Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/audit-discovery-preparation/05-departed-employee/

AUDIT AND DISCOVERY PREPARATION

Departed employee data gathering package

Identify devices, cloud accounts, messages, archives and logs for a departed employee matter. Prepare questions for counsel and client IT.

Help counsel and a forensic consultant identify relevant people, devices, accounts, repositories and short lived records before collection.

Attorneys, paralegals, business/medical contacts, project coordinators and client IT

Employment, confidential information and departure disputes. The package starts from the facts, and theft, recoverability, employer ownership of personal accounts and authority to access another organization are each questions for the attorneys and the examiner to work through.

Before you gather

Begin with the alleged events and dates, not with a request for every record on every device. Ask counsel to identify the issues, the custodians, the time ranges and the preservation priorities, and include records that may support or contradict the allegation, because a forensic examiner who later testifies will be asked whether the search was one sided.

Account disablement, license removal, transfer of ownership, device wipe and replacement can all affect evidence, and they are routine offboarding steps that run on IT's schedule, so bring the legal team into that schedule early. Coordinate security containment and preservation with the legal team and authorized IT. Necessary containment goes ahead; document what changed and when, with the ticket or change record that shows it.

Federal and New York practice differ. Counsel reviews preservation, proportionality, possession, custody or control, privacy, privilege, local rules and case orders. New York CPLR 3130 sets conditions on the use of interrogatories in specified circumstances, and the commercial and uniform rules add their own requirements. The sample questions are a drafting bank for counsel to tailor before service.

Give each request to the suggested owner. Record each answer, including the items awaiting confirmation, in the editable CSV checklist. Keep the records themselves in a secure evidence location agreed with the recipient and use the checklist as the index that points to them; passwords stay with their owners, and real patient data and controlled technical information stay in the secure location.

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

Records to find

CSV files hold plain records, and your spreadsheet sets the layout. Import as UTF-8, keep IDs as text, wrap text and widen columns before use. Blank client fields are intentional.

EMP-R01 Matter facts and timeline

Ask
HR and legal

Gather
Employment/role dates, departure timeline, relevant business files/events, parties, issues and permitted time range.

Where to ask
HR, manager and counsel

Why it may be needed
Directs a proportionate, even handed information request.

If missing or uncertain
Separate known facts, allegations and questions.

Reference: LG01 26; NY05 11-c

LG01 NY05

EMP-R02 Preservation and offboarding status

Ask
Counsel and authorized IT

Gather
Hold instructions/implementation, relevant retention settings, pending deletions, license changes, account disabling, wipes and replacement/reassignment records.

Where to ask
Legal, messaging, identity and endpoint owner

Why it may be needed
Flags the time sensitive steps that protect relevant information.

If missing or uncertain
Escalate imminent deletion or open hold coverage at once so the hold reaches each source early, and record when each hold took effect; the examiner plans any recovery work from those dates.

Reference: LG01 37(e); MS03; GO01

LG01 MS03 GO01

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

EMP-R03 Custodian and identifier list

Ask
HR and IT

Gather
Names, roles, aliases, employee/user IDs, email addresses, tenant/domain IDs, device IDs and relevant shared/group accounts.

Where to ask
HR, identity and asset systems

Why it may be needed
Allows the collector to resolve actual identities and sources.

If missing or uncertain
Record open items for shared/renamed accounts and former/acquired domains.

Reference: NI04; MS01

NI04 MS01

EMP-R04 Devices and media

Ask
Asset owner and custodian

Gather
D01 to D03 and any home/personal device used for work, with ownership, location, custody, status and authority marked open where appropriate.

Where to ask
Asset records and interviews

Why it may be needed
Surfaces devices and removable copies beyond the returned laptop.

If missing or uncertain
Ask counsel first, then seek personal device data through the route counsel sets.

Reference: NI04; LG01

NI04 LG01

EMP-R05 Mail calendars and archives

Ask
Messaging and archive owner

Gather
D04/D08/D19, shared/delegated mail, aliases, mail journals, archive migrations and relevant holds.

Where to ask
Messaging and archive systems

Why it may be needed
Relevant communications can sit in shared mail, journals and archives beyond the active mailbox.

If missing or uncertain
Identify archived/inactive/deleted sources and documented capture gaps.

Reference: MS01; GO01; NI04

MS01 GO01 NI04

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

EMP-R06 Work drives and shared files

Ask
Cloud/file administrators

Gather
D05/D06/D09/D25, exact site/share paths, owners, external links, versions and relevant sharing records.

