DATA SAFE
SOLUTIONS

METHOD PAPER · SEPTEMBER 2026

Proving the data is gone.

One closed loop, nine steps. Fully automated, on each individual device, with no human decision and no fallback.

THE PROBLEM THIS SOLVES

You cannot know what will erase a drive without examining that individual drive.

The model number is not enough. Conventional platforms select a method first, then check whether the drive will run it. But Purge is a category, not a single command, and devices carrying the same model number can respond differently to the same selected method.

> **From a large UK ITAD's own erasure logs.** 61 drives of one identical model, all reporting that they support Purge, all issued a Purge command on that basis. On 57 it did not complete. On 4 it did. Same model, same reported capability, opposite results.
>
> Supporting Purge is not the same as that being the specific operation that destroys the data on that unit. The 57 were then wiped by a fallback overwrite and certified as erased anyway, and the data-bearing regions a Purge would have addressed were outside the reach of the method that ran.

If identical model numbers do not respond the same way to the same selected method, **you cannot know in advance what will erase the individual drive.**

STEPS ONE TO FOUR · DETERMINE AND ENFORCE

Remove the guess before anything is erased.

01 **Interrogate the individual device, in place.**

Read the drive's actual, true internal capability, as the physical unit reports it at the interface. Not the model printed on the label, not the batch, not an assumed device type.

02 **Determine the correct method from that capability.** THE PIVOT

From what the device actually is, determine the one method that will permanently destroy the data on it. This is the pivot the whole chain turns on, and it is a difference of purpose rather than of mechanism. Every other tool asks whether a method it already chose is permitted. This asks which method is correct.

03 **Seed the outcome test, before erasing.**

Write known verification data to randomly selected sectors and confirm it is genuinely present. That establishes a known pre-erasure state against which the outcome can later be tested. If the marker cannot be written and confirmed present, there is no valid known state to test against, so the device fails closed here. No marker, no trustworthy outcome test, no certificate.

04 **Enforce: execute the determined method.**

Run that one correct, device-native command. Only that one, and only on that device.

The method is not selected by an operator, a configuration or a hierarchy. **It is determined by the engine from the individual device.**

STEPS FIVE TO NINE · TEST, GATE AND CERTIFY

Two separate gates, and nothing to fall back to.

05 Fail closed if the command does not complete. NO FALLBACK

Because the engine selects the method that destroys the data rather than one chosen to pass, there is nothing to fall back to. Where the correct method does not complete, the device is not dropped to a weaker method that would pass. It fails closed and is diverted to remediation or physical destruction. The same applies where a model or firmware implementation is known to be unsafe.

06 Test the outcome: attempt to recover the seeded data.

After execution, attempt to recover the seeded data from the same locations. This is an empirical before-and-after test of the actual result, not a reading of the drive's status flag.

07 Fail closed if the outcome test fails. DISTINCT GATE

If any of the seeded data survives, the erase did not achieve the outcome, and the device fails and is not certified, whatever the drive reported about the command. This gate is distinct from step 5: there the command did not complete, here the command reported completion and the outcome is disproved.

08 Record re-checkable evidence.

Log the sectors before and after, the result, the device state, and a sanitisation signature: a hash of the evidence combined with the drive's own write counter, so the outcome can be re-verified later rather than taken on trust.

09 Certify only a passed outcome. OUTPUT

A certificate is issued only for a device that has passed the outcome test. Anything failed at either gate has already been diverted to destruction or remediation. Nothing is ever certified on a substitute.

A drive's status flag says the command finished. **The outcome test says the data is gone.** Only the second one is certified.

WHY IT MATTERS

Destruction proven, not assumed.

Nine steps
FULLY AUTOMATED, ON EACH INDIVIDUAL DEVICE

No human decision
NO OPERATOR SELECTS THE METHOD

No fallback
NOTHING IS CERTIFIED ON A SUBSTITUTE

Two gates
COMMAND COMPLETION AND OUTCOME, TESTED SEPARATELY

WHAT THIS CHANGES

The certificate stops being a belief and becomes re-checkable evidence. The outcome is tested on the device itself, before and after, and certified only when it is proven. On the most sensitive data, that removes the reason the world falls back to physically destroying working equipment.

THE PROTECTED DIFFERENCE

No single step is the invention. The integrated per device chain that removes the guess is, and it is covered by published UK patent application **GB2638704**, with a related US filing.

The conventional model certifies that a process ran.

We prove the data is gone, and only then certify it.

Evidence behind this paper. Operational erasure logs from live disposal operations, in redacted form. A patent landscape review of 18 competitors. Published competitor licence terms. Published UK patent application GB2638704.

Data Safe Solutions Ltd
2nd Floor, Port of Liverpool Building, Mann Island, Liverpool L3 1BY
0151 440 3200 · hello@datasafe360.com · datasafe360.com
VAT 425206721 · Company 12245066