INDEPENDENT FORENSICS

DIGITAL EVIDENCE FIRST AID KIT

A Legal & HR Guide to Evidence Preservation

Prepared by: Independent Forensics

CRITICAL RULE: DO NO HARM

Digital evidence is volatile. Standard IT practices (copying files, booting up, or "checking" folders) can alter metadata and make evidence inadmissible. To ensure a legally defensible investigation, follow these standards derived from IACIS and SWGDE best practices.

---

1. MOBILE DEVICE PROTOCOL

- **ISOLATE IMMEDIATELY:** Place the device in **Airplane Mode** to prevent a remote wipe or incoming data (which overwrites deleted space).
- **POWER STATUS:** If the device is ON, keep it ON and connected to a power source. Modern encryption may make it impossible to re-enter a device once it is powered off (AFU vs. BFU states).
- **BIOMETRICS:** Do not look at the screen if FaceID is active. Repeated failed attempts can lock the device permanently.

2. COMPUTER & LAPTOP PROTOCOL

- **IF POWERED OFF: DO NOT TURN IT ON.** Booting an Operating System writes thousands of small files to the disk, potentially overwriting the "deleted" data you are looking for.
- **IF POWERED ON:** Do not perform a "Shut Down." This clears the **RAM (Volatile Memory)** which may contain active passwords, unencrypted files, or chat fragments. Call a specialist for a "Live Memory Capture."
- **ACCESS:** Stop all "triage" by internal IT staff. Standard administrative tools do not use **Hardware Write-Blockers**, meaning every file opened has its "Last Accessed" metadata permanently altered.

3. THE CHAIN OF CUSTODY (SWGDE STANDARD)

To survive a "Motion to Suppress," you must prove the evidence remained unchanged.

- **SECURE:** Place the device in a static-safe bag and a locked cabinet with restricted access.
- **DOCUMENT:** Create a log for every person who handles the device.
    - *Who took possession?*
    - *When (Date/Time)?*
    - *Where was it stored?*
    - *Why was it moved?*

4. CLOUD & REMOTE DATA

- **PASSWORD PROTOCOL:** If you have access to credentials for Microsoft 365, Google, or Dropbox, do not log in via a standard browser. This creates new "Access Logs" that can complicate a forensic timeline.
- **PRESERVATION LETTERS:** Immediately send a preservation letter to the service provider to prevent automated data retention rotations.

WHEN TO CALL INDEPENDENT FORENSICS

We utilize industry standard tools and certified forensic examiner to ensure your evidence is handled with the highest level of integrity.

- **Forensic Imaging:** Bit-for-bit cloning with physical write-protection.
- **Deleted Content Recovery:** Carving for fragments in unallocated space.
- **Expert Reporting:** Clear, technical analysis ready for the courtroom. **|**

mfeterick@independentforensics.net

765-357-4710