ITAD Compliance for Banks and Credit Unions
The examiner-ready one-pager

promo.ccrcyber.com/articles/itad-compliance-banks-credit-unions

The disposal duty is already inside your information security program. This page is what to have in the file when the examiner asks how the old equipment left.

01 · WHERE THE DUTY LIVES

Two documents, one obligation

- Banks: Interagency Guidelines Establishing Information Security Standards (OCC 12 CFR Part 30 App. B and the Fed/FDIC parallels) — the program must include measures to properly dispose of customer information and consumer information (FACTA disposal, incorporated 2004).
- Credit unions: NCUA Guidelines for Safeguarding Member Information, 12 CFR Part 748 App. A — same disposal objective. NCUA proposed (Dec 2025) to republish as a Letter to Credit Unions with no substantive change; confirm status.
- Technical benchmark: NIST SP 800-88 Rev. 2 (Clear / Purge / Destroy). Neither guideline names a technique; this is the one examiners and auditors recognize.

02 · THE VENDOR FILE

Your ITAD provider is a service provider

- Due diligence, dated before the first pickup: NAID AAA verified in i-SIGMA's directory; R2v3 with Appendix B verified in SERI's directory; certificate of insurance; references.
- Contract terms: named standard (NIST 800-88 Rev. 2); serialized certificate per device; chain of custody; notification if anything goes missing; subcontractor disclosure; audit/inspection rights.
- Monitoring: reconcile certificates to the asset list after every event; annual re-check of certifications and insurance; a line in the annual board report (both Guidelines require it to cover service-provider arrangements). Banks: map to the 2023 Interagency Third-Party Risk Management life cycle.

03 · THE INVENTORY

Device classes that hold customer or member data

Device class	Where the data hides	Path
ATMs / ITMs	HDD or SSD: journals, card data, images	Drive destroyed on site before cabinet moves; certificate
Check scanners / capture stations	Check images, buffers	Sanitize or destroy; certificate
Copiers / MFPs	Internal drive: scanned loan files, IDs, statements	Drive destroyed before lease return
Phones, tablets, desk phones	Email, messaging, auth tokens, call logs	Verified wipe or destroy (soldered storage)
Card readers, signature pads, POS	Transaction / config data	Treat as data-bearing until proven otherwise
Network gear, DVRs	Configs, VPN keys, credentials, branch footage	Config wipe or destroy; certificate
Backup tapes / removable media	Everything, forever	Degauss or destroy; serialized record

04 · THE CLOCK

Why a lost device is a same-week question

Banks: computer-security incident notification to the primary federal regulator no later than 36 hours after determining a notification incident occurred (rule in effect since 2022). Credit unions: NCUA reportable cyber incident within 72 hours (since Sept 1, 2023). State breach laws stack on top — Maryland notifies the AG before individuals; New Jersey notifies the State Police before customers. Whether a specific device is an incident is counsel's call; a device with a serialized certificate never enters the analysis.

05 · THE RECORDS

Keep these on the institution's records schedule

Asset inventory reconciled at pickup and at destruction · serialized certificates naming method and standard · chain-of-custody documentation to final disposition · vendor certifications, insurance, due-diligence memo, and contract (dated) · the board-report entry covering the service-provider arrangement, the year's events, and exceptions.

Sources: Interagency Guidelines Establishing Information Security Standards; 12 CFR Part 748 App. A and NCUA's Dec 2025 proposal (Federal Register); Interagency Guidance on Third-Party Relationships: Risk Management (June 2023); banking agencies' Computer-Security Incident Notification Rule; NCUA cyber incident reporting rule (12 CFR 748.1(c)); NIST SP 800-88 Rev. 2. Informational only — not legal, regulatory, or examination advice. Full brief: promo.ccrcyber.com/articles/itad-compliance-banks-credit-unions