

IT disposal audit evidence checklist

Use this to check your evidence pack before an auditor does. Each document should trace back to the same serial numbers.

	Document	What it proves	Who produces it	When
☐	Disposal policy	Who approves disposal; which method for which media; onsite rules	You	Reviewed yearly
☐	Retirement approval	Assets approved for disposal by their owner	You	Before collection
☐	Serial-level handover	Exactly which devices and drives left, signed by both sides	You and vendor	At collection
☐	Chain of custody log	Who held the devices at every step	Vendor, with your inputs	During the job
☐	Erase reports	Per-drive wipe result, method and verification	Erase software, via vendor	After processing
☐	Destruction log	Per-serial shredding or degaussing	Vendor	After processing
☐	Certificate of Destruction	Method and date for every serial, signed	Vendor	After processing
☐	E-waste manifest and recycling certificate	Hardware moved to and was recycled by an authorised recycler	Vendor and recycler	At collection and after
☐	Reconciliation note	Register and certificates match; exceptions explained	You	When certificates arrive
☐	Vendor due diligence file	Vendor certifications, registrations, agreement, right to audit	You	Before first job; yearly

Five checks an auditor will run

1. Pick 5 to 10 retired assets and trace each to a certificate line with the same serial.
2. Check the method suits the media. Degaussing does nothing to SSDs; a single overwrite on an SSD is weak.
3. Check the dates: collection, then destruction, then any resale.
4. Check the vendor's registrations and certifications were valid on the job date.
5. Ask what happened to anything that did not reconcile.

Guide: privace.in/guides/prove-data-destruction-for-audit/ . General guidance, not legal advice. Your compliance team should map the obligations that apply to you.