# Lost corporate laptop response checklist


Prey Inc.

# Lost corporate laptop response checklist


When a corporate laptop goes missing in a regulated environment, the incident is never "just" about the device. It immediately raises questions about exposure, compliance, and whether sensitive information may have been accessible — even briefly. A misplaced laptop can escalate from a minor inconvenience to a **potential breach notification**, depending on its controls, its user, and the data it touched.

The risk isn't only what's stored on the device, but what it **can** access: cached credentials that haven't expired yet, offline files that aren't encrypted, browsers still logged into production apps, VPN tunnels that auto-reconnect, and identity tokens quietly refreshing in the background.

And because most losses look like "just misplaced" incidents at first, teams often delay containment while they wait for clarity. A single endpoint can become an entry point for lateral movement, a compliance headache, or a forced audit if regulated data is involved.

That's why preparation matters. Before anything goes missing, the fastest way to protect your organization is knowing exactly **what you need to check** and **where to find it**.

This checklist highlights the critical information teams need during a lost-laptop incident, enabling faster response and more informed decision-making under time pressure.

## Here's what you should have ready, and why each one helps:

- **Device identifiers:** Having a clear list of the asset tag, serial or IMEI, assigned user, OS version, last check-in, and last-seen location gives you a precise starting point.

  These identifiers make sure you're working on the right device, especially if your fleet includes similar models or users with multiple endpoints.

- **Security posture:** Knowing whether the device has full disk encryption (BitLocker/FileVault), a proper screen-lock policy, an active EDR agent, or any risky local admin accounts helps you gauge potential exposure.

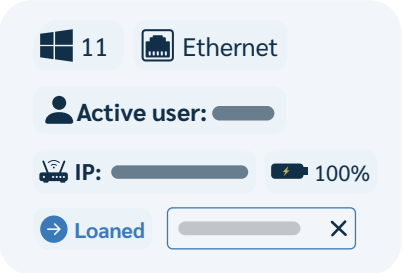
  Strong controls buy you time; weak or missing controls signal you may need to act more aggressively.

- **Data profile (estimated):** A quick sense of what the device can access, email, VPN, shared folders, business apps, cached files, or regulated data, helps you measure the impact if it's truly lost. Not every endpoint holds sensitive information, but the ones that do deserve a tighter response.

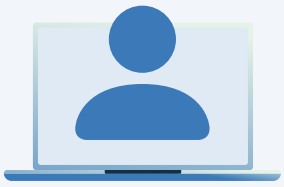
- **Ownership model:** Whether the laptop is corporate-owned or a BYOD device with a work profile determines the level of action you're allowed to take.

  Corporate devices can usually be locked or wiped without hesitation, while BYOD requires selective wipes and more coordination with the user.

- **Where to find this info:**




- **Prey Inventory:** Your quickest snapshot of the device. The card shows the assigned owner, the groups and tags it belongs to, plus the last-seen time and location. This is often the first place you go to confirm whether the device is active, offline, or behaving oddly.



- **IdP/SSO:** Your identity provider keeps a record of recent device sessions, active logins, and session tokens. Checking here helps you see whether the laptop was used after it went missing, or if the account linked to it is still active somewhere it shouldn't be.

- **EDR console:** Endpoint detection tools provide a technical heartbeat. You can view the last time the agent checked in, any alerts triggered, and the last IP address it reported. This is especially useful for spotting tampering or confirming whether the device was online more recently than Prey or the IdP suggests.

- **Tip:** Keep a short **Device Intake Card** in your IR runbook so your helpdesk team can gather all this in under two minutes. It keeps the process consistent and saves you from scrambling later.

# The first hour (T+0 → T+1h): containment


The first hour is all about shrinking the exposure window while giving yourself the best possible shot at recovering the laptop. Even if the device is only misplaced, quick containment cuts down the chance of unauthorized access and helps you stay ahead of any surprises.

## Here's what to handle right away and why each one matters:


### Account & token revocation

Start by cutting off access at the account level. Disable active SSO sessions and force an MFA re-enrollment so any existing tokens instantly become useless. Invalidate OAuth refresh tokens from apps like Google, Microsoft, or Slack to stop them from quietly reconnecting in the background.

Revoke any device certificates and terminate active VPN sessions to prevent network-level access. And don't forget to log each timestamp in the ticket, it helps build a clean incident timeline later.


## MDM actions (Prey)

Your device management tool is your anchor at this stage. Enable Lost Mode with a callback message to increase the chances of someone returning the laptop, and play an alert sound if the situation allows it. Apply a Remote Lock on corporate devices to freeze access, or enforce a passcode if one wasn't set. If the data risk is high, like missing encryption or sensitive information, go for a Selective Wipe on BYOD or a Full Wipe on corporate hardware, ideally with Legal's sign-off.

