/ CYBERCRIME INVESTIGATION

# EVIDENCE HANDLING GUIDE

What to preserve. Before we arrive. Before you touch anything.

| | |
|---|---|
| ISSUED BY | Acta Security // actasecurity.eu |
| JURISDICTION | EU — Portugal (ops) |
| EVIDENCE CHANNEL | Chat on website / browser-based |
| RESPONSE | < 1 hour target / 24 · 7 · 365 |
| DATA | EU-hosted · EU & ZA resident operators · EU chain of custody |
| APPLIES TO | Insider theft · driver/fleet devices · CRM & infrastructure misuse · payment fraud (BEC) · malware / RAT / MaaS exfiltration |
| VERSION | 2026.06 / for client use |

// CONTENTS



> *"We tell you what we found, what we couldn't find, and what we didn't have time to look for."*
>
> — ACTA SECURITY

// 01_GENERAL_RULES

# General evidence rules.

These apply no matter what you suspect. Get these right first — the specifics are on the next page.

**01 STAY CALM**
Panic causes people to destroy the exact evidence that would prove their case. Slow down — you have more time than it feels like.

**02 DON'T TOUCH THE DEVICE**
Don't open apps, scroll through it, or "just check something" on the device itself. Every touch can overwrite what you're trying to prove.

**03 DON'T REBOOT OR RESET**
Powering off, factory-resetting, or "logging out to be safe" destroys exactly the data an investigation depends on.

**04 DON'T LET OTHERS HANDLE IT**
Limit access to one person until Acta advises. Every extra hand that touches it is a break in the chain of custody.

**05 NOTE THE EXACT TIME**
Write down when you found this, what state the device or account was in, and who was present. Timestamps matter more than they seem to.

**06 PRESERVE THE ORIGINAL**
If it's a document, email, or letter — keep the original file, account, or device untouched. Work from a copy if you need to look again.

**07 ONE POINT OF CONTACT**
Designate one person — HR, legal, or management — to liaise with Acta. Don't loop in the wider team yet.

**08 CONTACT ACTA BEFORE ACTING**
Even if you're sure what happened, confirm with Acta before confronting anyone, changing access, or starting disciplinary action.

DO NOT — THESE ACTIONS DESTROY EVIDENCE OR TIP OFF THE SUSPECT

- Confront the suspected employee, driver, or contact before evidence is secured.
- Forward, print, or copy evidence into new places "for safekeeping."
- Delete anything — even things that seem unrelated or irrelevant.
- Send money or reply to a suspected fraudulent payment instruction before it's verified.
- Run cleanup tools, reset passwords, or "test" the account or device yourself.
- Post about it in Slack, Teams, or discuss it outside the case team.
- Return the device to the person under investigation.
- Assume it's fine because "it's just a phone" or "it's just a shared account."

// 02_CASE_TYPE

# Case-type guidance.

Preserve this, avoid that — specific to what you're actually dealing with.

## // INSIDER THREAT & EMPLOYEE DATA THEFT

| | |
|---|---|
| PRESERVE | The device in its current state, the company email account (don't disable it yet), CRM/cloud access logs, and USB or external-drive history. |
| DO NOT | Confront the employee, wipe or reissue the device, or revoke access before evidence is pulled — unless exfiltration is actively ongoing. |
| NOTE | Employee monitoring is subject to local labour law. Confirm legal basis with counsel before reviewing personal communications. |

## // FLEET / DRIVER DEVICE — TIME-OF-INCIDENT PHONE USE

| | |
|---|---|
| PRESERVE | The device exactly as it was at the time of the incident. Note the carrier/network and the exact incident timestamp, with time zone. |
| DO NOT | Let the driver factory-reset, update the OS, or delete messaging/call apps. Don't rely on the driver's own account of app usage. |
| NOTE | Carrier data retention windows are short — the sooner the device and timestamp are confirmed, the more is recoverable. |

