Below is Section 4.10 of the Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements, Version 2.0 (December 2016) in italic. Then read how in the green comment section how TechR2® complies and exceeds with the PCI standard.

4 Production Procedures and Audit Trails[1]

4.10 Destruction and Audit Procedures

a) All waste components must be counted before being destroyed in-house and under dual control. A record of destruction by reel number and item count must be maintained for 24 months.

TechR2®'s data security processes comply with 4.10.a with a secure data trail of tracking, containing and destroying the PCI devices. TechR2® exceeds the 24 months' timeframe

b) The following materials must be destroyed on a batch basis by shredding or grinding such that the resulting material cannot be reconstructed:

- *Spoiled or waste card products*
- *Holographic materials*
- *Signature panels*
- *Sample and test cards*
- *Any other sensitive card component material or courier material related to any phase of the card production and personalization process.*
- *Destruction of chips, modules, or chip cards must ensure that the chip itself is destroyed.*

TechR2®'s data security processes comply with 4.10.b by destroying the magnetic media with NSA certified degaussers or solid-state media by crushing the chips to unreadable particle sizes

- *d) The material waiting to be destroyed must be stored securely, under dual control.*

TechR2®'s data security processes comply with 4.10.d by using two trained audit technicians to prevent collusion. TechR2® preforms all data security procedures using at least a 2-person team.

- *e) Destruction must be carried out in a separate room as defined in 3.3.5.3.*

> "3.3.5.3 Card Product and Component Destruction Room(s)
>
> a) Destruction of card product and component waste must take place in a separate room(s) within the HSA that is dedicated for destruction.
> b) Destruction by a third party may take place in the loading bay using portable/mobile equipment. All requirements for a destruction room must be met for this temporary usage"

TechR2®'s data security processes comply with 4.10.e in every Statement of Work (SOW) where we require a secure Component Destruction Room.

[1] https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Physical_Security_Requirements_v2_Nov2016.pdf?agreement=true&time=1484176101226

f) Proper destruction requires the following:

- Individuals destroying the materials must ensure that they are rendered unusable and unreadable.
- Two employees must simultaneously count and shred the material.
- Before leaving the room, both employees must ensure that all material has been destroyed and not displaced in the machinery or equipment.
- Employees must prepare, sign, and maintain a destruction document.
- Once the destruction process is initiated, the process must not be interrupted.

TechR2®'s data security processes comply with 4.10.f by TechR2® using circuit board crushing machines to crush the chips to unreadable particle sizes. Work in the destruction room is completed in that session.

g) An audit log must be created which, at a minimum, contains the following information:

- Signatures of the individuals presenting waste material
- Description of item(s) to be destroyed (such as product type, job number, and issuer name)
- Signatures of the persons observing or carrying out the waste destruction
- Quantity of item(s) to be destroyed Date and time of destruction

TechR2®'s data security processes comply with 4.10.g by precise auditing of critical data applying a TechR2® product ID to each device and capturing the manufacturer, model, serial number, job number, issuer name, date and time of destruction, sanitizer and verifier name, title, signature, contact number. A complete Certificate of Destruction is issued with the computer data.

Destroyed material is weighed and sent to downstream recyclers to meet TechR2® ISO 14001 requirements.