BOF LOGISTICS & TRANSPORT ENTERPRISES

Document Retention Standard

Enterprise Compliance Policy — Commercial Trucking & Logistics Operations

Policy Number	BOF-POL-007	**Version**	2.0
Effective Date	July 16, 2026	**Review Cycle**	Annual
Policy Owner	Director of Compliance and Legal Affairs	**Approved By**	Chief Operating Officer (COO)
Classification	Internal Controlled Document	**Supersedes**	BOF-POL-007 v1.x (all prior versions)
Issuing Department	Compliance & Legal Affairs	**Next Review Date**	July 16, 2027

⚠️ Legal Notice

This policy is legally binding upon all employees, contractors, and agents of the company. Violation of this policy — including premature destruction of records, failure to implement a litigation hold, or unauthorized disclosure — may result in disciplinary action up to and including termination, and may expose the company to regulatory penalties and litigation sanctions. Questions regarding this policy should be directed to the Director of Compliance and Legal Affairs.

Table of Contents

1. Purpose and Scope

1.1 Purpose

This policy establishes binding retention schedules, storage standards, and destruction procedures for all operational, regulatory, financial, and personnel records across the enterprise. The purpose of this Document Retention Standard is to ensure that the company:

- Maintains full compliance with all applicable federal and state regulatory record-keeping mandates governing commercial trucking and logistics operations;
- Is prepared to respond to litigation, government investigations, audits, and regulatory compliance reviews with complete, authentic, and readily accessible records;
- Protects the company from adverse legal inferences, sanctions, and penalties that may result from premature, improper, or selective destruction of records;
- Manages records efficiently throughout their lifecycle — from creation or receipt through active use, inactive storage, and ultimate disposition — to minimize cost and operational burden;
- Protects employee, customer, and business partner privacy through appropriate controls on sensitive and personally identifiable information (PII).

1.2 Scope

This policy applies without exception to:

- **All personnel:** Full-time and part-time employees, independent contractors, owner-operators under lease, temporary workers, interns, and agents acting on behalf of the company;
- **All record types:** Physical (paper) records, electronic records (including email, text messages, electronic data interchange records, scanned documents, and database entries), and any other medium on which company information is stored;

- **All company locations:** Corporate headquarters, terminal and yard facilities, satellite offices, and all remote or home-office environments where company business is conducted;
- **All systems:** Company-owned and company-leased hardware, software, cloud platforms, Electronic Logging Devices (ELDs), Transportation Management Systems (TMS), and Electronic Records Management Systems (ERMS).

📌 **Scope Note**

This policy governs records in all formats. The retention period for a record is determined by its

content and regulatory category

, not by the medium on which it is stored. An electronic bill of lading has the same retention requirement as a paper bill of lading.

2. Regulatory References

This policy is developed in compliance with, and incorporates the requirements of, the following federal and state regulatory frameworks. In the event of a conflict between this policy and applicable law, the more stringent requirement shall govern.

Regulatory Authority	Citation / Reference	Primary Applicability
Federal Motor Carrier Safety Administration (FMCSA)	49 CFR Parts 390, 391, 395, 396	Driver qualification, hours of service, vehicle inspection and maintenance, general recordkeeping
Internal Revenue Service (IRS)	IRS Publication 583; IRC §§ 6001, 6501	Financial records, tax returns, payroll, business expense substantiation
Equal Employment Opportunity Commission	29 CFR Part 1602; Title VII; ADA; ADEA	Employment applications, personnel records,

Regulatory Authority	Citation / Reference	Primary Applicability
(EEOC)		discrimination complaint files
Occupational Safety and Health Administration (OSHA)	29 CFR Part 1904	Workplace injury and illness records, OSHA 300 Logs, incident reports
Department of Transportation (DOT) — Drug & Alcohol	49 CFR Part 40; 49 CFR Part 382	Drug and alcohol testing records, consortia records, return-to-duty documentation
Carmack Amendment	49 U.S.C. § 14706	Cargo claim records, bills of lading, freight liability documentation
Sarbanes-Oxley Act (SOX)	15 U.S.C. §§ 7241–7266; SEC Rules	Financial statements, audit records, internal controls documentation (as applicable)
Federal Rules of Civil Procedure (FRCP)	FRCP Rule 37(e); Rule 26	Electronically stored information (ESI), litigation hold obligations, spoliation avoidance
State Workers' Compensation Laws	Ohio Rev. Code § 4123 et seq. (and applicable state equivalents)	Workers' compensation claims, medical records, return-to-work documentation
State Employment and Privacy Laws	Various — Ohio, and each state of operation	Personnel records, wage records, benefits records, PII protection
Insurance Regulatory Requirements	Per applicable policy terms and state insurance codes	Insurance policies, certificates of insurance, claims files, endorsements

ⓘ Compliance Note

This table is not exhaustive. The Director of Compliance and Legal Affairs is responsible for monitoring regulatory changes and updating this policy accordingly. Department heads are responsible for flagging newly applicable regulatory requirements within their operational area to the Compliance department within 30 days of identification.

3. Definitions

For purposes of this policy, the following terms are defined as set forth below. Where a term is also defined by applicable law or regulation, the regulatory definition shall apply to the extent it is more specific or expansive.

Term	Definition
Record	Any document, data, or information — regardless of format or medium — created, received, or maintained by the company in the conduct of business, that serves as evidence of a transaction, decision, obligation, regulatory requirement, or operational activity. A Record is distinguished from a *convenience copy*, which is a duplicate maintained for reference only and which may be destroyed once the official Record is confirmed to exist.
Retention Period	The minimum length of time a Record must be maintained before it is eligible for scheduled destruction. Retention periods are expressed in years from the date of creation, last modification, or a triggering event (e.g., termination of employment, expiration of contract), as specified in Section 4.
Destruction	The permanent, irreversible elimination of a Record such that it cannot be read, reconstructed, or used. Destruction methods vary by record type and sensitivity, as specified in Section 8.
Litigation Hold	A directive issued by the Director of Compliance and Legal Affairs suspending the scheduled destruction of Records that are or may be relevant to pending, threatened, or reasonably anticipated litigation, government investigation, or regulatory proceeding. Also referred to as a Legal Hold.
Electronic Records Management System (ERMS)	A software platform or suite of platforms approved by the company for the creation, storage, indexing, retrieval, retention scheduling, and disposition of electronic Records. The ERMS is the authoritative repository for electronic records subject to this policy.
Active Record	A Record that is currently in use for ongoing business operations and is maintained in primary storage (on-site filing systems or active electronic repositories).
Inactive / Archived Record	A Record that is no longer needed for day-to-day operations but must be retained to satisfy retention schedule requirements. Inactive

