DIVERSIFIED RECYCLING

Form #57, Revision #4 Date 7/15/2015

Data Destruction and Sanitation Program

Mobile (ON-SITE) Data Destruction/Shredding Services

Diversified Recycling utilizes state of the art equipment for their data destruction and eradication services. When an individual or company makes the decision to upgrade their computer network, the older equipment is often restructured to work in another area of the business, sold on the secondary PC market, donated to charity or otherwise destroyed. In any of these scenarios, it is of the utmost importance that the existing data residing on the hard drives of the computers are effectively erased (sanitized).

Data sanitization is the process of deliberately, permanently, irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data. Sanitization processes include using a software utility that completely erases the data, a separate hardware device that connects to the device being sanitized and erases the data, and/or a mechanism that physically destroys the device so its data cannot be recovered.

Hard Drive Sorting

Diversified Recycling shall sanitize, purge, or destroy data on hard drives and other data storage devices ONSITE: to include but not exclude: (Digital copier, printer memory, cd rom, hard drives, data devices in cell phones, video tape, DVDs, and memory sticks.in compliance with (the National Institute of Standards and Technology's (NIST's) Guidelines for Media Sanitization – Special Publication 800-88 lists categories of devices which need sanitization consideration), unless otherwise requested in writing by the customer. Diversified Recycling shall adhere to the data sanitization, purging, or destruction practices described in the NIST Guidelines for Media Sanitization: Special Publication 800-88
(Rev.1).

1.1 Diversified shall ensure electronically---stored information is being handled in accordance with all national and state/provincial laws governing data destruction that apply to its operation. Diversified Recycling shall remain diligent and knowledgeable with national, as well as state/provincial laws that govern data management and destruction, which in some cases can have stronger data management requirements than the national regulations.

1.2 Diversified Recycling shall manage personal information in accordance with national regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm---Leach---Bliley Act (GLBA), and the Identity Theft Penalty Enhancement Act (ITPE) which create safeguards to protect private information.

1.3 Diversified Recycling has designated fenced in secure areas within ALL of our facilities to store and facilitate the data destruction process. These secure areas are under constant audio and video surveillance and locked when not occupied by the approved/authorized staff. Personal Protective Equipment (PPE) is not required while operating the degaussing and hard drive erasure machines.

Acceptable practices for the destruction of data depend on the type of media, the sensitivity of data, customer requirements, and the methods used. Diversified Recycling not only removes the circuit board from all hard drives determined to be tested, non-working/failed are then shredded through the use of our AMS-500 SERIES 2 HARD DRIVE SHREDDER which turns the drive into unusable particles, exceeding NIST Special Publication 800---88 specifies acceptable methods for data destruction by media type and classification (sensitivity). As new technologies emerge, generally accepted and published industry techniques may be acceptable through the validation process in 8(d).

If Diversified Recycling receives electronic data storage devices that are supposed to already be sanitized, Diversified Recycling shall be provided documentation by the vendor/customer of data destruction prior to the receipt of the media storage devices. Diversified Recycling shall run all received hard drives through the Tabernus Enterprise Erase LAN 7.3 Program to ensure that all data has been sanitized according to the identified specifications. Diversified Recycling shall also conduct periodic testing of previously sanitized devices to ensure data destruction has been performed. All activities involved in data destruction shall be clearly described and conveyed to employees. All information pertaining to data destruction procedures shall be documented. Documentation shall include material handling, labeling, processing, storage, physical security, and validation of results. In addition, ALL hard drive degaussing equipment may require equipment calibration and maintenance to ensure effectiveness. Evidence must be generated and maintained to show conformity to the data destruction procedures and effective processing.

Third Party Validation Process

An independent review of data destruction procedures shall include validation of the procedures, and performance of data destruction methods. The independent review shall be conducted by IT Service Professionals. On a monthly basis, randomly selected hard drives shall be sent to IT Service Professionals for third party validation. The following procedure shall be completed on each drive:

-IT Service Professionals Device and OS Review: IT Service Professionals shall separate external and internal methods to validate if the hard drive is bootable to test. IT Service Professionals will also run the hard drive on separate operating systems with separate software applications to ensuring that the material is tested thoroughly.

-IT Service Professionals Automated Review: Using proprietary software, the entire recording surface, including host-protected areas (HPA), is checked for any relevant file system structures. This includes boot records, NTSF file tables, Windows FAT file allocation, exFAT, HFS+, ISO9660, EXT2/3, Superblocks, inodes for UNIX, MAC based HDD's, and any presence of common file types as identified by file headers found in raw data.

-IT Service Professionals Shredded Material Review: If the material is shredded or destroyed, IT Service Professionals will inspect and validate if any data is recoverable. After running unique tests, IT Service Professionals experts will determine and record the results.

IT Service Professionals Manual Review: An IT Service Professional data recovery technician will manually review random portions of the HDD as an added safety measure.

IT Service Professionals Escalation Process: During the above processes if any data is discovered, IT Service Professionals will contact the Diversified Recycling immediately. Data shall remain secure and in of the organization at all times.

