Exhibit C - Facility and Security Practices

Last Updated: February 28, 2010

Our Facility Practices

Physical Access

Your Hosted System will be located in a controlled access data center operated by SecureData or a SecureData affiliated company. Access to the Facility will be restricted to SecureData employees or its agents, or specifically authorized customer representatives who need access for the purpose of providing or maintaining their Services.

The data center will be staffed twenty-four (24) hours a day, three hundred sixty five (365) days a year and will be monitored by video surveillance. Entrance to the data center will be authorized by proximity-based access cards and biometric hand scanners or other SecureData-approved security authentication methods.

Fire Protection

The SecureData Facility will be maintained with fire protection measures in accordance with industry standards. Such measures shall, at a minimum, be compliant with requirements set by applicable city ordinances, building codes, and other applicable rules or ordinances related to safety and fire prevention.

Power Backup and UPS

SecureData shall be responsible for maintaining an uninterruptible power supply (UPS) system and backup generator system for the Facility in accordance with industry standards. Our generators will be tested regularly to ensure working operations, and our Facility power backup system will be exercised no fewer than 2 times per year.

Our Security Practices

SecureData Personnel

- SecureData will perform pre-employment background screening of its employees who have access to customers' accounts and Customer Equipment.
- SecureData will restrict the use of any applicable administrative access codes for customer accounts to its employees and other agents who need the access codes for the purpose of providing the Services. SecureData personnel who use access codes shall be required to log on using an assigned user name and password.

Reports of and Response to Security Breach.

If, at any time, SecureData becomes aware of any unauthorized access to your Hosted System, SecureData will promptly report to you such unauthorized access; and, upon

request, will provide to you access to information and documentation in our possession relevant to such event.

Network Security

Our network core provides passive intrusion detection and a robust firewall to assist with the protection of your systems and data. SecureData provides you with the option of routing your network traffic through our network core to obtain these additional levels of protection.

Security Protection

SecureData continually monitors our Facility to help ensure the safety and security of the Facility and the Customer Equipment within. If we become aware of a breach that compromises the safety and security of our Facility or its contents, we will provide you with notification as soon as reasonably possible. We will work diligently to resolve the breach and to minimize any further breaches in a reasonable manner consistent with industry practices.