Term	Definition
	Records are transferred to secondary storage (off-site or archive repositories).
Legal Hold	See Litigation Hold. Used interchangeably within this policy.
Personally Identifiable Information (PII)	Any information that, alone or in combination with other information, can be used to identify a specific individual. Includes but is not limited to: Social Security numbers, driver's license numbers, date of birth, medical information, financial account numbers, drug test results, and biometric identifiers.
Confidential Record	A Record designated as sensitive due to its content, including but not limited to: personnel files, medical records, drug and alcohol test results, litigation files, attorney-client privileged communications, trade secrets, and financial records. Confidential Records require heightened access controls and specialized destruction procedures.
Record Custodian	The individual or department designated as responsible for the creation, maintenance, security, retention, and proper disposition of a specific category of Records. Custodians are identified in Section 4 (Retention Schedule) and Section 10 (Roles and Responsibilities).
Superseded Document	A prior version of a policy, procedure, form, or standard operating document that has been replaced by a current version. Superseded documents are subject to their own retention requirements as specified in applicable schedules and must not be destroyed if subject to a Litigation Hold.

4. Retention Schedule by Record Category

The Master Retention Schedule set forth in this section constitutes the binding minimum retention standards for all record categories within the scope of this policy. No record shall be destroyed before its minimum retention period has elapsed. In the event that a regulatory authority prescribes a longer retention period than set forth herein, the regulatory requirement shall govern. A condensed quick-reference version appears in Appendix A.

⚠️ **Critical Requirement**

Before initiating destruction of any record, the responsible custodian MUST verify: (1) the minimum retention period has elapsed; (2) no Litigation Hold or Legal Hold is in effect for the record or its category; and (3) a completed Destruction Authorization Form (Appendix C) has been signed by the authorizing officer. Failure to satisfy all three conditions constitutes a policy violation.

4.1 Driver and Qualification Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
Driver Qualification Files — Active Drivers	Duration of employment + 3 years post-termination	49 CFR § 391.51	HR/Safety — locked physical file; ERMS driver profile	Safety Department	Cross-cut shred / Secure electronic wipe
Driver Qualification Files — Terminated Drivers	3 years post-termination	49 CFR § 391.51	Off-site archive; ERMS archived folder	Safety Department	Certified shred vendor / Secure wipe
Drug and Alcohol Testing Records — Positive Results / Refusals	5 years	49 CFR § 382.401; 49 CFR § 40.333	Locked DER file; ERMS — restricted access	Designated Employer Representative (DER) / Safety	Certified shred / Secure electronic destruction
Drug and Alcohol Testing Records — Negative Results	1 year	49 CFR § 382.401	Locked DER file; ERMS — restricted access	Designated Employer Representative (DER)	Cross-cut shred / Secure wipe
Medical Examiner Certificates (DOT Physical)	3 years from date of examination	49 CFR § 391.51(b)(7)	Driver Qualification File; ERMS	Safety Department	Cross-cut shred / Secure wipe
Road Test Certificates	3 years from date of test	49 CFR § 391.51(b)(3)	Driver Qualification File; ERMS	Safety Department	Cross-cut shred / Secure wipe
Motor Vehicle Record (MVR)	3 years per annual pull	49 CFR § 391.51(b)(9)	Driver Qualification	Safety Department	Certified shred /

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
/ Pre-Employment Screening Program (PSP) Reports			File; ERMS — restricted access		Secure wipe (PII)

4.2 Hours of Service and ELD Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
Electronic Logging Device (ELD) Records — On Device	6 months on ELD device	49 CFR § 395.22(i)	ELD device (driver-assigned unit)	Safety / IT Department	Device-level secure wipe per ELD vendor protocol
ELD Records — Company Server Backup	6 months additional after device transfer (12 months total)	49 CFR § 395.22	Company server / ERMS cloud backup	IT Department / Safety	DOD 5220.22-M wipe / certified media destruction
Driver Logs — Paper (Pre-ELD Mandate / Exemptions)	6 months from date of creation	49 CFR § 395.8(k)	Safety Department locked file	Safety Department	Cross-cut shred
Hours of Service (HOS) Violation Records	3 years	49 CFR § 395; FMCSA Enforcement Guidelines	Safety Department; ERMS	Safety Department	Secure shred / Secure wipe
HOS Supporting Documents (Fuel Receipts, Toll Records, Dispatch Records)	6 months	49 CFR § 395.8(k)(1)	Safety / Operations file; ERMS	Operations / Safety Department	Cross-cut shred / Standard electronic deletion

4.3 Vehicle and Maintenance Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
Driver Vehicle Inspection Reports (DVIR)	3 months from date of inspection	49 CFR § 396.11(c)	Terminal/yard office; ERMS	Maintenance / Safety Department	Cross-cut shred / Standard deletion
Preventive Maintenance (PM) Records	Life of vehicle + 1 year post-disposal	49 CFR § 396.3(b)	Maintenance file per unit; ERMS vehicle record	Maintenance Department	Secure shred / Secure electronic wipe
Accident and Incident Reports (DOT Reportable)	3 years from date of accident	49 CFR § 390.15(b)	Safety Department; ERMS — restricted access	Safety Department	Secure shred / Secure wipe
DOT Roadside Inspection Records	1 year from date of inspection	49 CFR § 396.9(d)	Safety Department; ERMS	Safety Department	Cross-cut shred / Standard deletion
Vehicle Lease Agreements (Owner-Operator / Equipment Lease)	Duration of lease + 3 years	49 CFR §§ 376.12; Carmack Amendment	Operations / Legal file; ERMS	Operations / Legal	Secure shred / Secure wipe

