Data Retention & Disposal Policy

PHOCIS Tech's data retention policy defines retention periods for all data categories, aligned with regulatory requirements under RESPA, FCRA, GLBA, and applicable state mortgage regulations. This policy ensures data is retained only as long as necessary and disposed of securely.

Retention Schedule by Data Category

Data Category	Retention Period	Regulatory Basis
Loan Application Records	7 years from closing/denial	RESPA / ECOA
Borrower PII (SSN, DOB, etc.)	7 years post-loan closure	GLBA / State
Credit Reports & Scores	25 months from access date	FCRA § 1681e
Servicing & Payment Records	7 years from final payment	RESPA / State
BSA / AML Transaction Logs	5 years from transaction	BSA 31 U.S.C. § 5318
Email Communications (Business)	3 years standard, 7 years loan-related	Internal Policy
Audit & Access Logs	12 months active, 7 years archived	SOC 2 / GLBA
Investor & Capital Records	7 years from fund close	SEC / State Blue Sky
Employee Records	7 years post-separation	IRS / EEOC
Marketing & Analytics Data	2 years from collection	CCPA / Internal

Data Disposal Standards

- Digital data: cryptographic erasure (key destruction) for encrypted stores; DoD 5220.22-M multi-pass overwrite for unencrypted media
- Physical media: NIST 800-88 compliant degaussing and shredding via certified destruction vendor
- Cloud data: verified deletion API calls with deletion confirmation receipts retained for 3 years
- Backup data: included in retention schedule; encrypted backups deleted per schedule with confirmation
- Third-party data: deletion confirmed in writing from all vendors within 30 days of retention expiry

Legal Hold Process

When litigation or regulatory inquiry is anticipated, a legal hold is issued by the General Counsel that suspends automated deletion for affected data categories. Legal holds are tracked in the Legal Hold Register and reviewed quarterly until lifted.

Audit & Compliance

- Automated deletion workflows run monthly; exceptions require CISO + Legal sign-off

- Annual audit of retention compliance conducted by internal security team
- Any unauthorized retention or premature deletion constitutes a policy violation