The ESI Preservation and Spoliation Defense Protocol

Coordinate legal authority, custodians, devices and cloud records. Includes practical questions for the legal and IT teams preserving evidence.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/preservation/

A preservation notice is the start of the record. This protocol connects counsel's instructions to named technical owners, identifiable sources and documented verification. GDF practitioners work alongside legal counsel, internal auditors and corporate IT security teams to preserve available evidence and explain the record.

The time bands below organize urgent work.

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. Target the pause so operations continue. The useful record identifies what was stopped, who stopped it and when the change became effective.

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 awaiting confirmation as open and assign an escalation time.

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 obtains by request. Counsel sets the legal boundaries, and the technical team maps them to actual account identifiers and storage locations.

Write down the initial assumptions behind any date or keyword restriction. Extend each search to aliases, attachments, linked documents and shared workspaces. 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.

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

3. Separate Federal and New York Preservation Analysis

For federal civil matters, Rule 37(e) addresses ESI that should have been preserved, was lost because reasonable steps were not taken and cannot be restored or replaced through additional discovery. Curative measures based on prejudice and the specified measures requiring intent to deprive have different requirements. In New York state practice, Pegasus Aviation addresses preservation obligations, culpability and relevance within the state's spoliation framework. [Federal Rule of Civil Procedure 37(e)] [Pegasus Aviation I v Varig Logistica]

4. Hours 2 to 6: Turn the Hold Into 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.

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.

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. Plan for expiring material across that interval. Preserve the hold definition, location identifiers, status records and later changes. Tenant activity logs are preserved on their own track, described next. [Microsoft guidance on creating eDiscovery holds]

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 activity history is preserved on its own terms. Keep the query, returned files and export record together. Where a gap exists, identify other lawful sources that might corroborate the event. [Microsoft guidance on audit log retention]

6. Preserve Google Workspace Without Losing 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. 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. [Google Vault guidance on holds]

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

Map Gmail, Drive, Chat and other relevant records separately. Google documents which service data Vault supports, and Chat coverage follows supported message conditions. Linked content and files owned outside the organization are preserved separately. Preserve available activity exports and ownership information, and record any inaccessible source. [Google Vault supported services and data types]

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. 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 is the foundational reference, applied to the particular handset by the examiner. [NIST SP 800-101 Revision 1]

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 goes first. Keep the reason, authorization and precise actions in the event record. [NIST SP 800-86]

8. Hours 6 to 24: 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. Name each collection by its actual method and coverage.

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.

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 identifies a particular set of bytes, and the custody record shows where the content came from and how complete the collection is.

Federal Evidence Rules 901 and 902 provide different routes for authentication. Rule 902(14) addresses qualifying certified copied data and includes procedural requirements. Counsel and the examiner should agree early on the foundation and records needed for the intended use. [Federal Rule of Evidence 901]

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

10. Hours 24 to 48: Reconcile the 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 and what was recovered, and label any later export or reconstructed document as such.

11. Prepare a Handoff Ready for the Next Decision

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 limits. Include a chronology of consequential changes and a short list of pending decisions. Keep confidential legal advice in the channel counsel directs.

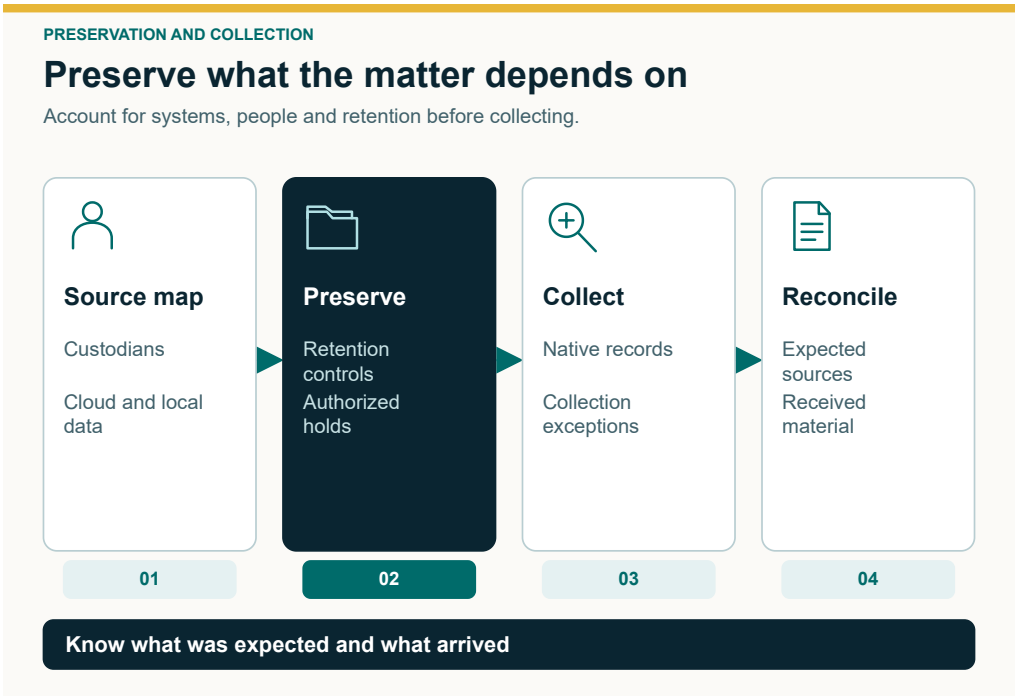
The strongest technical explanation distinguishes what was requested, what was performed and what the records show. That distinction gives counsel a basis to evaluate proportionality, explain exceptions and plan the next evidentiary step.