4.4 Cargo and Billing Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
Bills of Lading (BOL)	3 years from date of delivery	49 U.S.C. § 14706 (Carmack Amendment); IRS guidelines	Operations / Billing file; ERMS / TMS	Operations / Billing Department	Cross-cut shred / Standard deletion
Proof of Delivery (POD)	3 years from date of delivery	Carmack Amendment; IRS guidelines	ERMS / TMS; Billing file	Billing / Operations Department	Cross-cut shred / Standard deletion
Rate Confirmations / Load Confirmations	3 years from load date	IRS guidelines; contractual obligations	ERMS / TMS; Operations file	Operations / Sales Department	Cross-cut shred / Standard deletion
Cargo Claims Files (Active and Resolved)	5 years, or resolution + 3 years — whichever is	49 U.S.C. § 14706; 49 CFR § 370.9	Legal / Claims Department; ERMS — restricted	Director of Compliance and Legal Affairs /	Secure shred / Secure electronic

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
	longer		access	Claims	wipe
Customer Invoices and Accounts Receivable Records	7 years from date of invoice	IRS Publication 583; IRC § 6501	Finance Department; ERMS / accounting system	Finance / Accounting Department	Secure shred / Secure wipe
Factoring Agreements and Related Correspondence	Duration of agreement + 5 years	UCC; IRS guidelines; contractual obligations	Finance / Legal file; ERMS	Finance / Legal	Secure shred / Secure wipe

4.5 Financial and Corporate Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
General Ledger and Financial Statements	7 years	IRS; SOX (as applicable); state law	Finance Department; ERMS / accounting system	CFO / Finance Department	Secure shred / Secure electronic wipe
Federal and State Tax Returns and Supporting Documentation	7 years from filing date	IRS IRC § 6501(a); state tax codes	Finance / Legal file; ERMS — restricted access	CFO / Finance Department	Secure shred / Secure wipe (sensitive financial data)
Payroll Records (including wage garnishments, deductions)	7 years	IRS; FLSA; state wage and hour laws	HR / Finance Department; ERMS — restricted access	HR / Finance Department	Secure shred / Secure wipe (PII)
Corporate Governance Records (Board Minutes, Bylaws, Resolutions, Articles of Incorporation)	Permanent — Do Not Destroy	State corporate law; SOX (as applicable)	Corporate Secretary / Legal file; ERMS — highest security tier	Director of Compliance and Legal Affairs / Corporate Secretary	N/A — Permanent retention
Insurance Policies (Commercial Auto, General Liability,	Duration of policy + 10 years	State insurance codes; statute of limitations for	Legal / Finance Department; ERMS	Finance / Legal	Secure shred / Secure wipe

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
Cargo, Workers' Comp)		claims			
Contracts and Agreements (Customer, Vendor, Carrier)	Expiration or termination + 7 years	UCC § 2-725; applicable state statute of limitations	Legal / Operations file; ERMS	Director of Compliance and Legal Affairs / Operations	Secure shred / Secure wipe

4.6 Safety and Compliance Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
OSHA 300 Log (Injury and Illness Log) and OSHA 300A Summary	5 years from end of calendar year covered	29 CFR § 1904.33	Safety Department; ERMS	Safety Department	Secure shred / Secure wipe
Safety Training Records (including orientation, annual refresher, HazMat)	3 years post-training or duration of employment + 3 years (whichever is longer)	49 CFR Part 172 Subpart H; OSHA; DOT	Safety Department; ERMS; LMS platform	Safety Department / HR	Secure shred / Standard deletion
FMCSA Compliance Review Records and Corrective Action Plans	5 years from date of review	49 CFR Part 385; FMCSA enforcement guidelines	Safety / Legal Department; ERMS — restricted access	Director of Compliance and Legal Affairs / Safety	Secure shred / Secure wipe
Drug and Alcohol Program Records — General Program	Per 49 CFR §§ 382.401, 40.333 — see Section 4.1	49 CFR Part 382; 49 CFR Part 40	DER locked file; ERMS — restricted access	Designated Employer Representative (DER)	Certified shred / Secure electronic destruction

4.7 Personnel and Human Resources Records

Record Type	Minimum Retention Period	Regulatory Authority	Storage Location	Responsible Custodian	Destruction Method
Employment Applications — Hired Employees	Duration of employment + 3 years post-termination	EEOC regulations; 29 CFR § 1602.14	HR Department — locked personnel file; ERMS	Human Resources Department	Secure shred / Secure wipe (PII)
Employment Applications — Not Hired (Rejected Applicants)	1 year from date of application	29 CFR § 1602.14; ADEA regulations	HR Department file; ERMS	Human Resources Department	Secure shred / Secure wipe (PII)
Performance Reviews and Evaluations	Duration of employment + 3 years post-termination	EEOC guidelines; state employment law	HR Department — locked personnel file; ERMS	Human Resources Department	Secure shred / Secure wipe
Form I-9 (Employment Eligibility Verification)	3 years post-hire date, OR 1 year post-termination — whichever is longer	8 CFR § 274a.2(b)(2); INA § 274A	HR Department — separate I-9 binder; ERMS	Human Resources Department	Secure shred / Secure wipe (PII)
Disciplinary Records, Warnings, and Corrective Action Documentation	Duration of employment + 3 years post-termination	EEOC guidelines; state employment law; litigation preparedness	HR Department — locked personnel file; ERMS	Human Resources Department	Secure shred / Secure wipe
Workers' Compensation Claims Records (including medical and wage records)	5 years from date of claim closure	Ohio Rev. Code § 4123; state workers' comp laws	HR / Legal Department; ERMS — restricted access	HR Department / Director of Compliance and Legal Affairs	Secure shred / Secure wipe (PII/medical data)

5. Electronic Records Management

5.1 Approved Platforms

All electronic records within the scope of this policy must be created, stored, and managed within company-approved systems. The following platform categories are approved for enterprise records management:

- **Electronic Records Management System (ERMS):** The company's designated ERMS is the authoritative repository for all electronic records subject to mandatory retention. All Records must be migrated to the ERMS within 30 days of creation or receipt unless the originating system (e.g., TMS, ELD platform) is formally integrated with the ERMS through an approved data connector;
- **Transportation Management System (TMS):** Approved as the primary repository for bills of lading, load records, rate confirmations, and dispatch documents, provided TMS records are backed up to the ERMS per the schedule in Section 5.2;
- **ELD Provider Platforms:** Approved for initial HOS data capture; ELD data must be transferred to company servers within regulatory timelines;
- **Accounting and Financial Systems:** Approved for financial records subject to this policy, provided data is backed up per Section 5.2;
- **HR Information System (HRIS):** Approved for personnel records, with strict role-based access controls per Section 5.4;
- **Company-Approved Cloud Storage:** Only platforms approved in writing by IT and Compliance are permitted for storage of company records. Personal cloud storage accounts (e.g., personal Google Drive, personal Dropbox) are expressly prohibited for storage of any company records.

