

Certificate of Erasure Checklist

Check every field before the report is filed. Labels match the PC-Doctor Erasure Report; NIST terms in parentheses where they differ.

1 Required by NIST SP 800-88 Rev. 2, Section 4.6

Missing any of these: not a certificate under the guideline

- | | |
|--|---|
| ☐ Manufacturer / Model | System block and disk block both present. Must match intake log. |
| ☐ Serial (system) + Serial (disk) | Two serials. The disk serial identifies the media; drives get swapped. |
| ☐ Bus (media type) | NVMe, SATA, USB. Determines which technique can reach Purge. |
| ☐ Method (method + technique) | Standard, level, and command on one line, e.g. NIST 800-88 Purge (NVMe Secure Erase). |
| ☐ Software Version (tool + version) | Full build string. "PC-Doctor Factory" alone is a brand name, not evidence. |
| ☐ Verification Method | Full or sampling. If sampling, your SOP must define the percentage; the report does not print it. |
| ☐ Technician ID (responsible person) | Must resolve to a named person in your records. Position is the signature-line role. |
| ☐ Location | Not on the report. Record on the batch log or cover sheet the report is filed with. |

2 Expected by auditors and enterprise customers

Compliant is not the same as useful

- | | |
|--|---|
| ☐ Asset ID | Customer asset tag. Configured before the run; blank means it was not. |
| ☐ Size (drive capacity) | Reported capacity should match the label. A shortfall suggests a hidden area. |
| ☐ Start/End Time + Duration | A pair, not a date. Seconds for a firmware Purge; hours for an overwrite. |
| ☐ Status: Erased | Explicit result. Anything other than Erased is a failed drive, whatever else the page says. |
| ☐ Standard + level in Method | Exactly one standard, one level. Record the revision (Rev. 1 vs Rev. 2) in your SOP. |
| ☐ Erasure Provider | Your company name, from configuration. Ties the report to the operation that ran it. |

3 Also on the report: evidence the level claim rests on

These are why a Purge is defensible

- | | |
|--|---|
| ☐ HPA / DCO: Doesn't Exist | If either exists, the drive was not fully addressed. Do not file as Purge. |
| ☐ Remapped Sectors, before / after | Both values. A non-zero after-count is a retired-sector question for the SOP. |
| ☐ Health Status | A failing drive cannot be verified. Route to Destroy. |
| ☐ Erasure Rounds (firmware) | Confirms the drive's firmware performed the erase, not a host overwrite. |
| ☐ Report UUID + Digital Signature | Authenticates the report contents. Not a substitute for the operator signature. |

4 Before the first drive runs

The tool cannot fill these in

- | | |
|---|--|
| ☐ Technician ID, Provider, Asset ID set | All three are configuration. The fields most often blank at audit. |
| ☐ Signature process decided | Operator and supervisor lines: wet signature on each report, or a batch attestation the Report UUID refers to. |

Reject the report if

- Method names two standards. They require different things of the same drive; a reader cannot tell which applied.
- Method names a standard but no level. A drive can be sanitized under a standard and still only reach Clear.
- HPA or DCO shows Exists, or Status is anything other than Erased, and the report is filed as a Purge.
- Technician ID or the operator signature line is blank. The sanitization may be sound; the certificate is not.

Report reviewed

Report UUID: _____	Asset ID: _____
Reviewed by: _____	Date / Location: _____
Findings / fields missing: _____	