Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/insider-threat-checklist/

DEPARTING EMPLOYEE CHECKLIST

Insider Threat Checklist: Hold the Accounts, Seal the Laptop

When customer lists, pricing models or code are at issue, the weeks before a resignation are where the examiner looks first, and the returned laptop is often the key source. This checklist is the protocol for holding the devices and accounts and exporting the shortest lived logs first, so the record is preserved before anyone reviews it.

Why the Resignation Week Matters Most

Departing employee examinations show the same pattern across industries. Exfiltration peaks in the weeks before the resignation letter, while the insider still holds legitimate credentials and can stage files onto a personal USB drive, a personal cloud account or a personal phone without tripping an alarm. By the time the resignation arrives the copying is usually finished, and the examination turns to the places that record it: USB device history and shellbags on the laptop, FileDownloaded and sync events in the tenant audit log, and browser history for personal webmail and cloud uploads. That record is what counsel works from for a demand letter, a negotiated return or a temporary restraining order, and the company's own offboarding is where preserving it begins. Our 48 hour preservation protocol for general counsel describes the hour by hour sequence.

GDF documents the access controls, account activity, endpoint artifacts and transfers relevant to a trade secret matter. Our examiners correlate those records to explain acquisition, disclosure and use, giving the legal team a source documented chronology for the case.

The Sequence From the Resignation Call to the Verified Image

If the computer involved is already powered off, leave it off and place it in documented custody. If it is still running, record what it shows and contact GDF promptly, and our examiners will plan the preservation, network isolation and live acquisition with your authorized technical team.

GDF works with the authorized Microsoft 365 administrator to preserve the relevant mailboxes, OneDrive records and activity logs.

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

Who Calls Counsel, Holds the Accounts and Images the Laptop

HR or the manager makes the first call and receives the returned hardware, bagging and labeling it while it stays powered off. Counsel directs the matter from that call, issues the hold, decides when and how the employee or the new employer is contacted and engages the examiner so the analysis runs under its direction. The Global Administrator or Super Administrator holds the accounts and runs the exports from a written list. The MDM administrator suspends remote wipe and retire commands. The security team exports its own log sources. The examiner images and analyzes. Writing those roles into the offboarding procedure, so that HR's notice of a sensitive departure triggers quarantine and hold automatically, is the change that makes preservation part of the routine rather than a matter of memory.

The people with the most reason to look are the ones who leave the looking to the examiner. A manager who wants to see what was taken reviews the preserved mailbox and OneDrive export, which keeps every file's access timestamps as the employee left them and gives the other side a clean record to read. Any conversation with the employee happens when and how the company's lawyers decide, so the timing of the holds stays in the company's hands. Each of those steps is taken from a preserved copy, under legal direction, where it strengthens the record.

Habits That Build the Case From the Start

We establish the account and license state, confirm the preservation controls and scope the collection around the matter.

The analytical discipline is keeping three findings distinct. Access means the custodian opened a file, which the audit log and LNK artifacts show well. Copying means the file was written somewhere else, which the examiner corroborates from the destination's file system, the USB artifacts, the sync client logs or the browser upload records. Exfiltration means the copy left the company's control, which depends on the destination being a personal account, device or recipient. A declaration that states each finding at the level the record supports, opened, copied or sent, gives the company's attorneys a document to stand behind at the hearing and lends weight to everything else the judge reads. The preservation checklist holds all three layers of evidence for examination, and the report is written so each is stated separately.

How GDF Supports Legal, Audit and Security Teams

Global Digital Forensics has supported trade secret and employment attorneys, internal auditors and corporate security teams since 1992, from sixteen US offices and a 24/7 hotline. On the first call we walk the administrator through the holds and exports in order while the laptop is still in its bag, then image it, verify the image and triage the artifacts that matter at a temporary restraining order hearing: USB history, shellbags, jump lists, browser uploads and the execution traces of wiping tools in Prefetch, Amcache, UserAssist, the USN journal and SRUM. The result is a short preliminary findings memorandum for counsel. Our trade secret and employee forensics page describes the device and cloud sources we correlate and why both are needed.

Where the matter involves phones, Veronica Perez leads the mobile collection, and our supported remote collection runs through a link and a computer connection, usually from a few minutes to overnight depending on setup, so an executive can keep working while the record is preserved. Where the matter involves source code, SourceScan comparisons show what was taken and where it reappeared. Our examiners have testified

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

in federal and state courts, our clients include AmLaw 100 firms and Fortune 1000 companies, and the examiner who runs the analysis is the one who signs the declaration and explains it. The initial consultation is free. If a resignation has landed and the laptop is still powered on in someone's office, call (800) 868-8189 and the examiner will plan its handling with you.

The Checklist at a Glance

The accounts, devices and logs to hold when a sensitive employee departs, who holds each one, where it lives and how quickly it is gone.

Item	Who acts	Where it lives	How fast it expires
Call to counsel	HR or the manager, time noted	Phone, with the time recorded	Every later step is cleaner under legal direction
Account preserved in place	Global Administrator	Entra sign in block and Purview litigation hold	Thirty days after deletion under the Microsoft default
OneDrive and SharePoint download events	Compliance administrator	Purview audit search, FileDownloaded and sync events	180 days standard, longer by license
Microsoft Entra sign in logs	Global Administrator	Entra portal or SIEM export	Seven or thirty days by license
Google Drive and login audit logs	Super Administrator	Admin console reports or export	About six months
Returned laptop	HR, bagged and powered off	Locked evidence cabinet with a custody form	Held as is until IT reimages it
Company phone and MDM wipe	MDM administrator, suspend wipe and retire	MDM console such as Intune or Jamf	Held once the wipe is suspended
Badge, VPN and endpoint logs	Security team	Physical access system, VPN concentrator, EDR console	Rolls over by log size or vendor retention

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

FREQUENTLY ASKED

Notice Periods, Wiped Laptops and Audit Logs

The employee is still working through a notice period. Should we take the laptop now?

That is counsel's decision, and it depends on what the matter needs. Taking the device now preserves the endpoint record at once, and it also signals the company's interest to the employee. Letting the notice run while the cloud side is held and the logs are exported keeps the timing discreet and preserves most of the record, while the device stays in the employee's hands for those weeks. We advise the legal team on which approach keeps the most evidence in the particular setup.

Can the manager check the employee's OneDrive to see what was taken?

Hold the account and let the examiner answer that question. Block sign in, revoke sessions and place the account on hold, which keeps every file's access timestamps as the employee left them. Once the audit log and the drive contents are exported and verified, the examiner walks your attorneys through the download and sharing records, from a copy held untouched since preservation.

What if the employee already wiped the laptop before returning it?

Tell the examiner first. Wiping tools, mass deletions and factory resets often leave execution and timing traces in Prefetch, Amcache, UserAssist, the USN journal and SRUM, and courts have found the record of concealment persuasive at the restraining order stage. The cloud audit log sits outside the laptop, and the examiner reads it for what was downloaded and when.

Do we need a forensic examination, or is the audit log enough?

The audit log records access and downloads by account and time, which is valuable, and the endpoint records are where the examiner follows the files afterward. Copying and exfiltration are examined in the endpoint, the USB artifacts, the sync client logs and the browser upload records, which live on the laptop and the phone. The two sources are correlated so each finding, access, copying and exfiltration, has its own support in the report.

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.