5.2 Electronic Record Integrity

The integrity of electronic records is essential to their admissibility in legal and regulatory proceedings and their value as audit evidence. The following integrity standards apply:

- **Hash Verification:** SHA-256 cryptographic hash verification shall be applied to all critical compliance records (including ELD data exports, drug and alcohol test results, driver qualification files, and accident records) at the time of ingestion into the ERMS and verified annually thereafter;

- **Audit Trail:** The ERMS shall maintain a complete, tamper-evident audit trail for all Records, capturing: date and time of creation or ingestion; user identity of creator or modifier; nature of any modification; and date and identity of any access event. Audit trail logs shall themselves be retained for a minimum of 7 years;
- **Backup Schedule:** Daily incremental backups and weekly full backups of all ERMS data shall be performed and verified. Backup data shall be stored in a geographically separate location from the primary server. Backup integrity shall be tested by IT on a quarterly basis, with results reported to the Director of Compliance and Legal Affairs.

5.3 File Naming and Organization

Consistent file naming is mandatory for all electronic records to ensure retrievability and compliance. The company standard naming convention is:

> 📄 **Standard File Naming Convention**
>
> [DEPT]_[RecordType]_[YYYY-MM-DD]_[SubjectID]_[Version]
>
> Example:
>
> SAFETY_DQF_2026-07-16_DRV-00147_v2
>
> Example:
>
> HR_I9_2026-03-01_EMP-00892_v1
>
> Example:
>
> OPS_BOL_2026-07-16_LD-20260716-004_v1
>
> Full naming convention guide and approved abbreviations are set forth in Appendix E.

Folder structures within the ERMS shall mirror the retention schedule categories set forth in Section 4. Sub-folders shall be organized by year and, where volume warrants, by quarter. IT and Compliance shall maintain and publish the approved folder structure map to all records custodians.

5.4 Access Controls

- **Role-Based Access Control (RBAC):** Access to electronic records in the ERMS shall be granted on the principle of least privilege — personnel shall have access only to those record categories required to perform their assigned job functions;
- **Permission Tiers:** Read-only access (available to authorized personnel for reference); Read/Write access (restricted to record custodians and their designees); Delete access (restricted to IT administrators and the Director of Compliance, and only exercisable pursuant to an authorized Destruction Authorization Form); System administration access (restricted to designated IT personnel, fully logged);
- **Administrator Access Logging:** All system administrator actions within the ERMS — including permission changes, deletions, exports, and configuration changes — shall be logged to a separate, read-only audit log reviewed by the Director of Compliance and Legal Affairs on a monthly basis;
- **Password and Authentication Standards:** Multi-factor authentication (MFA) is required for all ERMS access. Password complexity and rotation requirements shall comply with the company's Information Security Policy.

5.5 Email Records

- Corporate email accounts are company property. Emails that constitute Records under this policy (i.e., emails that document a transaction, obligation, decision, or regulatory event) must be saved to the ERMS or to the designated approved folder within 10 business days of the email's significance being recognized;
- Auto-archiving shall be configured to archive all corporate email to a compliance archive after 90 days. The compliance archive shall be integrated

with Litigation Hold functionality such that holds can be applied at the mailbox or keyword level;

- Emails that are non-records (purely personal, transient, or duplicative of records already filed) may be deleted in accordance with ordinary email hygiene practices, provided no Litigation Hold is in effect affecting the mailbox;
- Employees are prohibited from using personal email accounts for company business. Any business records inadvertently created in a personal email account must be forwarded to the employee's corporate email and filed per this policy within 5 business days.

6. Physical Records Management

6.1 On-Site Storage

- Active physical records shall be maintained in designated filing areas within each department. Filing must use a consistent, labeled system that enables prompt retrieval;
- Confidential Records (personnel files, drug test results, medical records, litigation files, financial records) must be stored in locked, access-controlled cabinets or rooms. Keys and access codes shall be managed by the designated record custodian and their designated backup;
- On-site storage areas must maintain environmental controls sufficient to prevent physical deterioration of records: temperature shall be maintained between 65°F and 75°F; relative humidity between 30% and 50%; fire suppression systems must be present and tested annually;
- Records must not be stored on floors, near windows, or in areas subject to water infiltration or pest infestation. Non-compliance must be reported to Facilities Management within 24 hours of discovery.

6.2 Off-Site Storage

- Inactive physical records that have not yet reached their retention period end date shall be transferred to a company-approved off-site records storage vendor. The approved vendor list is maintained by the Director of Compliance and Legal Affairs;
- Transfer of records to off-site storage requires completion of a Chain of Custody Transfer Form documenting: record type, date range covered, quantity (boxes and estimated document count), date of transfer, and signature of the transferring custodian and receiving vendor representative;
- The off-site storage vendor must provide a Service Level Agreement (SLA) guaranteeing record retrieval within 24 hours for standard requests and 4 hours for litigation hold or regulatory inspection requests;
- The company shall maintain an inventory of all records in off-site storage, cross-referenced to retention schedule end dates, updated no less than quarterly.

6.3 Labeling and Indexing

- Every physical storage box or binder containing company records must be labeled with: Department name; Record category (per Section 4 categories); Date range of records contained; Retention period end date (earliest date eligible for destruction); Custodian name and contact; Box or binder sequential number;
- A master physical records index shall be maintained by each department and submitted to Compliance on a semi-annual basis;
- Labels must be legible, affixed securely, and replaced immediately if damaged or illegible.