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 needs reconciling or an expert deadline is approaching. Ask for a practitioner whose experience fits the technology and the proposed testimony.

Call the New York office at (212) 561-5860 or the 24/7 emergency hotline at (800) 868-8189 for a free consultation. GDF practitioners work alongside legal counsel, internal auditors and corporate IT security teams to define the preservation question, identify urgent source risks and scope the engagement. Have the systems involved, device locations and deadline ready. Arrange secure transfer before sending evidence, credentials or sensitive personal records.

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



Preservation runs from authority and sources through collection to a documented handling record.

Information Gathering Q&A Checklist

Complete this record with counsel and the people who administer the systems. Identify what is known 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 the records as they stand, leaving settings, accounts and recovery processes as they are.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

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. Record who authorizes the examination scope for each device and account, which can differ from who holds the device or administers the account.

Answer:

Owner, source, date and open questions:

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

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 open 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 preservation has actually been verified, rather than treating the existence of a subscription as proof of coverage.

Answer:

Owner, source, date and open questions:

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 permission to examine personal material separately from company ownership.

Answer:

Owner, source, date and open 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 open questions:

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

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 is visible now, leaving each account signed in as it is. [Apple guidance on Activation Lock and device management; Android Enterprise guidance on work profiles]

Answer:

Owner, source, date and open 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. A device listed in a management console can also hold personal applications, messages or backups, and the examiner looks for them on the device itself. Preserve the management record as it stands.

Answer:

Owner, source, date and open questions:

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 availability for each device and record where the key is held. [Microsoft BitLocker recovery overview]

Answer:

Owner, source, date and open 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. Identify shared or delegated access so the examiner can attribute account activity to the right individual.

Answer:

Owner, source, date and open questions:

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

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. List linked files and separate conversations alongside the mailbox so each one is collected in its own right.

Answer:

Owner, source, date and open 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.

Answer:

Owner, source, date and open questions:

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 open 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 open 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 open questions:

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

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 open 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, and use the contact form to arrange the discussion.

Answer:

Owner, source, date and open questions:

Primary sources and further reading

Sources checked November 3, 2026.

1. Federal Rule of Civil Procedure 37(e), Failure to Preserve Electronically Stored Information https://www.law.cornell.edu/rules/frcp/rule_37
2. Pegasus Aviation I v Varig Logistica, New York Court of Appeals https://www.nycourts.gov/reporter/3dseries/2015/2015_09187.htm
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 https://csrc.nist.gov/pubs/sp/800/101/r1/final
8. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf
9. Federal Rule of Evidence 901, Authenticating or Identifying Evidence https://www.law.cornell.edu/rules/fre/rule_901 and Federal Rule of Evidence 902, Evidence That Is Self Authenticating https://www.law.cornell.edu/rules/fre/rule_902
10. Microsoft BitLocker recovery overview https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview
11. Apple guidance on Activation Lock and device management https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web
12. Android Enterprise guidance on work profiles https://support.google.com/work/android/answer/6191949?hl=en

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

Get a Free Consultation

The first call is a free consultation with a senior examiner. We review the matter, the evidence and the deadline, and outline the collection and analysis it needs. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

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