PRACTITIONER RESOURCE

# 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 · Updated November 3, 2026 · miami-computer-forensics.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 examiners work alongside legal counsel, internal auditors and corporate IT security teams, and the record we build is the one counsel takes into a demand letter, an injunction hearing or a deposition. Counsel applies trade secret, employment and privacy law to the facts; our work establishes those facts from the records. A USB connection, a download or a matching code fragment is where the analysis starts, and we corroborate it with file activity, cloud records and the timeline before we call anything a transfer.

## 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. Name the specific files and repositories that matter rather than an entire home directory. Counsel needs the business facts and the protection measures that surrounded the information, because those are what a trade secret claim is built on.

## 2. Pause Routine Reuse While the Organization Stays Protected

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. Evidence preservation should inform containment rather than become an excuse to leave harmful access available.

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

Keep the employee's folders, any recovered USB device and the original messages as they are, so the examiner receives the metadata and context intact. Give the examiner the original source under a documented transfer, and record any earlier informal handling in the chronology, where it helps the examiner explain the record accurately.

## 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 method chosen and what it covers, and reserve the term forensic image for a full acquisition. Live collection can change the source, and shutdown can remove volatile information, so document the tradeoff. [2]

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. Note who holds the passwords and recovery keys, and we collect them through the secure handoff agreed on the first call. Keeping that recovery material available keeps the engagement moving once the drive is preserved.

## 4. Treat USB Artifacts as a Connection Record That Needs Corroboration

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 documents Event 6416 as the record that the system recognized an external device; it identifies the device, and evidence of file activity comes from other sources. Correlate any such record with independent file activity, source documents, removable media content or other supported observations before asserting a transfer. The event may be absent if the relevant auditing or retained history is unavailable. [3]

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 how each source bears on the conclusion. A recovered removable drive is examined for what it held, and when the drive is missing, the computer's connection records are where we look for its use.

## 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 rather than relying on a screenshot of an alert summary. [4]

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

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. Recipient access records, where the service keeps them, are where we look for who opened the shared material. Permissions show who could reach a file; activity records show who actually opened, copied or shared it.

## 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 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; a sent message carrying the attachment is direct evidence of transmission, and we look for both. Personal accounts and private material are examined under the lawful basis and the agreed protocol counsel sets. Separate personal, privileged and irrelevant content during examination as counsel directs. Where external records come through consent or court process, the work plan records that route and its timing.

## 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, leaving the settings as they are. 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 matches them to the current handset and applications. [1]

Map the messaging applications, relevant cloud accounts and available backups alongside the handset. An export from one account may not contain every application record, deleted message or linked file. Preserve collection errors and unavailable sources. Describe each acquisition by what it actually captured, and assess the device and its sources before predicting what deleted content can be recovered.

## 8. Preserve Source Code With the Records That Explain Its Provenance

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 documents separate access and export options for organization audit records, so export the record rather than relying on what the web interface happens to display. [5]

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

Treat a matching block of code as the start of the comparison. Identify common libraries, generated material, public code, licensing and prior authorized access before forming a technical opinion. Tying a commit or an account action to a person combines those fields with access logs, device records, interviews and other corroboration. 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.

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 support more than one order or attribution, the chronology shows each possibility. A chronology becomes useful to counsel 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 allows counsel and another examiner to 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 the scope of each statement and alternative explanations. State every fact at the level the evidence supports, so each sentence in a declaration is tied to the record that supports it.

## 11. Deliver Decisions and Next Steps on a Documented Record

The initial handoff should explain what was preserved, what remains at risk, which sources were actually examined and what the current observations support. List relevant data that sits outside the current scope, with the person who can authorize it. Assign each remaining task an owner and a reason, such as collecting a device, obtaining provider records, validating an export or resolving a permission question. Keep the original concern separate from the technical conclusion.

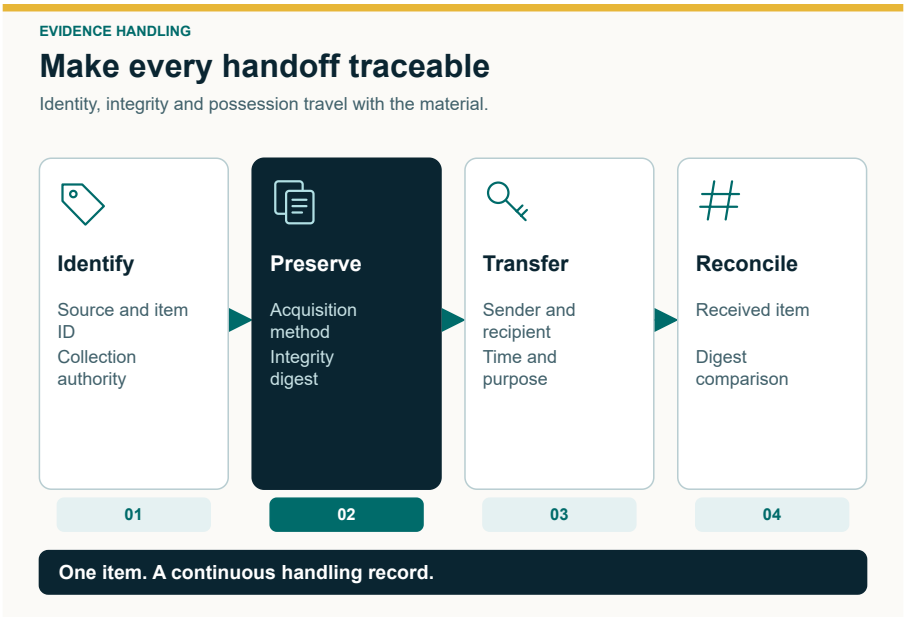
A short triage engagement sets priorities and points the full examination at the disputed issues that matter most. State whether the work is a preliminary assessment, a defined examination or an opinion prepared for testimony. If later records change the chronology or interpretation, retain the earlier version and explain the revision. That disciplined record carries more weight with a court than an early accusation.

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

## 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. Prepare the assignment history, methods, supporting exhibits and foundation questions for the proceeding.

Bring the departure timeline, the systems involved, where the equipment is now and your next deadline to a free consultation with a senior GDF examiner. On that first call we identify what must be preserved today, which sources answer your questions and how the examination will be scoped, and we arrange a secure way to receive evidence so nothing sensitive travels by ordinary email. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the forensics guide library.




How a source moves from collection through transfer to analysis, with a custody record at every step.

© 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. [7] [8]

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. [6]

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:

---

### 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 unresolved questions:

---

### 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. Keep the reported concern separate from a technical finding or counsel's determination that particular material meets a legal definition.

Answer:

---

Owner, source, date and unresolved 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 or destination records, so the examiner can look for other sources of the same activity.

Answer:

---

Owner, source, date and unresolved questions:

---

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

### 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 from what the holder already knows, leaving the device as it is. Arrange a documented, secure transfer and a device specific preservation discussion before further handling.

Answer:

---

Owner, source, date and unresolved questions:

---

## Primary sources and further reading

Sources checked November 3, 2026.


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

**2**: NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (August 2006)
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

**8**: 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.