IT Service Professionals Reporting: Upon validation completion, IT Service Professionals shall initially email as well as provide Diversified a Certificate of Validation with serial numbers with company seal for our records. When all tests are finalized and the material(s) deemed inoperable or sanitized IT Service Professionals will invoice Diversified and send back the hard drives and/or material(s). Material(s) will be shipped back at the expense of IT Service Professionals.

Reviews shall specifically include competency evaluations of employees, attempts at data recovery from sanitized devices, verification of calibration schedules, and verification of data sanitization records.

Diversified Recycling shall produce certificates, or evidence of regular review of data destruction procedures and validation of data destruction methods. For example, disk wiping methods may be validated using commercial software for data recovery to demonstrate no recoverable data on the wiped media. Forensic analysis or any other more rigorous data recovery method would only be necessary if the sensitivity of the data on the media warrants it in line with the NIST 800---88 guidelines. Additionally, physically destroyed media would not require data recovery attempts if the composition and/or size of the destroyed material is consistent with the NIST 800---88 specific guidelines. For example, shredded optical disks must meet a specific particle size.

ALL customers and prospective customers will receive an electronic copy of Diversified Recycling's Data Destruction and Sanitation Program Manual outlining our procedures and protocols for the data destruction/data security of all media devices received from their company or entity conducted in our facilities. This electronic copy will be sent via email submission with a delivery receipt confirmation confirming the documents and data destruction program has been communicated by our Sales Managers, Senior Account Managers and Account Managers.

a) Diversified Recycling shall inform customers of data security risks, and communicate in writing with customers the Diversified Recycling; explicit role, service obligations and agreements, and customer

b) Indemnifications, if any, regarding the data security services that are and/or are not provided. In addition, for customers that are utilizing the Diversified Recycling' data security services, this will include communication of the:

- Types of assets for which Diversified is sanitizing data,
- Method(s) by which data sanitization shall be accomplished, e.g. Tabernus Enterprise Erase software-based media overwriting processes, degaussing, and/or physical destruction of media, and
- Data security standard(s) that is achieved in securing and sanitizing Customer Data

c) Diversified Recycling has developed, implemented, and maintains written procedures for physically securing data storage devices, and data processing systems used in the delivery of data security services. Diversified Recycling has established, implemented, and maintains controls to physically and electronically protect all Customer Data until it is sanitized (or returned to the customer), whether data storage devices are going for reuse, Materials Recovery, or Final Disposal, for each device throughout the chain of custody. This system of controls shall:

- Identify the data-bearing characteristics of the assets types for which they provide services, on an ongoing basis,
- Establish and document a clearly defined chain of custody for Customer Data, including the following:

Stipulate when and where the transfer of custody to Diversified begins and ends for Customer Data, i.e. until it is sanitized (including destruction),

Provide secure logistics for data security, including the transport of customer/user assets to Diversified's facility(s), between Diversified's own facilities, and/or to the End Refurbisher(s), and maintain effective physical and electronic controls throughout the transport and transfer processes, and

Ensure that any locations where customer assets may be temporarily stored during transport and transfer processes operate under a comparable set of security requirements as defined below:

- Provide effective controls to physically and electronically secure facilities and equipment, in order to:
- Ensure that only authorized personnel are allowed access to areas where Customer Data is stored and where data security services are performed,
- Isolate areas where data security services are performed from locations where unauthorized people can enter the property, such as loading and unloading areas,
- Prevent data from being electronically accessible, even if physically controlled, and
- Restrict or control entry and exit of authorized guests in secure areas, as appropriate,
- Implement controls to mitigate data security risks associated with workers, including but not limited to background verification checks on all workers and temporary service providers who are involved in the delivery of data security services, and
- Establish effective inventory control by documenting and tracking the custody of all data storage devices and sanitization activities on them, including:

- Clearly identify all equipment and components that require data security services either by using a manufacturer-designated serial number or assigning a unique number for each device, or by designating secure accumulation areas for non-serialized data storage devices,
- Document their physical location and data security status throughout the chain of custody,
- Implement handling procedures to ensure inventory integrity until data sanitization is complete, that prevent access to accumulated media, and track accumulation containers' physical locations until Customer Data is sanitized (including media destruction), and
- Provide inventory tracking information to customers regarding their data storage devices and sanitization status, and allow customers to audit inventory tracking processes, upon their request,

All employees involved in the data destruction procedures shall be fully trained. As part of the "training on a regular basis", employees shall receive information about updated data destruction methods and regulatory requirements as they become available. All applicable employee training shall be documented.

The independent review of data destruction procedures shall include validation of the procedures, quality of employee training, calibration and maintenance of equipment, and performance of data destruction methods. The review may be conducted by an impartial member of the management team who has demonstrated expertise in NIST Guidelines, comparable international data destruction guidelines, or data forensics methods. As with any audit, the auditor must demonstrate that he/she is qualified and has the expertise and/or experience to evaluate the recycler's data destruction process. However, the person performing the internal review shall not be involved in the daily data destruction process, nor in any way be accountable to the management responsible for data destruction, so that the review can be truly independent. Depending upon the sensitivity of data being destroyed, methods used, type of equipment, and level of expertise in-house, an outside review may be necessary.

