e-RECYCLING OF CALIFORNIA

# Information Containing Devices (ICD) and Information Security Policy (external)

## I. POLICY

The purpose of this document is to explain and demonstrate e-Recycling of California's ICD Security Policy. ICD's are described as any item that may contain personal data. ICD's are contained in electronic devices such as: Cell Phones, Computer Processing Units, External Drives, Laptops, Notepads, PDA's, and Servers. As well as some copiers, printers, and fax machines.

ERC becomes the information owner of known transfer of ICD's.

A. It is the policy of e-Recycling of California that ICD's in all their forms—SIM Cards, Hard Drives, and media will be protected and secured until one of the following activities have been completed:
   a. Hard Drive (HD) - ICD Dismantlement. This practice involves the deconstruction of HD's in which the housing unit, printed circuit board, rare earth magnet, aluminum, steel, cast iron, ferrous/non-ferrous metals and HD discs are completely separated.
      i. HD Discs
         1. Aluminum HD Discs – Secured until they are smelted at Approved Downstream Vendor
         2. Ceramic HD Discs – Secured until physically broken on-site

OR:

         3. Sanitize - DOD Wipe Standards. Conducted either on-site or by Next Tier 3rd Party Approved Vendor
   b. SIM Cards – Secured until they are destroyed on-site

B. Confidential Information
   a. Confidential Information that is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
   b. Examples of Confidential Information may include: personnel information, key financial information, and proprietary information, system access passwords.
   c. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for e-Recycling of California, its customers, or its business partners. Decisions about access to this information must always be cleared through the information owner – e-Recycling of California

E-RECYCLING OF CALIFORNIA

# Information Containing Devices (ICD) and Information Security Policy (external)

## II. SCOPE

A. ERC will to the best of its abilities and resources prevent unauthorized access to or release of Customer Data. Further, ERC will offer data security services in-house and/or under ERC's control. ERC shall retain the responsibility for protecting and preventing unauthorized access or release of Customer Data.

B. ERC will ensure the physical security of ICD's until the time of disposition.
   - d. ICD's, Cell Phones, SIM Cards, and Media will be secured in sealed containers
     - i. Containers will be inventoried
     - ii. Containers will be monitored by CCTV
   - e. CPU's, Servers, Laptops prior to ICD extraction
     - i. Pallets/Containers will be inventoried
     - ii. Pallets/Containers will be monitored by CCTV

C. ERC will control access to Secure Areas

D. ERC will conduct employee background checks as a New Hire practice for employees required in controlled access areas. (Beginning September 2014)

## III. SECURITY BREACH

A. In the event of a Security Breach ERC will inform relevant authorities in a timely manner.

B. ERC will report the breach to the impacted Customer in a timely manner.

C. ERC will collect and transfer relevant evidence to the proper authorities in a timely manner.