6.4 Physical Records Access Controls

- A sign-out log must be maintained for all confidential physical records removed from their designated storage location. The log shall capture: date of removal; name and department of person removing the record; purpose of access; date of return;

- Personnel and financial records may only be accessed by: the record custodian; the employee to whom the record pertains (subject to applicable law); the Director of Compliance and Legal Affairs; the COO; and authorized external auditors or regulators in the course of an authorized proceeding;
- No physical record shall leave company premises (or approved off-site storage) without written authorization from the Director of Compliance and Legal Affairs, except in response to a valid legal subpoena or regulatory demand.

7. Litigation Hold Procedure

> ⚠️ **Critical Legal Obligation**
>
> Failure to implement a litigation hold upon the triggering of a legal hold obligation — and any resulting destruction or loss of relevant records — may constitute spoliation of evidence under FRCP Rule 37(e) and applicable case law. Sanctions for spoliation may include adverse inference instructions, monetary penalties, dismissal of claims or defenses, and referral for disciplinary action. This section must be strictly followed without exception.

7.1 Trigger Events

A litigation hold obligation is triggered upon any of the following events, each of which requires immediate notification to the Director of Compliance and Legal Affairs:

- Receipt of a lawsuit, complaint, or service of process naming the company as a party;
- Receipt of a written demand letter asserting a claim against the company;

- Receipt of a notice of government investigation, audit, or enforcement action;
- Receipt of a subpoena for documents, testimony, or electronically stored information;
- Reasonable anticipation of litigation — i.e., any circumstance in which a reasonable person would conclude that litigation is probable, including but not limited to: serious accidents involving company vehicles or personnel; cargo claims exceeding $25,000; employee grievances involving protected class allegations; OSHA fatality or serious injury investigations.

7.2 Legal Hold Notice

- Upon identification of a trigger event, the Director of Compliance and Legal Affairs shall issue a written Legal Hold Notice within 48 hours;
- The Legal Hold Notice shall specify: the nature of the matter triggering the hold; the categories of records subject to the hold (by record type, date range, department, and custodian); the scope of electronically stored information (ESI) subject to preservation; and instructions for immediate suspension of destruction;
- The Legal Hold Notice shall be distributed to all identified record custodians, department heads, and IT personnel with records potentially within scope. A template Legal Hold Notice is set forth in Appendix B.

7.3 Suspension of Destruction

- Upon receipt of a Legal Hold Notice, all scheduled destruction of in-scope records — both physical and electronic — shall be immediately and completely suspended;
- IT shall implement a technical hold on any automated deletion, overwrite, or purge functions (including email auto-deletion, ERMS purge rules, and ELD device overwrite) affecting in-scope records within 24 hours of the Legal Hold Notice being issued;
- Records subject to a hold that have already been transferred to off-site storage or the approved destruction vendor shall be recalled immediately.

7.4 Custodian Acknowledgment

Each custodian named in a Legal Hold Notice must return a signed written acknowledgment to the Director of Compliance and Legal Affairs within 72 hours of receipt, confirming: receipt of the notice; understanding of the scope of the hold; confirmation that scheduled destruction has been suspended; and identification of any records within scope that may be at risk.

7.5 Hold Maintenance

- The Director of Compliance and Legal Affairs shall issue quarterly reminders to all active hold custodians reiterating their obligations;
- The Legal Hold Notice shall be updated and reissued if the scope of the hold expands (e.g., additional record categories or custodians identified) or the nature of the proceedings changes materially;
- A litigation hold register shall be maintained by the Director of Compliance and Legal Affairs tracking: matter name; date hold issued; custodians notified; records in scope; date of each quarterly reminder; date hold released.

7.6 Hold Release

- A hold is released only upon written authorization from the Director of Compliance and Legal Affairs, issued after confirmed final resolution of the triggering matter (including exhaustion of all appeal periods);
- Upon issuance of a Hold Release Notice, the normal retention schedule shall resume for in-scope records. Records that have passed their retention period end date during the hold period shall be reviewed by the Director of Compliance and Legal Affairs before destruction is authorized;
- IT shall restore any suspended automated deletion or purge functions only after the Hold Release Notice has been confirmed in writing.

8. Records Destruction Procedure

8.1 Destruction Authorization

- No record shall be destroyed before its minimum retention period has expired under the schedule in Section 4;
- Before any destruction is executed, the responsible custodian must confirm in writing (via the Destruction Authorization Form, Appendix C) that: the retention period has been met; no active or pending Litigation Hold covers the records; and destruction is authorized by the Director of Compliance and Legal Affairs or designated deputy;
- Mass or batch destructions (e.g., annual purge of records whose retention periods have expired) must be pre-approved by the Director of Compliance and Legal Affairs and reported to the COO.

8.2 Destruction Methods by Record Type

Record Format	Approved Destruction Method	Minimum Standard	Certificate Required?
Paper / Physical Records (non-confidential)	Cross-cut shredding — in-house equipment	DIN 66399 Level P-3 minimum (shred particle ≤ 320 mm²)	No (destruction log entry sufficient)
Paper / Physical Records (confidential, PII, personnel, financial)	Cross-cut shredding (P-4 minimum) OR certified destruction vendor	DIN 66399 Level P-4 (shred particle ≤ 160 mm²)	Yes — Certificate of Destruction from vendor retained permanently
Electronic Records — Magnetic Media (HDD, tape)	DOD 5220.22-M wipe standard (3-pass overwrite) OR physical media destruction	NIST SP 800-88 Guidelines for Media Sanitization	Yes — IT-generated certificate of sanitization retained permanently
Electronic Records — Solid-State Media (SSD, USB, flash)	Cryptographic erasure + physical destruction (degaussing not effective for SSD)	NIST SP 800-88 Rev. 1	Yes — IT-generated certificate of destruction retained permanently
Electronic Records — Cloud / ERMS Hosted	Permanent deletion per vendor-certified secure deletion protocol; vendor certificate obtained	Vendor must certify NIST-compliant deletion; confirm no backup copies retained	Yes — Vendor certificate of deletion retained permanently

Record Format	Approved Destruction Method	Minimum Standard	Certificate Required?
ELD Device Records	ELD vendor-protocol secure wipe; device-level destruction for decommissioned units	FMCSA ELD technical specifications; NIST SP 800-88	Yes — IT log entry; vendor certificate for decommissioned devices

8.3 Destruction Log

A Destruction Log shall be maintained permanently and shall record for each destruction event:

- Date of destruction;
- Record type and description (per Section 4 category);
- Date range covered by the records destroyed;
- Quantity (number of boxes, files, or electronic records);
- Destruction method employed;
- Name and title of the authorizing officer;
- Name of individual or vendor executing destruction;
- Certificate of Destruction reference number (if applicable).

