The Ins and Outs of Data Sanitization

Procurri specializes in ITAD (IT Asset Disposition) that prioritizes the recycling, refurbishment and resale of equipment over ever destroying it – and we never send anything to landfill. However, as a result of the hardware being reused, data-bearing equipment does need to have all of its information securely and permanently removed. This process is known as data sanitization and is something Procurri offers both on-site at client's own locations or through our own secured facilities. There are various methods of data destruction used by ITAD companies, and here's an explanation of each…

Physical Destruction

Physical destruction of equipment involves the use of industrial shredders to break hardware into pieces so that it would not be suitable for reuse and the data could not be salvaged from it. In these cases, it may be that the hardware (or portions of it) could be recycled into new materials or items but they would not be suitable for reuse as is. If shredders are unsuitable because of the materials the equipment is made of, it may be physical crushed or bent.

Degaussing

Degaussing equipment is the practice of exposing devices to a strong magnetic field. This irreversibly erases data on hard disk drives and most kinds of tapes. An electrical charge is passed through a degaussing coil to generate a magnetic field and there are several complementary technologies that can be implemented to ensure further erasure.

Data Erasure

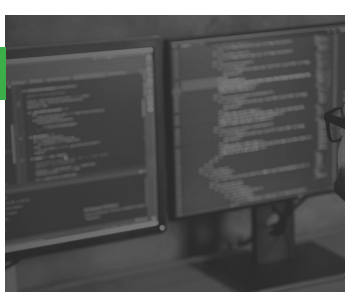
Data erasure is the usage of software to write in random 0s and 1s throughout storage equipment sectors, ensuring that none of the existing data can be retained. This is a reliable form of data sanitization because it validates 100% of data being replaced at byte level but it's very time-consuming and requires every decommissioned device to go through a very strict sanitization process. However, hardware subject to data erasure can be reused and resold and so it needn't be disposed of to landfill – and further value can be derived from it.

Cryptographic Erasure

Cryptographic data erasure uses public-key cryptography with a key of at least 128 bits to encrypt all data on a device. Once encrypted, the private key is discarded – encrypting the data and making it effectively entirely irretrievable. Cryptographic data erasure is a fast and effective form of data sanitization but does rely on the equipment itself holding sufficient encryption features to render it secure. There is also the risk of the key being obtained before it is disposed of, which could put the data at risk of later malicious retrieval. What's more, cryptographic data erasure does not usually meet legal regulatory standards as technically the data remains on the device and is not actually removed.

Data Masking

A widely used technique that's favoured by compliance standards in many territories, data masking creates fake versions of the data present, retaining structural properties of it but shuffling characters, replacing words and randomizing text. The masked version of the data cannot be reverse engineered to obtain the original values and so this is considered a highly effective sanitization method.



Want to learn more on Procurri's approach to data sanitization and to learn more about how it could be used for your decommissioned hardware?

Get in touch!

PROCURRI