# Exhibit A - Acceptable Use Policy

***Last Updated: February 28, 2010***

This Acceptable Use Policy (AUP) is incorporated by reference into your SecureData Services Agreement.

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

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

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

Capitalized terms used in this AUP shall have the meaning given in the Services Agreement.

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

### Monitoring

You acknowledge and agree that your use of SecureData's Services, and your compliance with the Services Agreement, is subject to physical and electronic monitoring by SecureData of any and all data that is transmitted using the SecureData network. Monitoring is also conducted for purposes of identifying and resolving security breaches, as well as for general system administration.

You acknowledge and agree that SecureData has the right to disclose results from its monitoring activities:

- when it is legally required, such as in response to a subpoena or law enforcement investigation,
- to protect itself or its customers (as determined by SecureData in its sole discretion); and/or
- as otherwise required by law.

### Lawful Use

SecureData Services may only be used for lawful purposes and consistent with all rights of other parties. Without limiting the foregoing, our Services shall not be used in a manner which would violate any law or infringe any copyright, trademark, trade secret, right of publicity, privacy right, or any other right of any third person or entity, for the purpose of transmitting or storing of content or data which is obscene, libelous, defamatory, or considered "Offensive Content" under this AUP.

Use of or access to other networks through SecureData must comply with the rules, regulations, terms, policies and/or conditions established by such other networks.

### Abuse

You may not use SecureData's network or Services to engage in, foster, or promote illegal, unauthorized, abusive, or irresponsible behavior, including:

- Unauthorized access to or use of third party data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures, without express authorization of the owner of the system or network;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Use of programs or methods which compromise the security of any system or device on the SecureData network or any external network, or attempt to bring about a denial of service or other negative impact of any form of service on our network or any external network.
- Interference with service to any user of the SecureData or other network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks; or
- Any conduct that is likely to result in retaliation against the SecureData network or website, or SecureData's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

### Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of a SecureData system or network or to breach SecureData's security or authentication measures, whether by passive or intrusive techniques, without SecureData's express written consent.

### System Security

Users are prohibited from violating or attempting to violate the security of SecureData Services, including without limitation:

- Accessing data not intended for your use;
- Impersonating SecureData personnel;
- Attempting to probe, scan or test the vulnerability of the SecureData network or to breach security or authentication measures without proper authorization;
- Attempting to interfere with, disrupt, or disable service to any user, system, or network by any means;
- Taking action in order to obtain Services to which you are not entitled;
- Attempting any action designed to circumvent or alter any method of measuring or billing for SecureData Services.

Violations of system or network security may result in civil or criminal liability. SecureData will investigate alleged violations and may involve, and cooperate with, law enforcement authorities in prosecuting Users who are involved in such violations.

### Offensive Content

You may not publish, transmit or store on or via SecureData's network and equipment any content or links to any content that SecureData reasonably believes:

- Constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, or non-consensual sex acts;

- is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
- contains a virus, trojan horse, worm, time bomb or other component that may adversely affect any hardware or software, or that intercepts or expropriates any data or information;
- is unfair or deceptive under the consumer protection laws of any jurisdiction;
- is defamatory or violates a person's privacy;
- creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- is intended to assist others in defeating technical copyright protections;
- infringes on another person's copyright, trade or service mark, patent, or other intellectual property right;
- promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking;
- constitutes illegal SPAM;
- is malicious, fraudulent, or may result in retaliation against SecureData by offended viewers; or
- is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to SecureData.

Content "published or transmitted" via SecureData's network or equipment includes any data, including audio and video, and any other type of posting or transmission that relies on the Internet.

### Changes to Service

The SecureData Services are expected to change from time to time as technology changes and systems are upgraded. SecureData reserves the right to change any Service offered or the features of any Service offered on its network without notice, including changes to access and use procedures and all system hardware and software.

### Affect on SLA

No credit will be available under your SecureData Service Level Agreement, nor will SecureData incur any liability, for interruptions of service resulting from AUP violations by you.

### Investigations

We agree to reasonably cooperate with any reasonable investigation request by or on behalf of you or your insurers, relating to any loss, damage, destruction, or unauthorized use by a third party of your Hosted System. We also agree to reasonably cooperate with you in any litigation or prosecution against a third party arising in connection with any loss, damage, destruction, or unauthorized use by a third party of your Hosted System. You agree to reimburse SecureData for any reasonable out-of-pocket expenses associated with SecureData’s cooperation with any such investigation, unless it is determined that the loss was the sole responsibility of SecureData under the Services Agreement.