Where to ask
File servers, OneDrive, SharePoint, Drive and DMS

Why it may be needed
Finds the cloud original and collaboration history beyond synced copies.

If missing or uncertain
List external owner links and the recycle bin and hold settings.

Reference: MS03; MS05; GO01

MS03 MS05 GO01

EMP-R07 Messages and meetings

Ask
Collaboration owners and custodians

Gather
D07/D10/D11/D12, direct/group chats, external/shared channels, recordings/transcripts and linked attachments.

Where to ask
Collaboration systems and interview

Why it may be needed
Covers communications held in chat, meeting and collaboration tools.

If missing or uncertain
Ask about actual apps, subscriptions, history and retention settings.

Reference: MS02; GO01; SL01; SL02

MS02 GO01 SL01 SL02

EMP-R08 Access transfer and security traces

Ask
Security and network teams

Gather
D13 to D18 and relevant D34; log coverage, earliest/latest dates, field legend, device/IP mappings and permissions.

Where to ask
Identity, SIEM/EDR/DLP, VPN, proxy and cloud admins

Why it may be needed
Lets the forensic specialist evaluate leads and gaps.

If missing or uncertain
Record open actor and content questions and the coverage periods to confirm.

Reference: NI04; MS04; GO02; AW01

NI04 MS04 GO02 AW01

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

EMP-R09 Business and project sources

Ask
Business and application owners

Gather
D22 to D28, customer/project lists, code/design repositories, tickets and relevant documents/workflows.

Where to ask
CRM, engineering, projects and practice systems

Why it may be needed
Can show legitimate work, chronology and alternate explanations as well as disputed activity.

If missing or uncertain
Identify the actual modules and what each export includes, and confirm report coverage with the owner.

Reference: NI04; CL01

NI04 CL01

EMP-R10 Backups and historical environments

Ask
Backup/migration owner

Gather
D20/D21, catalogs, retention/overwrite dates, restore dependencies, keys held by owner and earlier export copies.

Where to ask
Backup provider and migration project

Why it may be needed
Checks where potentially relevant earlier copies may exist.

If missing or uncertain
Request a cost/scope estimate for specialist planned isolated restoration.

Reference: NI04; LG01 26(b)(2)

NI04 LG01

EMP-R11 Personal external and third party sources

Ask
Counsel and custodian

Gather
Known work related external accounts, recipient organizations and relevant third party systems, with the basis for knowledge and control.

Where to ask
Interview and business records

Why it may be needed
Enables counsel to choose consent, party request or lawful third party process.

If missing or uncertain
Access runs through consent, a party request or lawful process, and counsel tailors any request that reaches a private account.

Reference: LG01 34,45; NY05

LG01 NY05

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

EMP-R12 Collection and response index

Ask
Coordinator and collector

Gather
What was actually preserved/collected, who performed it, exact scope/filters, date/time zone, hashes where used, errors and sources queued for collection.

Where to ask
Collection report and file index

Why it may be needed
Allows the receiving expert to assess coverage and request remaining work.

If missing or uncertain
Confirm a completed download or a zero search result against the source scope, filters and error reports before reading it as final.

Reference: NI04; MS06

NI04 MS06

Questions for client IT and owners

A useful answer names the actual system, period, supporting record and its coverage. Where the answer sits with someone else, name the person or provider who can give it.

1. Which accounts and devices did the person use for the relevant work, including shared and renamed accounts?

Suggested responder
Client IT or system owner

Useful supporting record
Identifier crosswalk with dates and ownership.

2. Which offboarding actions have occurred and what remains scheduled?

Suggested responder
Client IT or system owner

Useful supporting record
Dated action/change records and preservation confirmation.

3. Where do linked cloud files live, and who owns the external/shared copies?

Suggested responder
Client IT or system owner

Useful supporting record
Exact tenant/site/share/workspace IDs and owner list.

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

4. Which non email tools did the person and coworkers actually use?

Suggested responder
Client IT or system owner

Useful supporting record
Custodian interview notes with apps/accounts and purpose.

5. What event types were logged at the time and how far back can each source be retrieved?

Suggested responder
Client IT or system owner

Useful supporting record
Coverage/retention table, earliest/latest examples and field legend.

6. Could a device, account, IP or badge have been shared or used by an administrator?

Suggested responder
Client IT or system owner

Useful supporting record
Assignment, delegation and remote support records.

