Proprietary Data & Technology Destruction Standards

Client Disclosure

Our standards presented here represent our commitment to complete Data Security within all parameters of business services provided. This commitment extends to Proprietary Technology and includes client customers, subsidiaries, partners, and branch locations which we serve.

Scope of Data Security

- Identification and application of consistent and effective measures for data security while performing all services rendered to Client. The result is full compliance to applicable regulations and standards: NIST 800-88, DSS DOD (DOD5220.22), HIPAA, SOX, PCI-DSS, and FACTA.
- Transparency Measures and Data Destruction Reporting

Steps

1. *IDENTIFICATION*
   Data Security starts with our driver identifying, tagging, and presorting all materials we receive. Known "data-sensitive" devices, are labeled. We provide secure transportation and no co-mingling of Client's material with other material occurs.

Copyright ©2018 ewasteSF. All Rights Reserved

2. *DESTRUCTION PROCESS*
   Upon receipt of materials at our facility, a thorough sorting takes place. We identify data holding devices, including Internal/ External Storage Drives, SD, Sim, Optical (opening internal drives to verify), Flash Memory, Cellular devices of all types, PDA, etc. These items go through an immediate step of being "cancelled out" by physical destruction the same day as received. We remove all corporate identifiers and tags. Our staff is trained to identify data devices of all types and in any form. This includes documents and memos inadvertently left behind in printers, file cabinets, etc. Pulp/paper containing information is shredded. All devices and all forms of data are ground and smelted after they have been made permanently inoperable. For SSD carrying devices and/or devices with storage embedded in the logic board or motherboard, the following form of data destruction will occur (at minimum):

   a) The device will have storage wiped and overwritten three times using an onboard disk utility or will be factory restored for cellular- or Google-based systems.
   b) A screenshot of the device will be provided showing the serial number and "zero data" remaining on the storage component. This will be date/time stamped within the metadata of the picture produced.
   c) If a device is password protected, won't power on, or if its storage component is in any way inaccessible, then the storage component will be shredded. Shredding will occur immediately and pictures or video will be provided accordingly.

3. *REPORTING*
   Reporting on the destruction of media occurs within 24 hours of receipt. Reporting can occur in any medium the client prefers. A secure, online client-specific portal is provided that includes a detailed description of items destroyed, including serial numbers, if applicable.

Services Provided by Third Parties

ewasteSF may procure the services of a federally certified third party processor to perform recycling of materials. The services of a refinery/processor will be engaged only after the device or material has been made permanently inoperable by physical destruction and the risk of data loss is zero. Chain of Custody will be documented all the way through the process until the materials are converted to pellets or granules.

Performance of Services

All data destruction methods meet or exceed NIST 800-88 Standards, DoD 5200.22-M Data Sanitization and/or all different standards, such as HIPAA/HITECH, Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, FACTA Disposal

Copyright ©2018 ewasteSF. All Rights Reserved

Rule, Bank Secrecy Act, Patriot Act of 2002, Identity Theft and Assumption Deterrence Act, US Safe Harbor Provisions, FDA Security Regulations, PCI Data Security Standard, and all other various local, state, and federal regulations.

All services performed will be done in a professional manner in accordance with National Association of Industry Destruction (NAID) standards and practices. We identify with NAID criteria in all areas of our operation where information may knowingly or unknowingly be transferred to our custody for processing.

Material Accounting and Access
Itemized lists or descriptions of materials submitted from Client to ewasteSF shall be used for record keeping, reconciliation, and reference purposes. To maintain integrity of zero tolerance data loss, all lists or record keeping will be subject to audit and any discrepancies disclosed to Client. All materials received by ewasteSF will be made available at any time, pre-grinding, for Client's re-inspection or diligence.

Proprietary Technology Destruction
As directed by the Client, Proprietary Technology Destruction will also be included. Methods for Proprietary Technology Destruction will have same level of scrutiny as Data. Style of destruction may vary due to physical size, composition, and type of materials.

Terms, Conditions, and Termination
All measures in place for Client's Data Security will be maintained, ongoing, whenever ewasteSF is utilized by Client.

ewasteSF is a member of and adheres to the tenants of the following organizations:

e-Stewards

R2 is Responsible Recycling

G4 SUSTAINABILITY REPORTING GUIDELINES

NAID®

Copyright ©2018 ewasteSF. All Rights Reserved