What to Do Before and After a Key Employee Leaves

Coordinate HR, IT and counsel around devices, cloud accounts and business records before routine offboarding changes the evidence.

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

An employee's departure can create an immediate conflict between business continuity, access control and evidence preservation. A routine reset or account cleanup may remove the material needed to explain disputed file movement. At the same time, leaving unnecessary access active can expose the organization to further harm. This guide organizes those decisions around an authorized scope, preserved sources and findings that distinguish observed activity from suspicion.

GDF practitioners work alongside legal counsel, internal auditors and corporate IT security teams. The technical record can support those decisions. A USB connection, downloaded file or matching code fragment is a starting point; intent and use need corroborating records.

1. Open a Controlled Triage Record Before Offboarding Proceeds

Name the directing lawyer, HR contact, IT security lead and person responsible for equipment custody. Record the departure date, last authorized access, reported concern and exact facts already known. Separate a witnessed event from an alert, an employee report or an inference. Identify any competing requirement to disable access immediately and preserve the reason for the decision. A coordinated record reduces the risk that one team preserves a laptop while another deletes the associated account or mobile backup.

Ask the business owner to identify the specific information at issue and its business significance. Record relevant projects, repositories, client materials, design files, pricing records or other claimed confidential material, with the access restrictions that actually existed. Give counsel the underlying business facts and the protection measures in place for each item.

2. Stop Routine Reuse Without Leaving the Organization Exposed

Place relevant company equipment into controlled custody before a reset, operating system installation, repair or reassignment. Record the asset identifier, assigned user, visible condition, power state and the person receiving it. Preserve available account and security records while an authorized lead plans access restrictions. Where immediate containment is necessary, perform it and document the reason, time and effect.

Give the examiner the original source under a documented transfer, so its metadata and context reach the examination intact, and keep any earlier informal handling in the chronology. A complete account of that handling strengthens the record.

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

3. Preserve Laptops and Drives Under a Device Specific Plan

Identify internal storage, removable media, encryption, attached devices and any active session that may affect acquisition. An examiner should choose an appropriate method for the operating system, storage design, encryption state and authorized scope. A full image may be appropriate in one matter; a controlled logical collection may be justified in another. Record the choice and name each copy by the method that made it. Live collection can change the source, and shutdown can remove volatile information, so document the tradeoff. [NIST SP 800-86]

Before equipment leaves IT, retain the asset record, relevant endpoint alerts, device management events and records of administrator actions already taken. Preserve lawful access to necessary recovery material through the organization's approved secure process. Arranging that access early keeps the examination of an encrypted drive on schedule.

4. Read USB Artifacts as Connection Records, Then Corroborate

Where available, collect relevant Windows device recognition records, registry artifacts, installation logs and endpoint telemetry. Record device identifiers and the user and system context in which they appear. Microsoft's description of Event 6416 concerns recognition of an external device, and the examiner correlates it with independent file activity, source documents, removable media content or other supported observations to show what was transferred. [Microsoft description of Windows Event 6416]

The examination should ask whether a device was connected, whether relevant files were accessed or staged, and whether there is evidence of a destination copy. Those are separate propositions. Shared workstations, automated processes and ordinary job duties may explain some activity. A report should identify those alternatives and explain which sources support the conclusion and how strongly.

5. Preserve Cloud Sync and Sharing Records Beyond the Endpoint

Identify the organization's file platforms, sanctioned synchronization tools and any known external sharing paths. Preserve available activity records, file identifiers, permissions, export parameters and relevant account history. Microsoft documents distinct actions for file access, downloads, synchronization and sharing. An action recorded against an account must be interpreted in its service and client context; automated synchronization and authorized collaboration can produce activity that differs from deliberate disclosure. Preserve the underlying records behind any alert summary. [Microsoft definitions of audit log activities]

Compare cloud observations with the endpoint and business record. A downloaded file may have been part of an established sync set, while a newly created external sharing link may require a different inquiry into access and recipient activity. Identify what the records establish about the action, destination and timing. Report recipient access from the records that capture it, and distinguish permission to access information from evidence that it was read, copied or used.