## Access boundary changes

Next, tighten the walls around the device. Remove it from any conditional access allow-lists so it can't authenticate into trusted environments. If your file services or collaboration tools support offline access, disable it to keep cached folders or shared drives from being exposed.


## Evidence capture (don't skip)

Finally, capture proof of every action. Take screenshots or export PDFs showing the Prey device view, Lost Mode activation, lock/wipe confirmations, and any IdP session revocations. Save everything in your incident evidence folder using ISO timestamps. These artifacts save you time during reviews, audits, or regulatory follow-up—and protect your team by showing exactly what was done and when.


## Decision cues

There are a few quick judgment calls that can steer your response in the right direction. These aren't long investigations—just simple cues that help you decide how aggressive you need to be in the first hour. Keeping these in mind prevents hesitation and keeps the incident moving smoothly. Here's what to look for and how each one affects your next step:

- **Unencrypted device:** If the laptop isn't encrypted, assume a higher level of exposure. Loop in Legal or Privacy right away and lean toward performing a full wipe on corporate devices. Without encryption, even a short window of unauthorized access could matter.

- **Theft vs. misplacement:** Try to get a sense of whether the laptop was likely stolen or simply left behind. Clear signs of theft—forced entry, suspicious activity, or a last-seen location that raises concerns—mean you should involve the police and alert your insurance provider. If it's probably just misplaced, focus on Lost Mode, tracking, and short-term monitoring before escalating.

- **BYOD considerations:** When the device belongs to the employee, the rules change. Stick to selective wipes that target work data only, and coordinate directly with the user to avoid disrupting their personal content. Transparency matters here—keep them informed as you proceed.

# T+1 → T+2h: verification & risk triage

Once the immediate containment steps are done, the next few hours are about understanding the real level of risk and picking the right response path. You're no longer reacting—you're validating. This stage helps you separate low-impact losses from situations that need broader escalation. Here's what to review and why it matters:

- **Confirm encryption and screen-lock status:** Check whether BitLocker, MBAM, FileVault, or LUKS was active and verify that the device enforced a proper screen lock. Encryption gives you breathing room; missing controls push the risk higher.
- **Review last-seen and geo context:** Look at the last known location and what it tells you—was the laptop at the office, on a commute route, at an airport, or somewhere known for theft? Mark anything that signals elevated risk.
- **Check data sensitivity:** Consider the kind of work tied to this device. Did the user handle regulated data like PHI, PCI, student records, or export-controlled information? Also check whether any apps might have cached files locally, including sync clients or browser downloads.
- **Identity & access checks:** Review your IdP logs for suspicious post-loss activity—impossible travel alerts, unusual IP addresses, or unfamiliar device fingerprints. If the user holds elevated privileges, rotate passwords immediately to prevent unauthorized access through their accounts.

## Risk branch selection

Once you've reviewed the facts, it's time to decide which response path fits the situation. This "risk branch" determines how far you need to go and how quickly. Choosing the right one keeps your effort aligned with the actual exposure—neither overreacting nor leaving gaps. Here's how to interpret what you've found:

- **Low risk:** If the device is encrypted, the user doesn't handle regulated data, and all sessions have already been revoked, you're in the safest category. Keep tracking the device and avoid wiping it unless recovery starts to look unlikely.
- **Moderate risk:** This applies when the device is encrypted but tied to sensitive tasks, or when a BYOD laptop has broad access to work apps and data. In these situations, go ahead with a selective wipe and loop in Legal to confirm you've met internal requirements.
- **High risk:** Unencrypted laptops, regulated data exposure, or devices belonging to users with elevated privileges fall into the highest concern level. These cases usually warrant a full wipe on corporate devices, wider credential rotation, and the start of a formal breach assessment.

# T+3 → T+24h: notifications & external reporting

By the four-hour mark, you should have a clear sense of the situation. Now the focus shifts to keeping the right people informed and meeting any legal or contractual requirements. This window is about coordination, making sure stakeholders understand what happened, what's been done, and what comes next. It also ensures you don't miss any obligations tied to theft, insurance, or potential data exposure.

## Here's what to cover:

- **Internal notifications:** Update the manager, Privacy/Legal, Compliance, and Security leadership so everyone is aligned on the incident's status. Loop in HR if the loss involves policy violations or disciplinary follow-up.
- **External notifications (when necessary):**
  - **Insurance:** Share the police report number (if applicable), the device's asset value, encryption status, and the actions already taken.
  - **Law enforcement:** Contact police when theft is probable—such as forced entry, CCTV confirmation, or a suspicious last-seen location. Provide the serial or IMEI, last-seen details, and your company's contact information.
  - **Regulatory/contractual:** If regulated data may be at risk and the device wasn't encrypted, you may need to start the breach-assessment process. Legal and Privacy should guide you in drafting notices for customers, partners, or authorities.

