licensing, workload and policy, so confirm activity history retention separately from the mailbox hold. Keep the query, returned files and export record together. Where a gap exists, identify other lawful sources that might corroborate the event. [4]

6. Preserve Google Workspace With Its Account Context

For an authorized Google Workspace matter, identify the accounts, shared drives and supported services that require preservation. Confirm Vault entitlement, administrative scope and the actual hold configuration rather than treating an active Workspace account as a preservation control. Google describes holds as service specific and distinguishes their operation from retention rules. Protect relevant licensing and account state during offboarding, and verify the current administrative workflow before any deletion or downgrade. A hold protects what exists when it takes effect, which is why speed matters. [5]

Map Gmail, Drive, Chat and other relevant records separately. Google documents which service data Vault supports; for example, Chat coverage depends on supported message conditions. Linked content and files owned outside the organization require separate attention. Preserve available activity exports and ownership information, and record any inaccessible source. List linked files, shared conversations and external records as sources separate from the custodian's mailbox export. [6]

7. Make Mobile and Volatile Evidence Decisions Before Routine Handling

Identify phones and computers that may hold unique messages, application data or active session information. Record who has possession and the observable power, lock and connection state, leaving the device as it is. Escalate decisions about network isolation, power changes and acquisition to a qualified examiner who understands the device and the operational risk. Turning a device off, interacting with it or allowing it to remain connected can each affect preservation. The examiner fits that decision to the actual device and circumstances. NIST's mobile guidance sets the foundation, and the examiner confirms current tool support for the specific handset and operating system. [7]

For a running computer, volatile evidence collection can itself alter the system, while shutdown can remove information that exists only in memory. A technical lead should weigh those consequences against active harm and record the decision. Containment that protects people, essential operations or continuing exposure comes first, and collection is planned around it. Keep the reason, authorization and precise actions in the event record. [8]

8. Hours Six to Twenty Four: Collect Under a Reproducible Protocol

Before collection, identify the account or device, the lawful authority, the requested scope, the acquisition method and the person responsible. Preserve native records and associated metadata where available, together with export reports, errors and source identifiers. Record software versions, relevant settings and the distinction between a full acquisition and a selective export. Describe each collection by what it captured, so a selective export of visible documents carries that label throughout the matter.

© 2026 Global Digital Forensics, Inc. All rights reserved.

For cloud collections, retain the request parameters, job identifiers, location list, status reports, returned packages and exception records. Reconcile what the provider reports with what was actually received. If items were skipped, unavailable or encrypted, preserve that information and agree on the next step. Reconciliation against the source list, beyond a successful job status, shows that every relevant source and item arrived.

9. Build Chain of Custody Around Every Meaningful Transfer

Assign a stable evidence identifier at receipt. Record the source, custodian, collector, acquisition time and time zone, method, storage location, access restrictions and every transfer of possession or control. For each exported package or acquisition file, record an appropriate cryptographic hash and verify it at relevant transfers. Retain the original acquisition and conduct examination on controlled copies where practicable. A hash proves that a particular set of bytes is unchanged; authorship, completeness and truth each rest on other evidence the examiner documents.

In federal court, Federal Rules of Evidence 901 and 902 provide the routes for authentication, including certification of electronic records and copied data under Rules 902(13) and 902(14). [9] In Florida state court, Fla. Stat. 90.901 requires evidence sufficient to support a finding that the matter is what its proponent claims, and 90.902(11) allows a business record to be authenticated by a certification or declaration from the custodian or another qualified person, provided the offering party serves the reasonable written notice that 90.803(6)(c) requires. Florida has no counterpart to federal Rules 902(13) and 902(14), so in state court the examiner's testimony and the custody record carry the foundation for collected data. Agree early with counsel on the foundation the intended use needs. [10] [11] [12]

10. Hours Twenty Four Through Forty Eight: Reconcile the Preservation Record

Bring the hold instructions, acknowledgments, configured controls and received collections into one source register. Give each source an explicit status such as verified preserved, collection pending, inaccessible, already expired or further scope decision required. Attach the supporting receipt and identify who will close each open issue. Revisit scheduled deletion, account changes and device reuse before ordinary operations resume. The purpose is a record another professional can follow without depending on the memory of the person who performed the work.

