SUBJECT: PCI COMPLIANCE	ORIGINATING DEPT: SYSTEMS & TECHNOLOGY GROUP / TREASURY / LEGAL	SECTION: PRIVACY
DATE ISSUED: 01-15-09	SUPERSEDES: New	PAGE: 1 OF 2
INITIATED BY: STG / Treasury	APPROVED BY: Legal	

I. POLICY/PURPOSE

Protection of customer credit card information is important to Compass Group and its clients. Security of cardholder data is governed by the Payment Card Industry ("PCI") Security Standards Council. This Policy outlines the responsibility and standards related to protection of credit and debit card numbers and other customer information in accordance with PCI data security standards. All references to credit cards in this Policy are also applicable to debit card transactions.

II. ASSOCIATES COVERED BY THE POLICY

This Policy applies to all Company locations accepting credit or debit cards as a form of payment.

III. RESPONSIBILITY FOR ADMINISTRATION

The PCI Steering Committee and all levels of management.

IV. ENFORCEMENT

Non-compliance with this Policy is a security violation and will be reported to management. Depending on the severity of the infraction, a user may lose short term or permanent access to the system, and/or be subject to disciplinary action up to and including termination.

V. PROCEDURES

It is the Company's policy to comply with the security standards published by the PCI Security Standards Council. Company locations must follow the following data security standard:

1. Compass Group locations accepting credit cards must operate in a secure network environment.

a. Locations utilizing high-speed internet access must be secured by a Compass approved router and/or firewall. Wireless network configurations are considered high risk and shall be carefully evaluated. Isolated networks for the credit card processing application are preferred.

b. All anti-virus software must be up to date.

c. All log-in credentials should be unique.

d. Old copies of databases, spreadsheets, and other documents that contain credit card data are to be erased.

2. All new Compass locations accepting debit or credit card payments must utilize a PCI certified payment application, and all existing locations accepting debit or credit cards on a non-certified payment application (e.g. point of sale software, catering order software, cashless software) must be migrated to a PCI certified payment application by July 2010. New merchant identification numbers (MIDs) will not be issued to locations using a non-certified payment application.

3. No Compass Associate shall permit any alteration to a location's payment application or environment without first notifying ***creditcards@compass-usa.com*** for evaluation and approval**.**

4. All vendor agreements involving credit or debit card payments shall provide for the vendor to protect cardholder data in compliance with all applicable laws, regulations and PCI data security standards. In the vendor provides a credit or debit card payment solution, the vendor's solution must maintain certification with the PCI Security Standards Council.

5. Client agreements that involve locations in which the credit or debit card payment system interfaces or interconnects with a client system should include a provision that requires the client to reasonably cooperate with Compass to ensure Compass's compliance with PCI data security standards.