

Data Security Policy for Information Containing Devices (ICD)

I. POLICY

The purpose of this document is to explain and demonstrate e-Recycling of California's Information Containing Devices (ICD) Security Policy.

ERC is committed to data security and protecting our clients assets.

- ERC prohibits unauthorized individuals from accessing or handling equipment containing data.
- ERC has assigned a Data Protection Representative with overall responsibility and authority for ERC's data security and legal compliance, including oversight of all related duties otherwise assigned.
- ERC mandates reporting of known and suspected breaches of security and data to the Data Protection Representative.
- ERC requires completed training and confidentiality agreements prior to individual authorization to handle equipment containing data.
- Employees found to violate this policy will be subject to disciplinary action that could include immediate dismissal.
- Employees found to violate this policy or found to have conducted a criminal act related to data security will be held financially and criminally responsible for damages and/or material loss to ERC and its clients to the extent allowed by law.

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

- A. It is the policy of e-Recycling of California that ICD's will be protected and secured until physical data destruction has been completed.
- 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

Data Security Policy for Information Containing Devices (ICD)

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
- B. ERC will ensure the physical security of ICD's until the time of disposition.
 - a. ICD's will be secured in sealed containers
 - i. Containers will be inventoried
 - ii. 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.