- **Communications pack:** Prepare short, helpful messages:
  - **Employee update:** “We’ve placed your device in Lost Mode and revoked access. If found, please call … We may proceed with a wipe to protect data.”
  - **Executive briefing:** Five concise bullets covering what happened, actions taken, the risk level, planned next steps, and the estimated time to resolution.
  - **Evidence consolidation:** Collect and attach logs, screenshots, wipe or lock confirmations, and email threads to the incident ticket. Update your loss register to keep asset records current and ensure the case is traceable later.

# BYOD vs Corporate: divergent paths

When a laptop goes missing, the response isn’t one-size-fits-all. How you proceed depends heavily on whether the device belongs to the company or the employee. Clear paths for each model help you stay consistent, respect boundaries, and apply the right level of control without slowing down containment or recovery.

## BYOD (work profile/container)

For personally owned devices, the priority is protecting work data without touching anything personal. The goal is to keep the response respectful, minimal, and compliant with the agreements the employee accepted when enrolling the device.

- **Default:** Apply a selective wipe that removes only work apps and data. Personal photos, messages, and files must remain untouched.
- **Consent & notice:** Reference the BYOD consent form and remind the user of any privacy guardrails, especially around off-hours actions.
- **User steps:** Provide instructions for unenrolling the device if they choose, and confirm once the recovery or unenroll process is complete.

## Corporate-owned

Company hardware gives you full administrative authority, and your response can be more direct. These devices typically hold more sensitive data and are bound by stricter policies, so faster and broader actions are justified.

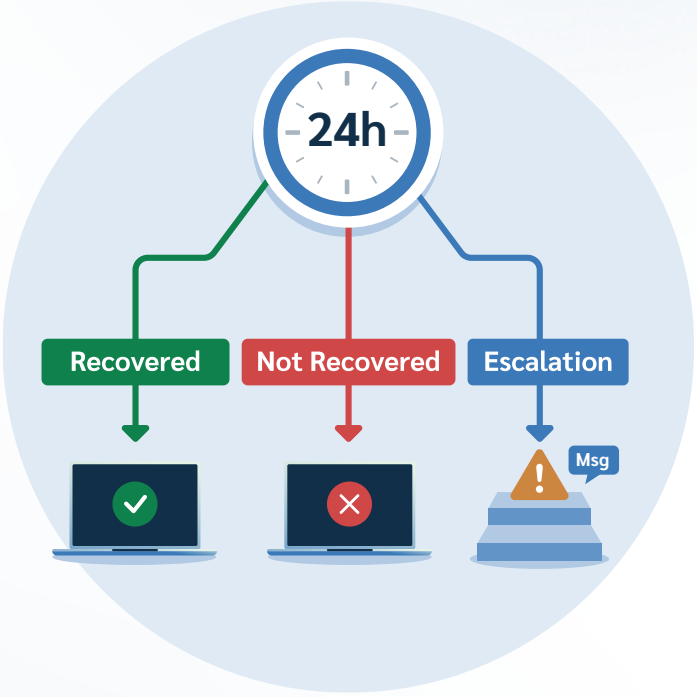
- **Default:** Lock the laptop immediately and perform a full wipe in high-risk cases or once 24 hours pass without recovery and risk remains unclear.
- **Return & intake:** If the device is returned, send it to IT for forensic checks and a full re-image. It should not go back to the user in its existing state.

### Edge cases (both models)

Traveling executives, journalists, researchers, and employees in unionized environments may have communications that require extra handling. Consult Legal before performing a full wipe if the device may contain protected or sensitive materials, and document the reasoning behind your decision.

## After 24 hours: recovery, closure, or escalation

After the first day, you should have enough information to either close the case, continue tracking, or escalate. This window is where you shift from rapid response to follow-through: confirming outcomes, tightening any loose ends, and preparing for the longer-term steps that keep your incident process reliable and repeatable.



## If recovered

When the laptop makes its way back, don't hand it right back to the user. Treat it as evidence first. You'll need to confirm whether it was tampered with, validate its security posture, and properly re-enroll it before returning it to service. This protects both the organization and the person assigned to the device.

- **Chain of custody:** Record who found it, where it was found, and when. Capture signatures and timestamps so there's a clear trail.
- **Forensics:** Review EDR logs, check for tamper events, and compare file or disk hashes as needed. Use these findings to decide whether a clean-up is enough or if a full re-image is safer.
- **Re-enroll:** Add the device back to your MDM, apply your hardening baseline, and give the user a quick refresher on safe handling before returning it.

## If not recovered

If the device still hasn't surfaced by the 24-hour mark, move into finalization mode. At this point, your focus is ensuring all protective actions completed correctly and that credentials or secrets tied to the device are fully rotated. Wrapping up cleanly here prevents long-term risk from lingering.

