DATA BEARING DEVICE POLICIES AND PROCEDURES

Data security is important to Kramden and to our donors. Kramden is an i-SIGMA (International Secure Information Governance & Management Association) member and adheres to industry best practices for data sanitization and destruction. The following procedures are performed to ensure that all data is completely removed from donated equipment in full compliance with HIPAA, NIST, and DoD standards.

Transportation & Storage

Data bearing devices received by authorized Kramden personnel are stored in a secure and monitored facility until processed.

Hard Drive Sanitization

All data bearing are wiped to the NIST 800-88 classification of "PURGE" specification which prevents data recovery by all software and physical measures. All devices go through this sanitization process and are scanned again during a verification pass to ensure data has been destroyed. Any device that fails this process is sent for physical destruction.

Physical Destruction

All data-bearing devices that fail the sanitization process or are deemed unusable are sent for physical destruction. All devices marked for physical destruction are transferred in locked totes will full chain of custody to our R2 certified e-waste partner Sprout. All devices are shredded to an 8mm edge length to ensure data destruction.

Certificate of Destruction

Kramden Institute will provide a Certificate of Destruction (CoD) for any business donor at request. Kramden takes full ownership of all devices and data contained within.

Data Removal Tools

The HDPARM utility is our software of choice for software sanitization of devices. The ATA Sanitize command, designed for the newest SATA hard disk drives as well as SATA, mSATA, m.2, and m.2 PCI-E NVME Solid Sate Drives (SSDs), is currently the most advanced method of data destruction. Wherever possible, the ATA Sanitize command is used as standard procedure for erasing all incoming devices. It should be noted that not all drives support the ATA Sanitize command. In such instances, a standard DoD 5220.22 3 pass wipe is implemented.

ATA Sanitize is implemented in three different ways, depending on the make and model of drive.

Sanitize Block Erase - a procedure in which all data is purged from all data blocks, including any caches.

Sanitize Cryptographic Scramble - a procedure in which the internally-held encryption keys used to access the data on the drive are destroyed, along with a Block Erase.

Sanitize Overwrite - a procedure that fills the user data area with a pre-defined four byte pattern. Parameters for this method include a count for multiple overwrites and the option to invert the four byte pattern between consecutive overwrite passes. The Sanitize Overwrite operation also removes any user data held in caches.

The ATA Sanitize procedure is compliant with the NIST “PURGE” specification.

Verification of data deletion is done in a final pass, which checks 10% of the drive to confirm data deletion. Erasure logs are stored on a separate flash drive. Once the erase procedure is complete, HDPARM is run again to check for any locked drives. Locked drives are flagged for an additional Secure Erase procedure. Additionally, random drives are manually verified by inspection of the drive’s partition table using Parted Magic’s built-in partitioning tool.