

Document Retention Periods

Document Type	Retention Period
Accident reports/claims (settled cases)	7 years
Accounts payable ledgers & schedules	7 years
Accounts receivable ledgers & schedules	8 years
Audit reports	Permanently
Bank statements	3 years
Capital stock & bond records	Permanently
Cash books	Permanently
Charts of accounts	Permanently
Checks (canceled - important payments, contracts, assets, taxes, etc.)	Permanently
Checks (canceled - general)	7 years
Contracts & leases (expired)	7 years
Correspondence (general)	2 years
Correspondence (legal and tax-related)	Permanently
Deeds, mortgages & bills of sale	Permanently
Deposit slips	3 years
Depreciation schedules	Permanently
Employee personnel records (after termination)	7 years
Employee applications	5 years
Expense reports	7 years
Financial statements (year-end)	Permanently
Fixed asset records (invoices, canceled checks, depreciation schedules)	Permanently
Forms 1099 Received	7 years

Document Type	Retention Period
General ledgers, year-end trial balance	Permanently
Insurance policies (expired)	3 years
Insurance records (accident reports, claims, policies, etc.)	Permanently
Internal audit reports (miscellaneous)	3 years
Inventory records	7 years
Invoices (to customers or from vendors)	7 years
IRA/Keogh plan contributions, rollovers, transfers & distributions	Permanently
Minute books of directors, stockholders, bylaws & charter	Permanently
Payroll records, summaries & tax returns	7 years
Petty cash vouchers	3 years
Purchase orders	3 years
Receiving sheets	1 year
Retirement plan records	Permanently
Safety records	6 years
Sales records	7 years
Subsidiary ledgers	7 years
Tax returns, revenue agents' reports & related documents	Permanently
Time cards and daily reports	7 years
Trademark registration, patents & copyrights	Permanently
Trial balances (monthly)	3 years
W-2 Forms	7 years

Guidelines for Digital Record Retention

- Electronic storage is allowed if documents are scanned and stored securely according to IRS and industry rules.
- Use encrypted cloud storage or secured on-premises servers to prevent unauthorized access.
- Implement automatic backups and version control for critical financial and legal documents.
- Ensure audit trails are maintained for document modifications and access history.
- For disaster recovery, backup permanent digital documents in multiple locations.

This document provides general guidelines for record retention. Retention requirements vary by state, industry, and regulatory authority. Businesses should consult their legal and financial advisors to ensure compliance with applicable laws and regulations before destroying any records. For specific inquiries, contact an LBMC professional for guidance.