- **Finalize actions:** Confirm the device wipe succeeded and store the log or receipt. Keep Lost Mode active if it still adds recovery value.
- **Accounts & secrets:** Rotate all passwords, tokens, and API keys tied to the user. For developer devices, treat repo secrets and SSH keys as compromised and rotate accordingly.
- **Closure packet:** Gather the ticket summary, evidence, cost impact, and any KPIs that need updating, then attach them to the incident record.

# Post-mortem (within 7 days)

A short, structured review within a week helps strengthen your response process and reduces repeat incidents. Keep it focused, factual, and tied to specific actions your team can take.

- **Root cause:** Identify whether the issue stemmed from process gaps, user habits, or physical security weaknesses.
- **Control improvements:** Check for missing encryption, poor screen-lock habits, geofencing settings, or flaws in your asset checkout process, and update controls as needed.
- **Training & awareness:** Schedule quick refreshers if user behavior contributed, and update the runbook if any step in the response caused unnecessary delays.

## 7) Downloadables (deliver with the article)

- **1-page Lost Corporate Laptop Checklist** (PDF/DOCX): 10–12 numbered steps (fits on a single page).
- **Incident Report Template:**
  - Reporter, date/time, asset tag/serial, owner, last-seen, encryption status, data sensitivity, actions taken (timestamps), evidence links, notification log, decision branch, final disposition, lessons learned.
- **Helpdesk Intake Script:** 6 questions to confirm identity, last known location/time, sensitive data flags, and whether law enforcement was contacted.

## 8) Appendix — Evidence & audit log cheat sheet

- **What to export (and from where):**
  - **Prey:** Device card (PDF), Lost Mode activation/log, Lock/Wipe receipts, last-seen timeline.
  - **IdP/SSO:** Session revocations, password reset events, suspicious login report.
  - **EDR:** Last heartbeat, alerts post-loss, tamper events.
  - **Ticketing system:** Full action timeline (who/what/when), attached artifacts.

## 9) Decision trees (visuals recommended in-article)

- **A) Ownership branch**
  - Corp → encrypted? → yes (monitor+lock) / no (wipe+notify)
  - BYOD → selective wipe? → if regulated data → yes; else monitor+revoke tokens
- **B) Data sensitivity branch**
  - Regulated data present → initiate breach assessment with Legal
  - No regulated data, encrypted → standard closure path

# Metrics & ops health

Tracking the right metrics helps you show that your lost-device process is more than a quick reaction, and it's a measurable, reliable part of your security program. These numbers highlight whether your team is moving fast enough, documenting thoroughly, and improving over time. They also make it easier to justify investments and fix recurring gaps before they grow.

- **Time-to-lock (goal ≤ 30 min):** How quickly you freeze access once a device is reported missing.
- **Time-to-wipe (goal ≤ 2 hrs after decision):** If a wipe is required, the speed of execution matters just as much as the decision itself.
- **% devices with verified encryption (goal 100%):** A simple but critical baseline, every device should be encrypted, no **exceptions.**
- **% incidents with full evidence bundle attached (goal 100%):** Ensures clean documentation for audits, legal reviews, and internal accountability.
- **Recovery rate vs wiped:** Track how many devices come back versus how many require wiping, and monitor trends each quarter.
- **Mean Time to Resolution (MTTR):** Your overall efficiency, how long it takes to close an incident from first report to final documentation.

# Integrating Prey Into Your Lost-Laptop Playbook


Prey fits neatly into a lost-device workflow because it stays light on complexity while delivering a lot of practical value. It gives teams the essentials they need: fast visibility, quick actions, and clean evidence, without adding extra overhead.

These touchpoints help streamline each stage of the incident and keep everything moving with less friction. Here's where it shines:

- **Inventory & tags:** Quickly identify the device owner, last-seen details, and apply bulk actions to specific groups like "Sales-Laptops-US."
- **Lost Mode:** Add a custom callback message and optional audible alert to boost recovery odds without leaking personal information.
- **Remote Lock/Wipe:** Apply the right control depending on ownership, full wipes for corporate laptops, selective wipes for BYOD.
- **Audit logs & automation:** Export logs as evidence and use webhooks or the API to automatically attach lock/wipe receipts to your incident ticket.

# About Prey

Founded in 2009, we began with a singular mission: to help organizations master control over their technology. Today, Prey has evolved into an **all-in-one management and security ecosystem for global fleets**. Moving far beyond recovery, we empower businesses to orchestrate software deployment, enforce strict security policies, and safeguard critical data. We are the strategic partner built to secure the modern remote workforce, ensuring both regulatory compliance and seamless operational continuity.

Prey for: **Organizations** | **Education** | **People**

Prey Inc. © 2022548 Market St. #30152

San Francisco, CA 94104

United States of America