Freedom of Information Request: Our Reference CTMUHB_143_26

You asked:

Under the Freedom of Information Act 2000, please provide the following recorded information held by your organisation regarding assurance processes for software based data erasure of end of life IT equipment.

For clarity, this request relates specifically to the erasure of storage media associated with end of life hardware such as laptops, desktops, servers, storage arrays, or other data bearing IT equipment. It does not relate to operational deletion of data within live systems, routine account management, or DSP Toolkit self assessment processes.

Physical destruction methods such as shredding, crushing, degaussing, or disintegration are outside the scope of this request. This request concerns software based erasure only.

This request seeks to distinguish between confirmation that an erasure process was carried out and recorded evidence demonstrating that the final data state of a specific storage device is irrecoverable. I am not seeking technical configuration detail or security sensitive information, only the recorded assurance basis relied upon when concluding that personal data has been rendered irrecoverable.

Please confirm:

1) Whether your organisation's policies, contractual terms, or internal procedures require an explicit outcome based warranty or guarantee that personal data on a specific storage device has been rendered irrecoverable as a final data state following software based erasure.

2) Where software based erasure of storage media is undertaken internally, what recorded evidential assurance is relied upon to conclude that the final data state of the specific storage device is irrecoverable, as distinct from confirmation that an erasure process was executed.

3) Where software based erasure is undertaken by a third party provider:

a. Do the certificates or contractual documents held constitute an explicit outcome based warranty or guarantee of irrecoverability for each specific storage device processed?

b. Beyond reliance on supplier accreditation or recognised standards including but not limited to ADISA certification, ISO accreditation, NIST alignment, HMG IA standards, NHS Digital guidance, or Data Security and Protection Toolkit assertions, and beyond confirmation that a wiping process was completed, does the organisation hold any recorded, device specific documentation evidencing independent verification, testing, or validation that the data on the storage media has been rendered irrecoverable in practice?

4) If no explicit outcome based warranty or device specific outcome evidence is held beyond certification, accreditation, or confirmation of process completion, please confirm what recorded form of evidential assurance is relied upon when concluding that personal data has been rendered irrecoverable.

Our response:

We use a 3rd Party company call Lifecycle solutions. All kit is logged for disposal on internal systems, and then collected by the company for asset disposal.

All data baring kit is wiped with Blancco Data Erasing Software and checked with our ISS software which are all CESG Level 5, which is Department of Defence standard. It is then recycled as per our R2v3 accreditation which we understand is the highest standard of recycling globally. R2v3 (Responsible Recycling Standard Version 3) is the premier international certification for electronics repair and recycling, focusing on data security, environmental protection, and worker health.

It mandates strict, audited procedures for handling, testing, and tracking electronic devices throughout the entire recycling chain to prevent improper disposal.