7. What migrations, deletions, license changes or policy changes may have affected records?

Suggested responder
Client IT or system owner

Useful supporting record
Change log with known gaps and decision owners.

8. What does a permitted export include, and which errors or unindexed items need separate work?

Suggested responder
Client IT or system owner

Useful supporting record
Export process report and documented limitations.

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

Sample discovery questions to tailor

Sample questions are drafting prompts for counsel, who shapes them into requests that fit the matter. Define the event, source, period and parties. Check relevance, proportionality, privilege, privacy, possession/custody/control, current local rules and case orders. Federal Rule 33 ordinarily allows up to 25 interrogatories, including discrete subparts, unless a stipulation or court order sets another number. New York uniform and Commercial Division rules and CPLR 3130 set their own conditions on interrogatories; especially check the interrogatory/deposition choice in negligence personal injury, property or wrongful death actions. Split or narrow prompts as the rules permit, and use a document request, interview or deposition topic where that is the appropriate device. Counsel decides what is served; these packages prepare the facts behind it.

Supporting procedural sources: LG01, NY05, NY06, NY07 and NY08. These questions are separate from the internal IT interview.

LG01 NY05 NY06 NY07 NY08

1. Identify the custodians of records concerning [defined disputed event] during [period] and each custodian role.
2. Identify the devices assigned to [person] during [period], including their unique identifiers and current custodian.
3. Identify the business accounts used by [person] for [defined project], including aliases and shared accounts.
4. Identify the repositories holding [defined project records] during [period], their responsible administrators and relevant external owners.
5. Describe the retention/deletion settings applicable to [defined source] during [period], including material changes and known data gaps.
6. Identify the log sources that record [defined activity] for [period] and the person able to explain their coverage and fields.
7. Identify the preservation and collection actions actually taken for [defined source], including dates and persons performing them, without requesting privileged advice.
8. Identify responsive sources not searched or produced and the factual basis for claimed inaccessibility or limitation, subject to the applicable rules and orders.

Worked gathering example

Example only: A returned laptop contains an online only shortcut to a project folder. The coordinator records the shortcut and asks IT for the tenant/site owner, relevant versions and sharing records. The specialist chooses a collection method for the cloud folder, and the coordinator logs the shortcut as a pointer to that folder.

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

Facts to confirm and specialist decisions

These are explicit handoff questions, and each one closes with the specialist's written answer, drawing on the records marked Received. Add client specific questions and a responsible person.

EMP-Q01 What sources and time ranges are proportionate and within lawful possession, custody or control?

Ask
Counsel

Gather
Claims, issues, chronology, ownership and proposed source inventory

Resolution needed
Counsel approved scope and authority before collection; preserve separately where required.

EMP-Q02 Can the relevant activity be attributed, and what alternatives remain?

Ask
Forensic specialist

Gather
Original records, timestamps, IDs, mappings and limitations

Resolution needed
Expert analysis after collection, combining the device record with access logs, interviews and other corroboration.

Preparing the handoff

The handoff is ready when the issue, date and custodian scope and the authority to collect are agreed with counsel; when imminent deletion and offboarding actions are recorded and escalated; when cloud repositories, archives, backups and business systems are addressed alongside the endpoints; and when the source inventory distinguishes possible, confirmed, preserved and collected locations so the examiner can plan the next steps.

Sources for this package

Official laws/rules establish duties within their scope. Guidance explains programs; NIST supplies methods; vendor documentation describes possible product behavior. The package works alongside the actual contracts, facts, configuration and case orders.

- New York Commercial Division rules (NY05)
- New York Uniform Civil Rules Part 202 (NY06)
- New York CPLR 3130 (NY07)
- New York CPLR 3133 (NY08)
- NIST SP 800-86 (NI04)
- Federal Rules of Civil Procedure December 2025 (LG01)
- Federal Rules of Evidence (LG02)

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

- Microsoft eDiscovery data sources (MS01)
- Microsoft Teams content in eDiscovery (MS02)
- OneDrive retention and deletion (MS03)
- Microsoft audit retention (MS04)
- SharePoint and OneDrive retention (MS05)
- Microsoft eDiscovery process reports (MS06)
- Google Vault overview (GO01)
- Google audit lag and retention (GO02)
- Slack Discovery APIs (SL01)
- Slack Connect data management (SL02)
- AWS CloudTrail event history (AW01)
- Clio matter export scope (CL01)

Bring the completed pack to a free scoping call and a senior examiner sets the scope from it. Call (800) 868-8189.

Source review date: October 18 2026.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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