6. Examine Personal Email Questions Within Lawful Access Boundaries

Preserve corporate mailbox records, relevant message content, attachments, forwarding settings and available gateway or security events under counsel's direction. Identify the precise record supporting a claimed transmission, including the sender, recipient, attachment or linked item, timing and source. A

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

message in Sent Items, a delivery record and a record of recipient access answer different questions. Where only a link was sent, establish what the link could reach and what access evidence exists before describing the underlying documents as transferred.

A personal email address in browser history or an autocomplete entry is a lead the examiner tests against transmission records. Personal accounts and private material are examined under a lawful basis and an agreed protocol, and personal, privileged and irrelevant content is separated during examination as counsel directs. Where external records come through consent or court process, the work plan schedules that step.

7. Protect Mobile Evidence Before a Wipe or Ownership Change

Identify whether the phone is company owned, personally owned or subject to a managed work profile, then record the authorized scope. Coordinate any pause in a scheduled wipe or device retirement with counsel and the security lead. Photograph or otherwise document the observable state as it is. Ask an examiner to assess isolation, power and acquisition options for the actual device. NIST's mobile guidance explains why these preservation choices matter, and the examiner assesses current handset and application capabilities for the device in hand. [NIST SP 800-101 Revision 1]

Map the messaging applications, relevant cloud accounts and available backups alongside the handset. Each account export covers its own application records, messages and linked files, so preserve collection errors with the export. Call an acquisition complete once its sources have been reconciled, and let the examiner assess the device before estimating what deleted content can be recovered.

8. Preserve Source Code With Its Provenance Records

Where code or technical designs are disputed, preserve the relevant repositories, commit history, branches, tags, releases, access permissions and available audit exports. Keep build configuration, dependency records and the versions actually supplied to customers or deployed internally when they bear on the issue. Repository administrators should preserve available audit material promptly and document the product tier, retention and export method. GitHub describes separate access and export options for organization audit records; collect the full audit export alongside the history shown in the interface. [GitHub guidance on reviewing organization audit records]

A matching block of code is the start of the comparison. Identify common libraries, generated material, public code, licensing and prior authorized access before forming a technical opinion, and read commit author fields and account activity in context to attribute an action to a person. Preserve the material needed to evaluate alternative explanations and describe the basis for any attribution.

9. Build a Timeline That Preserves the Original Time Evidence

Retain original timestamps, time zone information, source precision and available clock context before converting events into a common display. Identify whether each timestamp represents creation, modification, synchronization, an application event or an export process. A copied file can acquire a new filesystem timestamp without changing its contents, and a cloud record may describe a service action rather than a user's direct action. Make the conversion rules visible so another examiner can reproduce the chronology.

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

Correlate the departure, relevant access changes, device activity, file handling and communications with independent business records. Describe each event at the level the source supports. Where two records carry no reliable order, show them side by side. A chronology becomes useful when it distinguishes confirmed events, supported interpretations and questions that remain open.

10. Preserve Custody and Exceptions Before Preparing a Court Package

Assign evidence identifiers to acquired devices, exports and derived examination files. Record collection authority, collector, method, acquisition time, access history, transfer details and appropriate integrity checks. Keep native records, relevant metadata, reports from collection tools and known errors with the working file. Distinguish preserved originals from analyst notes, screenshots, reconstructed exhibits and later exports. That separation lets every later reader, including another examiner, understand what an exhibit actually represents.

For a potential temporary restraining order or other urgent application, ask counsel what propositions must be supported and when. Provide a concise factual chronology, a source index and the technical basis for each proposed statement, including its scope and alternative explanations.

11. Deliver Decisions and Next Steps Grounded in the Record

The initial handoff should explain what was preserved, which sources were examined and what the current observations support. Assign each next task an owner and a reason, such as collecting a device, obtaining provider records, validating an export or confirming a permission. Keep the original concern separate from the technical conclusion.