The Destruction Log and all Certificates of Destruction shall be retained **permanently** as evidence of compliance with retention and destruction obligations.

8.4 PII and Sensitive Data Destruction

- Records containing PII, medical information, drug and alcohol test results, Social Security numbers, or financial account information require enhanced destruction standards as set forth in Section 8.2 for confidential records;
- All third-party destruction vendors handling PII must execute a Business Associate Agreement or Data Processing Agreement (as applicable) with the company prior to handling any such records, and must provide proof of commercial general liability insurance and errors and omissions coverage;

- Improper destruction of PII (including destruction that renders PII accessible to unauthorized parties) may constitute a data security incident triggering breach notification obligations under applicable state and federal law. Any such occurrence must be reported to the Director of Compliance and Legal Affairs within 24 hours of discovery.

9. Special Categories of Records

9.1 Personally Identifiable Information (PII)

- All records containing PII shall be subject to heightened access controls as described in Sections 5.4 and 6.4, and shall be clearly marked "CONFIDENTIAL — PII" in both physical labeling and ERMS metadata;
- The Director of Compliance and Legal Affairs shall conduct an annual review of PII record categories to assess applicability of the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR) (where applicable to international data subjects), and any newly enacted state privacy laws in jurisdictions where the company operates;
- In the event of a breach, loss, or unauthorized disclosure of PII, the Director of Compliance and Legal Affairs shall be notified within 24 hours. Breach notification obligations under Ohio Rev. Code § 1347.12 and applicable federal law shall be evaluated and implemented as required.

9.2 Privileged Documents

- Communications between company personnel and legal counsel that are protected by the attorney-client privilege shall be marked "ATTORNEY-CLIENT PRIVILEGED — CONFIDENTIAL" and stored in a segregated, restricted-access folder within the ERMS accessible only to the Director of Compliance and Legal Affairs, outside counsel, and the COO;
- Work product prepared by or at the direction of legal counsel in anticipation of litigation shall be similarly marked and segregated;

- No privileged document shall be disclosed to any third party without prior written authorization from legal counsel. Accidental disclosure must be reported to the Director of Compliance and Legal Affairs immediately.

9.3 Trade Secrets and Proprietary Information

- Records constituting trade secrets or proprietary business information (including customer lists, pricing algorithms, operational route data, and proprietary technology) shall be marked "CONFIDENTIAL — PROPRIETARY" and subject to restricted access controls equivalent to those for privileged documents;
- Destruction of trade secret records shall be performed only by personnel authorized in writing by the COO or Director of Compliance and Legal Affairs, using confidential-grade destruction methods regardless of record format.

10. Roles and Responsibilities

Role / Department	Primary Responsibilities	Authority Level
Director of Compliance and Legal Affairs	Policy ownership and maintenance; issuance and management of litigation holds; approval of all record destructions; annual policy review; training oversight; regulatory change monitoring; audit coordination; breach response	Policy authority; litigation hold authority; destruction authorization authority
Chief Operating Officer (COO)	Policy approval; receipt of annual audit findings; approval of trade secret destructions; escalation point for non-compliance matters	Executive authority; policy approval
IT Department	ERMS administration and integrity; backup execution and verification; access control implementation; electronic hold implementation; electronic destruction execution; audit log maintenance; vendor management for technology platforms	Technical authority for electronic records systems
Department Heads (All	Ensuring staff awareness of	Operational authority within

Role / Department	Primary Responsibilities	Authority Level
Departments)	and compliance with this policy within their department; designating and supporting record custodians; reporting non-compliance; ensuring training completion within their teams	department
Record Custodians (Designated per Department)	Day-to-day management of assigned record categories per the retention schedule; filing and indexing; transferring inactive records to archive; executing authorized destructions; responding to litigation hold notices; maintaining destruction logs	Operational custodial authority for assigned record types
Human Resources Department	Primary custodian for all personnel, employment, I-9, payroll, workers' compensation, and benefits records; coordination with Safety for employee drug program records; training record maintenance	Custodial authority for HR record categories
Finance / Accounting Department	Primary custodian for financial statements, tax records, accounts receivable, invoices, factoring agreements, and payroll records (in coordination with HR); coordination with external auditors	Custodial authority for financial record categories
Safety Department	Primary custodian for driver qualification files, ELD and HOS records, vehicle inspection and maintenance records, accident records, OSHA logs, safety training records, and drug and alcohol testing records; coordination with DER	Custodial authority for safety and regulatory record categories
Operations Department	Primary custodian for bills of lading, PODs, rate confirmations, and dispatch records (in coordination with Billing/TMS); vehicle lease agreement coordination	Custodial authority for operational record categories

11. Training and Awareness

- **Mandatory Annual Training:** All employees, contractors, and agents subject to this policy shall complete records management training annually. Training shall cover: retention schedule overview; proper filing and storage procedures; litigation hold obligations; destruction authorization procedures; PII handling; and consequences of non-compliance;
- **New-Hire Training:** All new employees shall complete records management training within 30 days of their start date as part of the onboarding curriculum. Completion must be documented in the HRIS before the 30-day deadline;
- **Custodian-Specific Training:** Designated record custodians in high-volume or high-complexity departments (Safety, HR, Finance, Operations) shall complete enhanced custodian training covering the specific retention schedules, filing systems, and destruction procedures applicable to their record categories. This training shall be completed within 60 days of designation as a custodian and annually thereafter;
- **Litigation Hold Training:** All employees who may be designated as custodians in litigation hold notices shall receive targeted training on litigation hold obligations, ESI preservation, and the consequences of spoliation;
- **Training Records:** All training completion records shall be maintained per the HR training record retention schedule (duration of employment + 3 years). The HR Department shall maintain training completion reports and provide them to the Director of Compliance and Legal Affairs on a semi-annual basis.

