Sensitive Customer Information

Macro Integration Services strives to protect the sensitive information of our Customers to the highest degree. We consider this obligation an extension of the Core Values of trust, integrity, quality, improvement and teamwork outlined on our website. This commitment is evidenced by our daily efforts to make our Customers successful.

At a minimum, the following provisions are made regarding our associates, technology and processes:

Associates

- Each full-time, part-time, temporary or contract employee must take and pass a background check and drug test as a prerequisite for employment. These checks and tests are redone on a recurring basis or if there is suspicion of a possible problem.
- Macro Associates are provided educational opportunities and resources about current PCI best practices to protect sensitive information.
- Macro maintains the Qualified Integrators & Resellers (QIR) qualification from the PCI Security Standards Council with a minimum of 3 certified individuals.
- Macro Integration maintains at least one Associate with the Payment Card Industry Professional (PCIP) designation.
- Associates are required to complete monthly security training focusing on the topics of common security threats, social engineering, phishing, secure passwords, multi-factor authentication, best practices while traveling etc…
- Associates are encouraged to hold each other accountable to the high customer service standards identified in our Mission Statement and Core Values.

Technology

- All inventory and customer service activities are conducted in our enterprise service management system.
- A surveillance camera system is maintained throughout the interior and exterior of Macro facilities.
- Macro maintains a high standard for its internal IT assets and processes on par with industry norms and outlined in our Security Policy.
- Hardened systems with malware protection, secure passwords, firewalls and network security are all maintained for internal security.
- All visitors are required to sign-in with ID and picture and are given nametags to wear at all times in any Macro facility.
- Physical access to Macro facilities is restricted by a secure badge access system. An added layer of access is required for devices that contain or may be used for PCI, PII, or PHI sensitive data or transactions.

Sensitive Customer Information

Processes

- Macro maintains membership in the PCI Security Standards Council as a Participating Organization.
- Access to internal and customer information is restricted to a “need to know” basis as directed by our customers.
- A Visitor sign-in/sign-out log is maintained in each Macro facility.
- Part serialization is systematically required for parts with serial numbers and tracked throughout Macro’s possession.
- As noted above, a special security area is maintained inside of Macro’s main warehousing facility for parts designated by the customer as needing an additional layer of protection. i.e. Pin pads, POS terminals containing sales data, Pharmacy servers, network equipment containing configuration files. No sensitive customer information or card data is ever stored on any equipment in any Macro facility.
- Macro maintains network segmentation whereby no customer data resides on or passes thru a Macro network. When access to a customer network is required it is done on a customer-provided circuit with customer-provided IDs and passwords. For any devices designated by our customers as “sensitive” or “secure”, we maintain chain of custody records to ensure we know and can trace the handling of those devices from warehouse, to staging, to shipping/delivery, to installation, or in reverse should those devices be deinstalled.