If information appears lost, preserve the facts of the loss and identify possible alternative sources such as another participant's account, a retained export, an authorized backup or a business system that recorded the same event. Document what was attempted, what was recovered and what remains open. Label any later export or reconstructed document as such and keep it beside the record of the original.

11. Prepare the Handoff Counsel Can Actually Use

The handoff should identify the matter reference, directing counsel, named technical owners, preservation start time and the next court or business deadline. For each source, describe its relevance, owner, control applied, verification evidence, collection method, custody identifier and known scope. Include a chronology of consequential changes and a short list of open decisions. Keep confidential legal advice in the channel counsel directs.

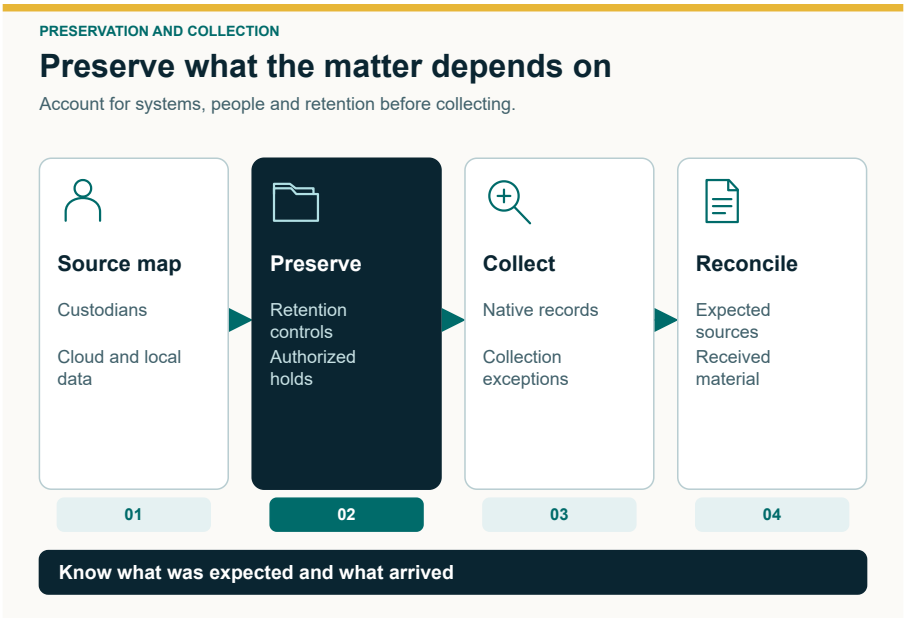
© 2026 Global Digital Forensics, Inc. All rights reserved.

The strongest technical explanation distinguishes what was requested, what was performed, what the records show and which questions remain open. That distinction gives counsel a basis to evaluate proportionality, explain exceptions and plan the next evidentiary step. The source record behind each entry is what gives the chronology its weight.

When to Escalate to a Specialist

Escalate when deletion may occur before controls are effective, a device may be wiped or reused, a mobile source contains unique evidence, a collection cannot be reconciled or an expert deadline is approaching. Ask for a practitioner whose experience fits the technology and the proposed testimony. GDF experts have testified in federal and state courts, and our work has been accepted by courts.

Bring the systems involved, where the devices are and your next court deadline to a free consultation with a senior GDF examiner. On that first call we identify the sources at risk today, the controls that will stop deletion and the collection plan that fits your forum, and we arrange secure transfer before any evidence, credential or personal record changes hands. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the eDiscovery guide library.



Preservation workflow from sources and authority through collection and documented handling.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Information Gathering Q&A Checklist

Complete this record with counsel and the people who administer the systems. Identify what is known, what remains unknown and who can confirm each answer. Ownership, account registration, management enrollment and authority to collect are separate questions. Record the source of an answer and the date it was confirmed. Answer from records and from the people who know; leave settings, sign ins and recovery processes untouched while you complete it.