12. Audit and Compliance Monitoring

- **Annual Compliance Audit:** The Director of Compliance and Legal Affairs shall conduct, or commission, an annual records management compliance audit covering all departments. The audit shall include: sample-based verification that records are being retained for required periods and in required formats; verification that expired records have been properly destroyed per the schedule; review of destruction logs and certificates; verification that litigation holds are properly implemented and documented; and review of training completion records;

- **Electronic Records Integrity Audit:** IT shall conduct an annual audit of ERMS integrity, including: hash verification of critical compliance records; backup restoration test; audit log review; access control review (confirming that no unauthorized access has occurred and that access permissions remain appropriate); and ERMS vendor compliance with contractual obligations;
- **Findings and Reporting:** Audit findings shall be compiled in a written Compliance Audit Report delivered to the COO within 45 days of audit completion. The report shall identify all deficiencies found, their risk severity rating (Critical, High, Medium, or Low), and recommended corrective actions;
- **Corrective Action Plans:** For each deficiency rated Critical or High, a Corrective Action Plan (CAP) specifying responsible party, remediation steps, and target completion date must be developed within 30 days of the audit report and submitted to the COO for approval. CAP completion shall be verified at the next annual audit.

13. Non-Compliance and Enforcement

13.1 Premature Destruction of Records

- Destruction of any record before its minimum retention period has expired — whether intentional, negligent, or inadvertent — constitutes a serious policy violation;
- Upon discovery of premature destruction, the Director of Compliance and Legal Affairs shall: immediately assess whether any regulatory notification obligation has been triggered; notify legal counsel and the COO; conduct a

root cause investigation; and implement corrective measures to prevent recurrence;

- Responsible personnel shall be subject to progressive discipline up to and including termination, depending on the severity, scope, and whether the destruction was intentional.

13.2 Failure to Implement a Litigation Hold

- Failure by any employee, custodian, or IT personnel to implement, maintain, or comply with a litigation hold directive — or failure to promptly report a trigger event that would require a hold — is a severe violation of this policy and of legal obligation;
- Such failure may expose the company to sanctions under FRCP Rule 37(e), including adverse inference instructions to a jury, monetary sanctions, or in egregious cases, dismissal of the company's claims or defenses;
- Responsible personnel shall be subject to disciplinary action up to and including immediate termination. In cases involving intentional destruction or concealment, referral for criminal prosecution may be appropriate.

13.3 Unauthorized Access or Disclosure

- Unauthorized access to, or disclosure of, confidential records — including personnel files, medical records, drug test results, PII, financial records, or litigation files — shall result in immediate investigation by the Director of Compliance and Legal Affairs;
- Depending on findings, disciplinary action up to and including termination shall be imposed. Where applicable law requires, breach notification to affected individuals and regulatory bodies shall be initiated;
- Unauthorized access to attorney-client privileged materials or trade secrets may result in additional legal action.

14. Policy Review and Amendment

- **Annual Review:** This policy shall be reviewed by the Director of Compliance and Legal Affairs no less than annually, with each review completed prior to the anniversary of the effective date;
- **Triggered Reviews:** In addition to the annual review, a review and potential amendment of this policy shall be triggered by any of the following: a material change in applicable federal or state law or regulation; the conclusion of significant litigation that reveals a gap or deficiency in company records management practices; a finding in the annual compliance audit rated Critical; or the introduction of a new records management technology platform or system;
- **Version Control:** All amendments shall be tracked with a version number increment and a notation of the changes made and the effective date. Prior versions shall be archived per this policy and retained for a minimum of 10 years;
- **Distribution:** Upon each approved revision, the Director of Compliance and Legal Affairs shall distribute the updated policy to all department heads and record custodians, post it to the company's internal policy repository, and notify all employees of the revision via company communication channels. Employees are responsible for reading and complying with the current version.

Appendix A: Master Retention Schedule — Quick Reference

This condensed table provides a rapid reference summary of the minimum retention periods by record category. For full details including storage location, custodian, and destruction method, refer to Section 4.

Record Category	Record Type	Minimum Retention	Authority
Driver & Qualification	DQ Files — Active Drivers	Employment + 3 yrs	49 CFR § 391.51

Record Category	Record Type	Minimum Retention	Authority
DQ Files — Terminated	3 yrs post-termination	49 CFR § 391.51	
Drug/Alcohol — Positive/Refusal	5 years	49 CFR § 382.401	
Drug/Alcohol — Negative	1 year	49 CFR § 382.401	
MVR/PSP Reports	3 yrs per annual pull	49 CFR § 391.51	
HOS / ELD	ELD Records — On Device	6 months	49 CFR § 395.22
ELD Records — Server Backup	6 months additional	49 CFR § 395.22	
HOS Violation Records	3 years	49 CFR § 395	
Supporting Documents	6 months	49 CFR § 395.8	
Vehicle / Maintenance	DVIR	3 months	49 CFR § 396.11
PM Records	Life of vehicle + 1 yr	49 CFR § 396.3	
Accident Reports	3 years	49 CFR § 390.15	
Vehicle Lease Agreements	Duration + 3 yrs	49 CFR § 376.12	
Cargo / Billing	Bills of Lading / POD	3 years	Carmack; IRS
Rate Confirmations	3 years	IRS	
Cargo Claims Files	5 yrs or resolution + 3 yrs	49 U.S.C. § 14706	
Invoices / AR Records	7 years	IRS	
Factoring Agreements	Duration + 5 yrs	UCC; IRS	
Financial / Corporate	General Ledger / Financial Statements	7 years	IRS; SOX
Tax Returns	7 years	IRC § 6501	
Payroll Records	7 years	IRS; FLSA	
Corporate Governance Records	**Permanent**	State corporate law	
Insurance Policies	Duration + 10 yrs	State insurance codes	
Safety / Compliance	OSHA 300 Logs	5 years	29 CFR § 1904.33
Safety Training Records	3 yrs or employment + 3 yrs	OSHA; DOT	
FMCSA Compliance Review Records	5 years	49 CFR § 385	

Record Category	Record Type	Minimum Retention	Authority
Personnel / HR	Employment Applications — Hired	Employment + 3 yrs	EEOC; 29 CFR § 1602
Employment Applications — Not Hired	1 year	29 CFR § 1602.14	
I-9 Forms	3 yrs post-hire or 1 yr post-term	INA § 274A	
Disciplinary Records	Employment + 3 yrs	EEOC; state law	
Workers' Comp Records	5 yrs post-closure	Ohio Rev. Code § 4123	

Appendix B: Litigation Hold Notice Template

📄 Template — Litigation Hold Notice

PRIVILEGED AND CONFIDENTIAL — ATTORNEY-CLIENT COMMUNICATION

LITIGATION HOLD NOTICE

To: [Custodian Name(s) / Department(s)]
From: Director of Compliance and Legal Affairs
Date: [Date of Issuance]
Re: Litigation Hold — [Matter Name / Reference Number]

Effective immediately, this notice places a litigation hold on the records described below in connection with [brief description of matter — e.g., "the accident occurring on [date] involving unit [number]" or "the employment dispute of [employee name]"]. You must preserve all records within scope without alteration or deletion pending further notice.

