

Digital Evidence Preservation Checklist (Quick Guide)

This quick-reference checklist summarizes commonly recognized early-stage practices intended to reduce the risk of alteration, loss, or evidentiary dispute involving digital information. It is provided for general informational purposes to support preservation-focused handling and documentation prior to detailed forensic analysis or legal strategy. Application may vary based on authorization, scope, and case circumstances.

Illustrative checklist only. Steps vary by source type, timing, authorization path, and confirmed scope.

1. Preserve first - avoid altering devices, accounts, or data before scope and authorization are defined.
2. Begin with written scope - identify potential data sources and preservation objectives.
3. Minimize handling - limit preservation activity to materials within defined scope.
4. Record context - document who provided the data, when it was obtained, and the method of transfer.
5. Maintain originals separately - perform review or processing from working copies where feasible.
6. Verify integrity where applicable - record hash values or comparable verification artifacts when feasible and within scope.
7. Use secure transfer methods - follow agreed transfer procedures and confirm receipt.
8. Document each hand-off - maintain a chronological custody and handling record.