C&S Wholesale Grocers, Inc. and Subsidiaries

Policy Title:	**Protection of Personal Information**		
Effective Date:	**February 14, 2017**		
Policy Number:	**130**	**Version Number:**	**1.2**
Policy Owner:	**Senior Vice President, Compliance & Administration**	**Department Owner:**	**Legal**

PURPOSE

At C&S Wholesale Grocers, we stress the importance of privacy and are committed to protecting the personal information of our employees, vendors and customers.

POLICY & RESPONSIBILITY

C&S safeguards the "personal identifiable information" (PII) of its employees, vendors and customers. "PII" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. It does not include an employee's work identification. It also includes information on customers or vendors, when such information is supplied to or recorded by C&S in the course of transacting business.

C&S' safeguarding steps include:

- Only collecting PII when necessary;
- Storing PII in a safe and secure manner;
- Not providing PII to anyone (either inside or outside the company) who does not have a need to know it;
- Requiring that those to whom we do provide PII maintain adequate privacy protection policies and procedures themselves; and
- Implementing secure destruction of PII as appropriate.

Specifically with respect to Social Security numbers, C&S protects the confidentiality of Social Security numbers, prohibits the unlawful disclosure of Social Security numbers, and limits access to Social Security numbers.

The data security policies and procedures will be maintained and updated by the Compliance, Internal Audit and IT departments jointly. These departments will identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any records containing PII. Along with assessing risks, these departments will evaluate the effectiveness of current safeguards and means for detecting and preventing security system failures.

C&S employees must follow the Protection of Personal Information Policy relating to the storage, access, and transportation of records containing personal information outside the business premises.

If an employee violates C&S policies and procedures relating to information security, that employee will be subject to disciplinary measures as stated in the C&S Code of Conduct.

Terminated employees are prevented from accessing records containing personal information immediately upon notification of termination.

C&S oversees third party service providers and requires such providers to maintain security measures to protect personal information consistent with federal and state regulations. C&S inserts a data protection clause for material third party service providers' contracts where applicable.

All C&S employees shall follow the C&S Records Retention Policy to help limit physical access to records containing personal information and storage of such records/data. C&S performs ongoing inventories of records and securely destroys all records identified for destruction based upon the Records Retention Policy.

C&S regularly monitors its security program, through internal monitoring and periodic audits, to ensure it is operating

in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information. C&S also monitors regularly the use of its systems for unauthorized use of or access to PII according to the IT Internet Use Policy and the internal program.

In the event of a security breach, C&S shall take such steps as required by applicable federal and state laws.

C&S and its employees follow the IS Security Policy, which includes detailed information regarding the security system covering company computers. Secure user authentication protocols, including control of user IDs, assigning and selecting passwords, and restricted access to active users and active user accounts only must be in place.

If C&S must send records and files containing PII across public networks, such data is transmitted by either encryption or secured FTP. PII shall not be stored on laptops or other portable devices unless the employee is considered a “required user” and given permission to store such information. Where technically feasible, C&S will encrypt PII stored on laptops or otherwise prohibit storage on laptops.

C&S follows the Anti-Virus Update Process to ensure up-to-date firewall protection and operating system security patches to maintain the integrity of PII. C&S maintains up-to-date system security agent software including malware protection, patches and virus definitions, and updates on a regular basis.

C&S, at least annually, educates employees about PII, and how to protect PII through employee communications and updates to policies and procedures.