Record who controls each password, recovery key or unlock code and how a secure handoff can be arranged, and we collect the secrets themselves through that handoff. Keep completed copies in the location counsel or the company approves, and share the completed record through the secure transfer method agreed on the first call.

Who is directing the matter and who can authorize technical access?

Identify directing counsel, the business decision maker, the IT security owner and any outside administrator. Record the immediate deadline, relevant period and known preservation risk. Authority to examine comes from ownership, policy and counsel's instruction, so record each one; possession of a device and administrator access are separate facts.

Answer:

Owner, source, date and unresolved questions:

Who provides the email service and who administers it?

Identify Microsoft 365, Google Workspace, an internal Exchange environment, a hosted service or a combination. Record the tenant or organization reference, relevant domains, mailbox owners, aliases, shared mailboxes and the MSP or administrator responsible. Identify available preservation and export permissions and any licensing question that needs confirmation.

Answer:

Owner, source, date and unresolved questions:

Does the company have archiving, backups or preservation holds in place?

Name each service and distinguish an archive or journal from a backup, a retention policy and a matter specific hold. Identify what each covers, the available dates, deletion or rotation rules and who can export or restore records. Record whether someone has verified coverage with a test search or export, since a subscription record shows purchase rather than coverage.

Answer:

Owner, source, date and unresolved questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Does the company supply the computers or do employees use their own?

Record company owned, personally owned, leased and shared equipment separately. Identify the assigned user, operating system, asset or serial reference and present location. Note any employee owned computer used for business and the applicable access agreement. Record company ownership and permission to examine personal material as two separate answers.

Answer:

Owner, source, date and unresolved questions:

Are mobile devices company owned, employee owned or a mixed arrangement?

Identify the phone or tablet, assigned user, model and operating system where known, and who currently holds it. Distinguish the owner of the handset from the owner of the cellular service account. Record whether work data is separated into a managed profile and whether a replacement, return or wipe is already scheduled.

Answer:

Owner, source, date and unresolved questions:

Whose Apple, Google or Samsung account is registered or signed in on each phone?

Record each relevant account as personal, company controlled or unknown, and identify who can lawfully arrange access. For Apple devices, note any organization enrollment and known Activation Lock status separately from the signed in Apple Account. For Android devices, distinguish personal and work profiles and note relevant Google and Samsung accounts separately. Answer from what the account owner and administrator already know, leaving each account signed in as it is. [14] [15]

Answer:

Owner, source, date and unresolved questions:

Does the company use MDM and what does it actually manage on these devices?

Name the management service, administrator and enrollment mode, including supervision or work profile details where applicable. Record the last known device contact and any pending retire, lock or wipe command. The management console shows what the organization controls on the device; personal applications, messages and backups usually sit outside it, so list them separately. Export the management record as it stands and issue no command just to test what the console can do.

Answer:

Owner, source, date and unresolved questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Can the company recover the BitLocker or other encryption keys for each relevant computer?

Ask whether recovery material is actually available for the identified device and drive, where it is escrowed and who has authorized retrieval permission. Possible locations include Microsoft Entra ID, Active Directory or another approved store. Note FileVault or other encryption separately. Confirm key escrow for each device by name, because enrollment and escrow are separate settings, and keep the key itself off this record. [13]

Answer:

Owner, source, date and unresolved questions:

Who controls identity, administrator access and multifactor authentication?

Identify the identity provider, relevant privileged accounts, outside administrator and person who can approve an export or collection. Note access dependencies such as an unavailable administrator or authentication device, naming who holds them. Identify shared or delegated access, because attributing that account activity to one person takes corroborating evidence.

Answer:

Owner, source, date and unresolved questions:

Which cloud storage, collaboration and messaging services contain relevant work?

Identify shared drives, Teams, SharePoint, OneDrive, Slack, Google Chat and other platforms actually used for the relevant work. Note external ownership, linked documents, personal accounts used for business and any unsupported or unavailable source. Linked files and separate chat conversations live outside the mailbox, so list them as sources of their own.

