SECURE ITAD CHECKLIST

for Cyber Security Threats

Improper disposition of IT assets is one of the most overlooked cyber security risks. From routers and firewalls to hard drives and switches, end-of-life devices can retain sensitive data that, if mishandled, may lead to costly breaches. At SK tes, we believe cyber security doesn't end when devices are unplugged. Use this checklist to ensure your IT asset disposition (ITAD) process is secure, compliant, and trustworthy.

1. CHAIN OF CUSTODY AND ASSET TRACKING

Is there a complete, auditable chain of custody for all IT assets?

- [ ] Ensure your ITAD provider maintains an end-to-end, documented chain of custody from collection to final disposition.
- [ ] Every asset or load should be tracked and reconciled at pickup and delivery.
- [ ] A secure, online platform should provide real-time visibility and audit trails.
- [ ] Look for GPS-tracked transportation and real-time logging to prevent loss or tampering.

2. INVENTORY MANAGEMENT AND CERTIFICATION

Do you receive detailed inventories and proof of service?

- [ ] All assets should be logged with serial numbers, make, model, and condition.
- [ ] Inventory should be reconciled against collection records.
- [ ] Certificates of data destruction and recycling should be issued for compliance and audit purposes.
- [ ] Look for GPS-tracked transportation and real-time logging to prevent loss or tampering.

3. DATA DESTRUCTION AND COMPLIANCE

Is data destroyed to recognized standards?

- [ ] Confirm that data-bearing devices are sanitized or destroyed using methods compliant with NIST 800-88 or IEEE 2883-2022
- [ ] Physical destruction (e.g., shredding) should be available for high-security needs.
- [ ] Ensure that data destruction is fully verified.

4. CERTIFICATIONS AND INDUSTRY STANDARDS

Is your ITAD provider certified to recognized global standards?

Look for certifications that demonstrate commitment to quality, security, and environmental responsibility:

- [ ] R2v3 – Responsible Recycling standard for ITAD and e waste management
- [ ] ISO 9001 – Quality Management System
- [ ] ISO 14001 – Environmental Management System
- [ ] ISO 45001 – Health and Safety Management System
- [ ] ISO 27001 – Information Security Management System

5. FACILITY AND ITAD PROCESS SECURITY?

Are physical and procedural safeguards in place?

Facilities should have:

- [ ] 24/7 CCTV surveillance
- [ ] Controlled badge access
- [ ] Segregated zones for receiving, processing, and shipping
- [ ] On-site security personnel

- [ ] Ensure secure transportation with GPS tracking and tamper-evident containers.
- [ ] Ask about incident response protocols in case of a breach or loss.

6. PERSONNEL AND PROCESS INTEGRITY

Are roles clearly defined and staff properly vetted?

- [ ] Ensure Separation of Duties: No single employee should control the entire process (e.g., collection, processing, certification).
- [ ] All staff handling sensitive data must undergo background checks and appropriate security clearances.
- [ ] Ask about training programs and ongoing compliance education for ITAD personnel.

7. TRANSPARENCY AND AUDITABILITY

Can you inspect or audit the ITAD process?

- [ ] Reputable ITAD providers should welcome site visits or offer virtual tours.
- [ ] Transparency builds trust, look for providers who proactively share process documentation and compliance reports.
- [ ] Ask for sample audit logs or past audit results.

8. FACILITY AND ITAD PROCESS SECURITY?

Is your ITAD process compliant?

- [ ] Ensure compliance with local, national, and international regulations
- [ ] Confirm that e waste is recycled or disposed of responsibly, with minimal environmental impact.
- [ ] Request downstream vendor audits and environmental impact reports.

Data breaches from improperly retired IT assets are real and costly, from medical records found at flea markets to firewalls leaking credentials. Factory resets aren't enough. Verified data destruction and airtight tracking are non-negotiable. At SK tes, we offer secure, certified ITAD solutions that protect your data, reputation, and compliance.

Download this checklist and share it with your IT, compliance, and procurement teams.