Records in Scope: [Record types, date ranges, systems, custodians]

Your Obligations:
1. Immediately suspend any scheduled destruction of in-scope records.
2. Preserve all in-scope records in their current state.
3. Notify IT immediately of any automated deletion systems affecting in-scope records.

4. Return the signed Custodian Acknowledgment below within 72 hours.
5. Notify [Director of Compliance] immediately if you become aware of any in-scope records that have already been destroyed or are at risk.

Questions should be directed to the Director of Compliance and Legal Affairs at [contact information].

CUSTODIAN ACKNOWLEDGMENT:
I acknowledge receipt of this Litigation Hold Notice and confirm that I understand my obligations. I have suspended all scheduled destruction of in-scope records.

Signature: ___________________________ Date: ___________
Printed Name: _______________________ Title: ___________

Appendix C: Destruction Authorization Form

📄 **Template — Destruction Authorization Form**

RECORD DESTRUCTION AUTHORIZATION
Policy Reference: BOF-POL-007 | Form Version: 2.0

Field	Entry
Record Category / Type	
Date Range of Records	
Quantity (boxes / files / records)	
Storage Location Prior to Destruction	
Retention Period End Date	

Date of Proposed Destruction

Destruction Method

Destruction Vendor (if applicable)

Litigation Hold Check (Y/N — if Y, do not proceed)

Custodian Name and Signature

Authorizing Officer Name and Signature

Date of Authorization

Certificate of Destruction Reference # (post-destruction)

This form must be completed and signed before any destruction is executed. Retain this form permanently in the Destruction Log.

Appendix D: Records Custodian Responsibility Matrix

Record Category	Primary Custodian	Secondary Custodian	Oversight Authority
Driver Qualification Files	Safety Director	Safety Coordinator	Director of Compliance
Drug and Alcohol Testing Records	Designated Employer Representative (DER)	Safety Director	Director of Compliance
ELD / HOS Records	Safety Department	IT Department	Director of Compliance
Vehicle / Maintenance Records	Maintenance Manager	Safety Coordinator	Safety Director
Bills of Lading / Cargo Records	Operations Manager	Billing Coordinator	COO
Cargo Claims Files	Director of Compliance	Operations Manager	COO
Financial Records	CFO / Controller	Accounting Staff	COO
Corporate Governance Records	Director of Compliance / Corporate Secretary	CFO	COO

Record Category	Primary Custodian	Secondary Custodian	Oversight Authority
Personnel / HR Records	HR Director	HR Coordinator	Director of Compliance
Safety / OSHA Records	Safety Director	Safety Coordinator	Director of Compliance
ERMS / Electronic Systems	IT Director	Systems Administrator	Director of Compliance
Litigation Files / Privileged Documents	Director of Compliance	Outside Counsel	COO

Appendix E: Electronic Records Naming Convention Guide

All electronic records stored in the ERMS must follow the naming convention below. This guide establishes approved abbreviations and formatting requirements.

Format: [DEPT]_[RecordType]_[YYYY-MM-DD]_[SubjectID]_[Version]

Element	Description	Examples
[DEPT]	Abbreviated department code	SAFETY, HR, FIN, OPS, LEGAL, IT, MAINT
[RecordType]	Abbreviated record type (see table below)	DQF, BOL, POD, I9, DVIR, OSHA300, PAYROLL
[YYYY-MM-DD]	Date of record creation or event date (ISO 8601 format)	2026-07-16
[SubjectID]	Employee ID, Load ID, Vehicle Unit #, or other unique identifier	DRV-00147, LD-20260716-004, VEH-0022
[Version]	Version number (v1 for original; increment for amendments)	v1, v2, v3

Record Type Code	Full Record Name	Section Reference
DQF	Driver Qualification File	4.1
DATEST	Drug and Alcohol Test Record	4.1
MVR	Motor Vehicle Record	4.1
MEDCERT	Medical Examiner Certificate	4.1
ELDLOG	ELD Data Log	4.2

Record Type Code	Full Record Name	Section Reference
HOSLOG	Hours of Service Log	4.2
DVIR	Driver Vehicle Inspection Report	4.3
PMREC	Preventive Maintenance Record	4.3
ACCID	Accident / Incident Report	4.3
BOL	Bill of Lading	4.4
POD	Proof of Delivery	4.4
RATECON	Rate Confirmation	4.4
CLAIM	Cargo Claim File	4.4
INV	Invoice / Accounts Receivable	4.4
FINST	Financial Statement	4.5
TAX	Tax Return	4.5
PAYROLL	Payroll Record	4.5
CONTRACT	Contract / Agreement	4.5
OSHA300	OSHA 300 Log	4.6
SAFETRAIN	Safety Training Record	4.6
I9	Form I-9	4.7
PERFILE	Personnel File Document	4.7
WCOMP	Workers' Compensation Record	4.7
LITHOLD	Litigation Hold Notice / Release	7
DESTAUTH	Destruction Authorization Form	8

Policy Approval and Certification

The undersigned certify that this policy has been reviewed, approved, and is effective as of the date indicated in the metadata block on page 1. This policy supersedes all prior versions of BOF-POL-007 and all predecessor document retention policies.

Role	Name	Signature	Date
Director of Compliance and Legal			July 16, 2026

Role	Name	Signature	Date
Affairs (Policy Owner)			
Chief Operating Officer (Approving Authority)			July 16, 2026