Reviews shall specifically include competency evaluations of employees, attempts at data recovery from sanitized devices, verification of calibration schedules, and verification of data sanitization records.

Diversified Recycling shall produce certificates, or evidence of regular review of data destruction procedures and validation of data destruction methods. For example, disk wiping methods may be validated using commercial software for data recovery to demonstrate no recoverable data on the wiped media. Forensic analysis or any other more rigorous data recovery method would only be necessary if the sensitivity of the data on the media warrants it in line with the NIST 800---88 guidelines. Additionally, physically destroyed media would not require data recovery attempts if the composition and/or size of the destroyed material is consistent with the NIST 800---88 specific guidelines. For example, shredded optical disks must meet a specific particle size. If the recycler's process does not correspond to the minimum size or form requirements of the NIST 800---88 guidelines, then forensic analysis would be needed to confirm the inability to recover data from the media.

1.4 Hard drives and/or other media storage devices are removed from all equipment. The hard drives and/or other media storage devices are then sorted and staged in the designated secure area with limited access until

ready to be degaussed or erased. Hard drives with a minimum storage capacity of 40G or greater are sorted for secure hard drive erasure and reused in refurbished computers, laptops, servers for resale.

(a) Diversified Recycling shall document its data destruction procedures and include this documentation as part of its EHSMS.

(b) Employees involved in data destruction shall receive appropriate training on a regular basis and be evaluated for competency in data destruction processing.

(c) Data destruction processes shall be reviewed and validated by an independent party on a periodic basis as defined in the documentation called for in subsection (a) above.

(d) Quality controls shall be documented, implemented, and monitored internally to ensure effectiveness of data sanitization, purging, and destruction techniques.

(e) Security controls that are appropriate to the most sensitive classification of media accepted at the facility shall be documented, implemented and maintained. Security controls shall consider physical security, monitoring, chain-of-custody, and personnel qualifications.

(f) Adequate records of data destruction shall be maintained.

(g) Diversified Recycling will ensure that all data destruction is facilitated and documented prior to any media storage devices being shipped to another downstream vendor:

2.0 Hard Drive Sanitizing

2.1 Hard drives are sanitized in a secured caged in area.

2.2 Hard drives serial number tracking is maintained through the Tabernus Enterprise Erase System.

2.4 Hard drives are then sanitized in compliance with (the National Institute of Standards and Technology's (NIST's) Guidelines for Media Sanitization – Special Publication 800-88 [12] and then sorted and staged by storage capacity for reuse and/or resale.

2.5 Once hard drives have been properly sanitized (as evidenced by the report generated by the Tabernus Enterprise System, a sticker reading "SANTIZED, Diversified Recycling, with the Date and initials of the Staff that facilitated the sanitation. The hard drives are then stored in the secured area until ready for reuse or resale. Hard drives with a storage capacity of 40G or less will be sanitized through the Tabernus Enterprise Erase System, stamped with "Sanitized" and staged for dismantling. These hard drives have limited storage capacity and therefore do not meet the reuse or resale criteria. Hard Drives with a storage capacity of greater than 40G shall be staged for re-installation in tested for key function computers, laptops and/or servers and/or designated for resale. Hard Drives that fail the Tabernus Enterprise Erase System will be stamped with the word "FAILED" and IMMEDIATELY staged in the data destruction cage for dismantling and shredding. No hard drive will

leave the secure cage unless it gets successfully sanitized through the Tabernus Enterprise Erase System and/or dismantled and shredded.

3.0 Hard Drive Erasure

3.1 Hard drives stored in the secure area are separated based on storage capacity and whether they support a SATA, IDE, SCSI or SAS connection.

3.2 The appropriate hard drive caddy is chosen for the hard drive's SATA, IDE, SCSI or SAS connection. The hard drive is firmly connected to the caddy.

3.3 Hard Drives may be erased one at a time or multiple drives can be sanitized simultaneously through the use of the Tabernus Enterprise Earase System.

The data destruction industry adheres to two specific sets of standards – D.O.D 5220.22-M and NIST publication 800-88. Both of which Diversified Recycling utilizes for our minimum requirements for our data destruction policy.

D.O.D 5220.22-M:

The Department of Defense Standard 5220.22-M, Section 5, Subsection 8.5.3 states that to effectively overwrite the data on recordable media, each section of the disk must be overwritten **three times**, or what's known as three passes. On the first pass, the data in each sector is replaced with a character. On the second pass, the character is replaced with its complement. And, on the third and final pass, the sector is filled with a random character. In addition, items which have been cleared must remain at the original level of classification and in a secure, controlled environment. It is important to note that 5220.22-M DOES NOT recommend the three pass system for sanitization of "top-secret' information. In this instance or upon the customer/vendor's request, Diversified uses physical destruction methods to permanently destroy the media and/or data.

For disks sanitization to fall under the D.O.D standards, the information on the disk must be removed through a two-step process in which the three pass procedure is completed first, and then followed by the physical destruction.