Answer:

Owner, source, date and unresolved questions:

What activity logs and endpoint records are available now?

Ask the responsible administrator which email, identity, endpoint, cloud sharing, USB, security and data protection records exist for the relevant period. Record actual date coverage, export permissions, known gaps and the next expiration or rotation point. Logging switched on today records activity from today forward, so note the date each source began recording.

Answer:

Owner, source, date and unresolved questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

What has already changed on the devices or accounts?

Record password resets, access restrictions, account deletions, mailbox conversions, software installations, cleanup activity, repairs, cloud sync changes and any device reset or wipe. Identify who acted, when and why. Include informal handling or earlier collections so the examiner can distinguish relevant historical activity from changes made during the response.

Answer:

Owner, source, date and unresolved questions:

Which custodians and locations are covered by the preservation instructions?

List the people, mailboxes, shared locations and outside providers included in counsel's instructions, then identify the technical owner for each source. Record acknowledgments, verified controls and unresolved locations separately. Include any date or keyword restriction and the person responsible for deciding whether the scope needs to change.

Answer:

Owner, source, date and unresolved questions:

Has anything already been exported, imaged or restored?

Identify the collector, collection method, source period and storage location for every existing package. Retain the original export reports, exception records and available integrity information. Record whether a package is a complete acquisition, a selected export or a restored copy so a later reviewer can understand what the material represents.

Answer:

Owner, source, date and unresolved questions:

Who will close the outstanding preservation questions and arrange secure transfer?

For each unknown answer, identify an owner and a date for confirmation. Record any source that could expire before then and the person authorized to escalate that risk. Agree on a secure transfer method with the receiving team; the public contact form is for arranging the discussion, not delivering evidence or credentials.

Answer:

Owner, source, date and unresolved questions:

Primary sources and further reading

Sources checked November 3, 2026.

1: Federal Rules of Civil Procedure, Rule 37(e) (United States Courts)
https://www.uscourts.gov/sites/default/files/document/federal-rules-of-civil-procedure.pdf

2: Florida Rules of Civil Procedure, October 1, 2026 edition, rules 1.280, 1.350 and 1.380 (The Florida Bar)
https://www-media.floridabar.org/uploads/2026/10/Civil-Procedure-Rules-10-01-26.pdf

© 2026 Global Digital Forensics, Inc. All rights reserved.

3: Microsoft guidance on creating eDiscovery holds
https://learn.microsoft.com/en-us/purview/edisc-hold-create

4: Microsoft guidance on audit log retention
https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

5: Google Vault guidance on holds
https://knowledge.workspace.google.com/vault/holds/get-started-with-holds-in-google-vault

6: Google Vault supported services and data types
https://knowledge.workspace.google.com/vault/getting-started/supported-services-and-data-types

7: NIST SP 800-101 Revision 1, Guidelines on Mobile Device Forensics (May 2014)
https://csrc.nist.gov/pubs/sp/800/101/r1/final

8: NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (August 2006)
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

9: Federal Rules of Evidence, Rules 901 and 902
https://www.uscourts.gov/sites/default/files/document/federal-rules-of-evidence.pdf

10: Florida Statutes section 90.901, Requirement of authentication or identification (2026)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0000-0099/0090/Sections/0090.901.html

11: Florida Statutes section 90.902, Self authentication (2026)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0000-0099/0090/Sections/0090.902.html

12: Florida Statutes section 90.803, Hearsay exceptions, including (6) business records (2026)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0000-0099/0090/Sections/0090.803.html

13: Microsoft BitLocker recovery overview
https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview

14: Apple guidance on Activation Lock and device management
https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web

15: Android Enterprise guidance on work profiles
https://support.google.com/work/android/answer/6191949?hl=en

Talk to a Senior GDF Examiner

Bring this guide to a free consultation. We review your answers, identify what to preserve or test first and set out the work, the timeline and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

© 2026 Global Digital Forensics, Inc. All rights reserved.