Exhibit B - Facility Usage Policy

Last Updated: February 28, 2010

This Facility Usage Policy (FUP) is incorporated by reference in your SecureData Services Agreement with SecureData.

Please read this Facility Usage Policy carefully before using any SecureData Services. Use of SecureData Services by you is expressly conditioned on your acceptance of this FUP. If you do not agree with any part of this FUP, you should not use the Services.

SecureData reserves the right to modify the FUP at any time. Continued use of the Services by you constitutes your acceptance of any revisions to the FUP.

In accordance with the Services Agreement, violation of this FUP may result in suspension or termination of the Services.

Capitalized terms used in this Facility Usage Policy shall have the meaning given in the Services Agreement.

Inquiries regarding this policy should be directed to legal@securedata365.com.

Customer and Guest Access

You may access the SecureData Facility only in accordance with this Facility Usage Policy.

Access to SecureData's Facility is restricted to those individuals you specifically identify to SecureData as your approved list of representatives, agents, or assigns (collectively "Your Representatives"). You are responsible for any and all actions of Your Representatives and those of any authorized persons accompanying them. You are not permitted to grant to any unauthorized persons access SecureData's Facility. You will notify SecureData in writing of any changes to the list of Your Representatives.

Customer access is only permitted through the front entrance of the SecureData Facility. Your Representatives must sign-in and present a valid government-issued identification document for inspection and photocopy by SecureData personnel. Your Representatives must also wear a SecureData issued identification badge in a prominent and visible location during the duration of their visit to the Facility.

Access to the data center floor of the Facility is permitted only with an escort from an authorized SecureData representative, unless otherwise expressly authorized by SecureData.

At no time is Customer access permitted to other data center related facilities outside of the floor, including, but not limited to the power room, loading dock, network room, fire suppression facility, and elevator room.

You and Your Representatives agree to adhere at all times to security measures that have been established by SecureData to protect the Facility, its equipment, and its customers' equipment.

Customer Possessions

You and Your Representatives may not bring or make use of any of the following items while on SecureData property or in a SecureData Facility:

- Food, drink, or other liquids;
- Tobacco products, alcohol or other intoxicants, illegal drugs;
- Explosives, firearms, or other weapons;
- Chemicals;
- Electro-magnetic devices;
- Radioactive materials; or
- Photographic or recording equipment of any type.

Customer Equipment

Your Customer Equipment is subject to several restrictions while located at SecureData's Facility, including:

- All equipment must be clearly labeled with a SecureData provided customer code. SecureData will also install/attach a standard inventory label to all equipment. Equipment includes, but is not limited to, cables, power cords, displays, servers, routers, switches, patch panels, and other computer equipment;
- You may not alter any Customer Equipment except as specifically pre-approved in writing by an authorized SecureData representative per the then applicable SecureData Change Control Process. Such approval must be granted at least two (2) Business Days in advance of any change or alteration;
- At all times, Customer Equipment must be configured to run in compliance with the manufacturer specifications and SecureData requirements;
- At our sole discretion, and with our prior written permission, SecureData will make our Facility and/or equipment (e.g. tools, floor space, computing equipment, storage space etc.) available for your temporary use. This equipment and Facility is provided "AS IS", without warranties of any kind, and your use of the equipment and Facility is at your own risk.

Misconduct

You and Your Representatives may not:

- Mis-use or make any unauthorized use of any SecureData property or equipment;
- Make any unauthorized use of, or interfere with, the equipment of any other SecureData customer;
- Harass any individual, including, but not limited to, SecureData personnel, guests and representatives, representatives of any other Customer, or any other SecureData authorized individual; or
- Engage in any illegal or criminal activity.

Facility Procedures

You and Your representatives must adhere to our safety and security policies at all times while in our Facility. These policies include, but are not limited to, fire drills, evacuation planning, and other severe weather related processes.