THE MOBILITY
MARKETPLACE
CELL PHONE DEVICE MANAGEMENT

A Comprehensive & Secured Recycling Choice

At The Mobility Marketplace we realize your proprietary information is important to you and that is why we make security our #1 priority.

The TMM Guarantee:

- Comprehensive data protection. The next owner of your device will have no idea who the original owner was
- Not worrying that your phone ends up overseas in a foreign country
- 33+ point inspection with each device

This is why we utilize the Greystone equipment in our secure facility in **Fort Worth, Texas**.

Greystone Data - ZeroIT Security

TMM data wipe solution is R2, NIST-800-88, NAID, and industry compliant utilizing Greystone Data Technology equipment and servers.

- For Iphone, Greystone solution flashes the device and updates to the latest OS. This is more secure than a manual Settings > General > Erase all Content and Settings (which is typically the industry standard for R2, NIST-800-88 and NAID).

- For Android, the device will be reformatted and factory reset (also R2, NIST-800-88 and NAID standards), reformatting is an additional service we provide to assure data sanitization.

- For Blackberry, the device will be reformatted and factory reset (also R2, NIST-800-88 and NAID standards), all existing IT Policies and data are removed to provide assure data sanitization.

- All devices are certified by Greystone (a third party) using automation and clear traceability tactics i.e. timestamps, and additional evidence… for example: we keep the transaction codes directly with Apple when doing data clears - Apple is the only one who can authorize erasure and update. This holds a lot of weight because the manufacturer/OEM controls the whole erasure process and having those update codes directly from them is unique evidence that a device has been data cleared which allows us to certify data clear on a device.

TMM Data wipe solution meets all standards of industry and satisfy requirement of authorities who oversee and define the methods that are sufficient for the electronics industry.

GSA Contract Holder
Contract GS-35F-017GA

BBB ACCREDITED BUSINESS
Rating: A+
Since May 2016
As of 12/9/2016
Click for BBB Review
Rating: A+

THE MOBILITY
MARKETPLACE
CELL PHONE DEVICE MANAGEMENT

Cell Phone Data Removal: Don’t Be a Victim, We Have the Solution

Most consumers or businesses claim to know how to securely remove/wipe all cell phone data, but most just do a high level factory reset which does not actually wipe the phone and only masks the user data/information on the device.

The Mobility Marketplace utilizes a method referred to as a High Level 3 Pass Secure erasure which meets DOD/HIPAA standards by utilizing a 3 pass overwrite. This allows any of our clients to run forensic tests (if they chose to audit us) which results in them not finding any remaining user data or information on their devices.

Below is a basic understanding of the types of data erasing available that consumers or businesses may or may not use.

Approx. 95% of Consumers and Business Customers do the following, which is NOT SECURE:
Factory Reset only deletes files, passwords, data, images, etc., which are still hidden on the devices and are somewhat encrypted to appear that the device has been erased. Anyone could use software to retrieve this user’s information.

Approx. 85% of recycling companies do not invest the time or money in equipment to properly and securely data wipe by only doing the following, which is NOT SECURE:
These recycling companies use a low level equipment to achieve a faster completion time per device by only doing a 1 Pass erasure to achieve the minimum requirements of a numeric or alpha sequence to encrypt a user’s information and sensitive data. This is better than a factory reset, but still hackable.

The Mobility Marketplace, along with approximately less than 15% of recycling companies, follows this next method to achieve the highest level of data removal for cell phones, tablets, iPads, and smartphones, which is SECURED:
The sophistication of our high-level equipment requires each device to run an encrypted numeric or alphabetic code sequence 3 consecutive times. This assures a customer’s information and data is encrypted and removed according to DoD/HIPAA requirements.

The following are case studies of consumers and businesses whose data was not properly erased:

Sony Hack:
https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022

Hillary-Rodham Clinton Cell Phone/Email Hack:
http://www.techrepublic.com/article/hillary-clintons-infamous-email-server-6-things-you-need-to-know/