

The Small Business ITAD One-Pager

A compliant program without a department

promo.ccr cyber.com/articles/small-business-itad-guide

The rules do not scale down with headcount. The program can. Five habits, one folder, four documents.

01 · WHAT APPLIES AT ANY SIZE

The laws with no headcount floor

- FTC Disposal Rule (16 CFR 682): any business holding consumer report information (tenant screening, background checks) — reasonable disposal measures; electronic media in scope.
- State destruction statutes: NJ (N.J.S.A. 56:8-162 — shred, erase, or make unreadable); DE (6 Del. C. Ch. 50C — reasonable steps; private right of action); MD (Com. Law §14-3502 — reasonable steps for customer and employee records). PA relies on its breach law and federal rules.
- Breach notification: all 50 states. A lost or unsanitized drive can be the breach.
- Disposal bans: PA (free programs only under 50 employees; ban applies to all); NJ (ban applies to all). DE/MD: federal RCRA still applies.
- Sector overlays: HIPAA for a solo practice; FTC Safeguards Rule for small lenders, brokers, tax preparers, dealers extending credit; PCI DSS for card terminals.

02 · THE FIVE-STEP PROGRAM

Everything the law asks, at small-business scale

- 1. Inventory every device with storage — a spreadsheet with serial numbers is enough.
- 2. Decide the path at retirement: redeploy · sanitize and remarket · destroy. Never "later."
- 3. Destroy data to NIST SP 800-88 Rev. 2 through a certified provider; deleting, formatting, or a factory reset is not destruction.
- 4. Use a certified vendor — sealed, tracked mail-back kit for a few devices; scheduled pickup for a refresh or move.
- 5. Keep the paperwork with insurance and tax records for your retention period.

03 · WHAT HOLDS DATA IN A SMALL OFFICE

Put all of these on the inventory

Laptops and desktops (modern SSDs need device-level sanitization, not overwriting) · servers · phones and tablets, including personal devices with company email · the copier / multifunction printer (its internal drive) · external and backup drives, USB sticks · point-of-sale terminals and card readers · the firewall and Wi-Fi access points · desk phones and the camera DVR. When the copier lease ends, the copier is a data-bearing device leaving the building.

04 · FOUR DOCUMENTS, ONE CHECK

What to demand from any vendor

Document	What it must show
Certificate of sanitization / destruction	Each device by serial number; method; standard (NIST SP 800-88 Rev. 2). No serials = a receipt, not a certificate.
Chain-of-custody record	Who took possession, when, how many, where it went.
Proof of certification — verified by you	NAID AAA in i-SIGMA's directory; R2v3 in SERI's directory. Five minutes.
Certificate of insurance	A policy behind the vendor, not just an apology.

05 · TWO QUESTIONS

Ask before the first pickup

Will anyone else take custody of our equipment? (Then that party needs the same verification.) What happens to a device that fails sanitization? (Physical destruction, recorded by serial.) And remember the upside: recent, properly sanitized equipment has resale value that can offset the program — while a closet full of retired hardware loses value every month it sits.

Sources: 16 CFR Part 682; N.J.S.A. 56:8-162; 6 Del. C. Ch. 50C; Md. Code, Com. Law §14-3502; Pennsylvania Covered Device Recycling Act; New Jersey Electronic Waste Management Act; HIPAA; FTC Safeguards Rule; NIST SP 800-88 Rev. 2. Informational only — not legal or compliance advice; no pricing stated or implied. Full guide: promo.ccr cyber.com/articles/small-business-itad-guide