## // CRM / INFRASTRUCTURE MISUSE

| | |
|---|---|
| PRESERVE | Access logs, export/download logs, and admin or audit-trail exports — before log retention windows roll over. |
| DO NOT | Revoke the suspected account's access in a way that alerts them, unless exfiltration is actively ongoing. |
| NOTE | Correlating access with known events (resignation date, competitor start date) is useful — but don't act on it until confirmed. |

## // BEC / PAYMENT FRAUD — FAKE BANK-CHANGE LETTERS

| | |
|---|---|
| PRESERVE | The original fraudulent email or letter with full headers (not just the text), the mailbox involved, and related invoices or correspondence. |
| DO NOT | Forward the fraudulent instruction further, delete it 'to stop it spreading,' or contact the fraudulent account holder yourself. |
| NOTE | Speed matters most here. Banks can sometimes recall a payment within hours. Contact Acta and your bank's fraud team immediately. |

## // MALWARE / RAT / MAAS DATA EXFILTRATION

| | |
|---|---|
| PRESERVE | The infected device disconnected from the network — Wi-Fi off, cable pulled — left powered on if at all possible. |
| DO NOT | Run antivirus or cleanup tools, reboot, or reinstall the OS. This overwrites the evidence of what the malware did. |
| NOTE | On mobile, don't factory-reset 'to be safe' — this is the single most common way spyware/RAT evidence gets destroyed. |

### ⏱ REGULATORY CLOCK — IF PERSONAL DATA WAS INVOLVED IN ANY OF THE ABOVE

**GDPR Art. 33:** notify the supervisory authority within 72h of discovery. **NIS2:** 24h early warning + 72h full notification.

**DORA:** 4h to report a major ICT-related incident once classified. The clock starts at discovery — not at confirmation.

// 03_CHAIN_OF_CUSTODY

# Chain of custody basics.

One gap in the chain and the evidence is worth less — to your board, your insurer, or a court.

### WHAT IT MEANS

Being able to account for a piece of evidence — who had it, when, and what happened to it — from the moment it was found to the moment it's used. If any step can't be accounted for, the value of the evidence drops.

### KEEP IT INTACT

Log every person who touches the device, account, or document, with date and time. Keep physical evidence locked away. Never route evidence through personal devices, email, or cloud storage. Hand off only to Acta or your designated legal contact.

## // 04 · HOW TO REACH ACTA

### PRIMARY CONTACT — BROWSER-BASED CHAT // NO APP REQUIRED

**STEP 1 — OPEN THE EVIDENCE CHANNEL**
Open the chat on our website in any browser — works on desktop or mobile.

**STEP 2 — NO ACCOUNT NEEDED**
No phone number, no email, no registration. The channel is always open.

**STEP 3 — SEND YOUR FIRST MESSAGE**
State: organisation name // what you suspect // what evidence exists // when it started.

**STEP 4 — RESPONSE TIME**
An operator responds within 1 hour — typically faster. 24 / 7 / 365.

/ no phone number · no account · EU-hosted · data stays in Europe

### // WHAT HAPPENS AFTER YOU CONTACT US

**T+0 — TRIAGE**
Operator confirms case type and any urgent preservation needs from your description.

**T+1H — SCOPE CALL**
Structured intake: what happened, what evidence exists, who's involved.

**T+24H — EVIDENCE PLAN**
Written plan: what to acquire, in what order, and any legal considerations flagged.

**T+3–5D — ACQUISITION**
Forensic imaging and collection begins under chain of custody.

**T+1–3W — ANALYSIS & REPORT**
Findings report, plus regulatory or legal reporting support where required.

EVIDENCE CHANNEL
**Chat on website / browser-based**

WEBSITE
**actasecurity.eu**

OPS BASE
**Porto, Portugal · Remote EU & South Africa**

*We tell you what we found, what we couldn't find, and what we didn't have time to look for.* — Acta Security