DIGITAL FORENSICS

Evidence Handling & Chain of Custody Checklist

Good evidence handling protects your investigation, insurance claim, and legal options. Follow these steps, and record every transfer on the chain-of-custody form.

Before collecting

- [ ] Confirm authority to collect (legal counsel, HR, and system owner as appropriate)
- [ ] Document the scene: photos, screen contents, running processes, network connections
- [ ] Decide on order of volatility: memory and live data before disk
- [ ] Use clean, write-protected collection media and forensic tools

Collecting

- [ ] Capture memory before shutting down when feasible
- [ ] Create forensic images of disks and record SHA-256 hashes
- [ ] Export cloud and SaaS audit logs (Microsoft 365, Google Workspace, identity provider)
- [ ] Collect firewall, VPN, endpoint, DNS, and email logs with time zones noted
- [ ] Record who collected each item, when, where, and how

Storing and transferring

- [ ] Label and seal each item; store in a locked, access-controlled location
- [ ] Work only on verified copies; keep originals untouched
- [ ] Record every transfer on the chain-of-custody form
- [ ] Retain evidence per legal hold, contract, and regulatory requirements (for example, 90 days for DFARS 252.204-7012 images)

Chain-of-Custody Form

Case / incident #		**Item #**	
Description (make, model, serial, label)			
Collected by / date / time		**Hash (SHA-256)**	

Date / time	Released by (name, signature)	Received by (name, signature)	Purpose / location

General guidance for training and planning, not legal advice. Adapt to your environment, contracts, and regulators.