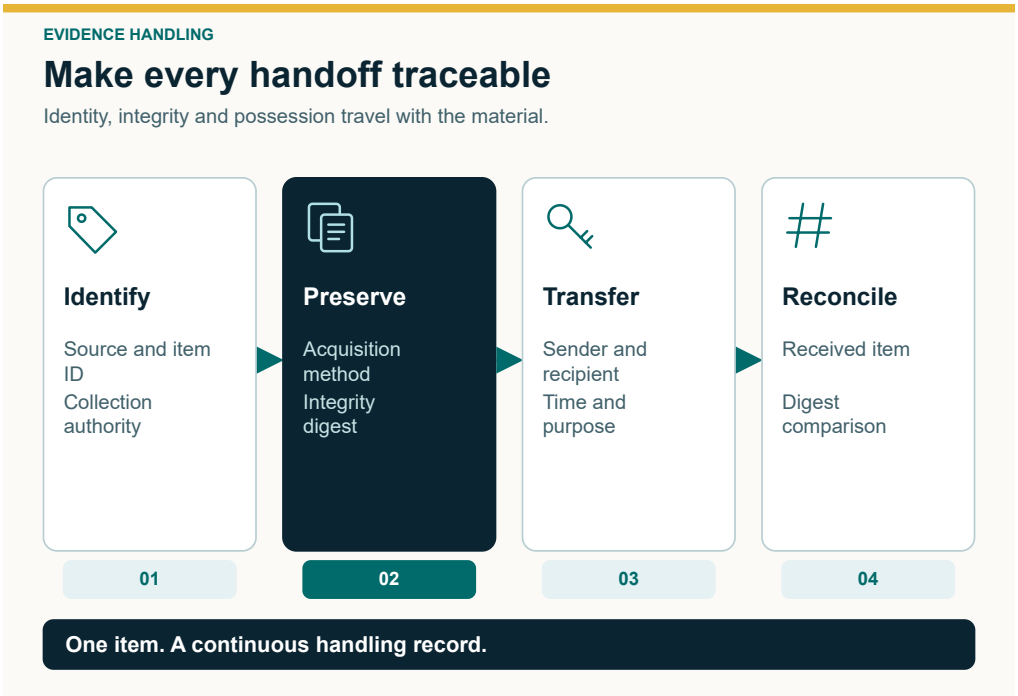
A triage engagement sets priorities quickly. State whether the work is a preliminary assessment, a defined examination or an opinion prepared for testimony. If later records change the chronology or interpretation, retain the earlier version and explain the revision. That disciplined record is what the matter relies on.

When to Escalate to a Specialist

Escalate before a device is reset, a phone is wiped, a source is about to expire or a departing account is deleted. Obtain specialist support where the matter involves competing ownership or privacy claims, encrypted devices, source code comparisons, contested attribution or an urgent expert deadline. Select a practitioner with relevant examination and testimony experience.

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 identify urgent preservation needs, define the questions the evidence must answer and scope the engagement. Have the departure timeline, systems involved, equipment location and immediate deadline ready.

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



Each device and account is collected and recorded before offboarding changes it.

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:

What is the departure timeline and when will normal offboarding change the record?

Record notice, last working day, last authorized access, equipment return and any scheduled reset, account deletion or reassignment. Identify who controls each scheduled action. Where access has already been restricted, retain the time and reason so the response itself can be separated from the activity under examination.

Answer:

Owner, source, date and open questions:

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

What specific information, code or business records are at issue?

Identify the actual projects, file locations, repositories, versions and access restrictions relevant to the concern. Record authorized sharing practices and known alternative sources such as common libraries or public code. Record the reported concern on its own line, apart from the technical findings.

Answer:

Owner, source, date and open questions:

Which devices and transfer paths should the examiner consider?

Record known removable media, corporate or personal cloud sync, external sharing links, email destinations, source code platforms and remote access tools that may be relevant. State the observation supporting each concern and any ordinary business explanation already known. List any missing devices and destination records so the examiner can locate them.

Answer:

Owner, source, date and open questions:

Who has the equipment now and how will it be handed over?

Identify the current holder, storage location and any earlier handling of each relevant device or removable medium. Note whether it is on, off, locked or already reset, as far as that state is visible without handling it. Arrange a documented, secure transfer and a device specific preservation discussion before further handling.

Answer:

Owner, source, date and open questions:

Primary sources and further reading

Sources checked November 3, 2026.

1. NIST SP 800-101 Revision 1, Guidelines on Mobile Device Forensics https://csrc.nist.gov/pubs/sp/800/101/r1/final
2. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf
3. Microsoft description of Windows Event 6416 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-6416
4. Microsoft definitions of audit log activities https://learn.microsoft.com/en-us/purview/audit-log-activities
5. GitHub guidance on reviewing organization audit records https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization
6. Microsoft BitLocker recovery overview https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview
7. Apple guidance on Activation Lock and device management https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web

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

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

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.