PROVIDED BY VENIO SYSTEMS

eDiscovery Chain of Custody Checklist and Record

A stage-by-stage checklist, plus a ready-to-use custody record and transfer log for defensible eDiscovery.

Provided as a free resource by Venio Systems — www.veniosystems.com. This resource is general guidance, not legal advice. Adapt it to your jurisdiction, your matters, and the advice of counsel.

SECTION 1

1 How to Use This Checklist

Chain of custody is the documented, unbroken record of who handled a piece of electronic evidence, when, how, and what changed. A clean record keeps your evidence admissible and lets you defend your process if it is challenged.

Use this document in three ways:

1. Complete one Chain of Custody Record (Section 2) for each evidence item or data set you collect.
2. Log every handoff in the Transfer and Access Log (Section 3) as it happens, not from memory later.
3. Work through the stage checklists (Sections 4 to 6) at each phase of the matter to confirm nothing is missed.

SECTION 2

2 Chain of Custody Record

Complete one record per evidence item or data set. Keep it with the evidence throughout the matter.

Matter name and number	
Evidence item or data set ID	
Description and data source	
Custodian (data owner)	
Collected by (name, role, organization)	
Collection date and time	
Collection method or tool	
Original location	
Storage location after collection	
Hash algorithm (for example, SHA-256)	
Hash value at collection	
Notes	

3

SECTION 3

Transfer and Access Log

Record every transfer, access, or processing step. An unexplained gap is what opposing counsel looks for.

Date and time	From	To	Purpose	Hash verified (Y/N)	Initials

4

SECTION 4

Stage-by-Stage Checklist

Confirm each item at the relevant phase of the eDiscovery lifecycle.

4.1 Identification and preservation

- [ ] Legal hold issued, and custodian acknowledgments tracked
- [ ] Data sources and custodians identified and mapped
- [ ] Automatic deletion and retention policies suspended for relevant data
- [ ] Preservation scope and decisions documented

4.2 Collection

- [ ] Collection performed by a qualified person using a forensically sound method
- [ ] Original data left unaltered, with write protection where applicable
- [ ] Hash value generated at the point of collection
- [ ] Source, date, time, method, and collector are recorded in the custody record
- [ ] Metadata is preserved and not overwritten by opening or copying files

4.3 Processing

- [ ] Hash values re-verified after ingestion into the platform
- [ ] Processing steps, errors, and exceptions logged
- [ ] De-duplication and filtering criteria documented

4.4 Review and analysis

- [ ] Role-based access controls applied to the data set
- [ ] All access and actions are captured in audit logs
- [ ] No data handled or edited outside controlled workflows

4.5 Production

- [ ] Produced items are traceable back to their original source
- [ ] Production format, Bates numbering, and any redactions documented
- [ ] Final hash verification completed before delivery
- [ ] Production log retained with the matter file

5

SECTION 5

Self-Authentication Readiness (FRE 902(14))

Under Federal Rule of Evidence 902(14), a digital copy of data can be self-authenticated by a written certification from a qualified person who verified that its hash value matches the original. Meeting the items below can remove the need for live foundation testimony at trial.

- [ ] Collection performed and documented by a qualified person
- [ ] Hash value of each item verified as identical to the original
- [ ] Written certification is prepared and available
- [ ] The opposing party was given reasonable notice and an opportunity to inspect

Confirm current requirements and your jurisdiction with counsel before relying on self-authentication.

SECTION 6

Red Flags That Break the Chain

Treat any of the following as a custody risk that needs to be corrected or documented.

- [ ] Self-collection by custodians without forensic guidance
- [ ] Files transferred by personal email or unsecured cloud storage
- [ ] Documents opened or edited outside controlled workflows
- [ ] Gaps or missing entries in the custody log
- [ ] Data moved between disconnected tools without re-verifying the hash

Want custody tracked automatically, end-to-end?

See how a unified platform keeps the chain of custody intact from legal hold through production: **book a Venio demo**.