ITAD Verification Framework

Purpose

A practical, enforceable approach to IT Asset Disposition (ITAD) that ensures SOC 2 and ISO 27001 compliance, protects against data breaches, and creates a provable chain of custody.

The Three Core Controls

1. **Verification Tag Tracking**
   - Apply a unique barcode tag to every device at the start of disposition.
   - Enables **two-key tracking** (combining barcode tags with another identifier) for far greater than serial number matching alone.
   - Deters theft and ensures traceability from start to finish.
2. **No Sharing of Serialized Inventory with Downstream Vendors**
   - Vendors do not receive serialized inventory to prevent "answer key" manipulation.
   - Ensures discrepancies are visible, auditable, and cannot be concealed.
3. **Equipment Verification Holds**
   - Upon receipt, the ITAD vendor places the equipment in a secure hold.
   - No resale or destruction until independent verification confirms **chain of custody**.
   - 99% of inventory discrepancies can be resolved with a second look.

ISO 27001 Alignment

Segregation of Duties (Control 5.3): Assign ITAD to a dedicated team or vetted third-party provider. Separate from internal IT asset management to avoid conflicts of interest.

Independent Verification (Annex A 5.35, Clause 9.2): Use an internal audit team or an independent third party to reconcile inventories. Never rely solely on vendor self-reports.

SOC 2 Alignment

Logical and Physical Access Controls (CC6.5): Systematic and validated tracking of hardware satisfies the mandate for traceability, evidence, and risk neutralization.

Monitoring Activities and Control Validation (General Criteria and CC6 series): Continuous evaluations of control performance to detect deficiencies and take corrective action.

Incident Response & Detection (CC7.2, CC7.3): Timely detection, documented investigation, and corrective actions for clearly defined incidents.

HIPAA Alignment

Security Incident Procedures (45 CFR 164.308(a)(6)(i)): Ensure prompt identification, response, and documentation of actual or suspected incidents, as required by the HIPAA Security Rule.

Breach Notification for Business Associates (45 CFR 164.410(a)(1)): Business Associates must notify covered entities without unreasonable delay (and within 60 days).

Business Associate Agreements (45 CFR 164.314(a)(2)(i)(C)): Comply with BAAs by reporting security incidents and maintaining transparency.

SEC Alignment

Cybersecurity Risk Management (17 CFR 229.106(b)): Companies must maintain processes for assessing, identifying, and managing risks.

Material Incident Disclosure (17 CFR 229.106(c)): Companies must disclose material incidents within four business days.

Why It Matters

- **Regulatory Defense**: Demonstrates adherence to SOC 2, ISO 27001, HIPAA, and SEC expectations.
- **Risk Reduction**: Prevents theft, fraud, and data loss during ITAD.
- **Transparency**: Creates a provable, verifiable chain of custody.
