Arkiva Secure IT Disposal Checklist

Protect your organisation's data

Retired laptops, servers, and storage devices can quietly retain sensitive information. Improper disposal can expose your company to costly data breaches and PDPA violations. Use this checklist to ensure your end-of-life IT assets are handled securely, responsibly, and in compliance.

1. Maintain a Documented Chain of Custody

Every asset should be traceable from pickup to final destruction.

- [ ] Use tamper-evident containers and GPS-tracked transport
- [ ] Record pickup and delivery timestamps
- [ ] Keep signed collection and delivery logs

Tip: Ask your vendor for real-time tracking and audit trail access.

2. Record a Verified Asset Inventory

Track each item with make, model, and serial number.

- [ ] Reconcile inventory after collection
- [ ] Retain digital records for audits
- [ ] Store copies of certificates and reports

Tip: Serial-number-based tracking ensures every item is accounted for.

3. Ensure Certified Data Destruction

All data-bearing devices must be sanitised or destroyed according to standards.

- [ ] Acceptable methods: NIST 800-88, IEEE 2883-2022, or physical shredding
- [ ] Request certificates for data erasure or media destruction

Tip: Always verify destruction with before-and-after documentation.

4. Verify Compliance with PDPA & Global Standards

Confirm your ITAD partner complies with recognised frameworks.

- [ ] BizSAFE3 (Work Safety)
- [ ] ISO 9001 (Quality Management System)
- [ ] ISO 14001 (Environmental Management)
- [ ] NEA Waste Collectors' License
- [ ] NEA Waste Facility License (E-Waste)

Tip: Certifications demonstrate operational discipline and data accountability.

5. Assess Facility Security & Staff Controls

A secure ITAD facility should include:

- ☐ 24/7 CCTV and controlled access zones
- ☐ Restricted data processing areas
- ☐ Background-checked staff

Tip: Separation of duties prevents internal misuse or mishandling.

6. Review Environmental & Recycling Practices

Responsible ITAD goes beyond data destruction.

- ☐ Ensure licensed downstream recyclers handle materials
- ☐ Request recycling and recovery reports
- ☐ Avoid vendors using informal or illegal offshore channels

Tip: Ethical recycling safeguards both compliance and brand reputation.

7. Confirm Transparency & Auditability

A trustworthy ITAD partner welcomes oversight.

- ☐ Request process documentation or site visits
- ☐ Review audit logs or service photos
- ☐ Ensure incident-response protocols are in place

Tip: Transparency builds long-term trust and accountability.

8. Train Your Internal Teams

Even the best processes fail without awareness.

- ☐ Train staff on IT asset handling procedures
- ☐ Maintain an internal IT disposal policy
- ☐ Assign responsibility for approval and verification

Tip: Regular training reduces errors and compliance risks.

Verified data destruction and full compliance are non-negotiable.

*At **Arkiva**, we provide **secure, certified IT Asset Disposal solution**s that protect your data, ensure PDPA compliance, and uphold your organisation's reputation.*

***Download this checklist** and share it with your **IT, compliance, and procurement teams** to strengthen your data security from start to finish.*

Contact our team: sales@arkiva.com.sg