INTEGRAL AD SCIENCE, INC.

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

When processing personal data which is subject to European Data Protection Law (as defined in the agreement between IAS and a Customer which incorporate these measures, the "**Agreement**"), IAS shall exercise appropriate security controls and measures to manage and protect personal data in its possession from unauthorized or unlawful access, use, alteration, disclosure, distribution, loss, destruction or damage.

In general, IAS has implemented technical and security measures that include, but are not limited to:

(a) treating and safeguarding personal data as strictly private and confidential and taking all steps necessary to preserve such confidentiality both during and after the termination of the Agreement;

(b) making personal data available to IAS's employees and/or agents strictly on a 'need to know' basis and by training and requiring IAS's employees, who are involved in the processing of personal data, that they shall not collect, process or use personal data without authorization and that they shall keep personal data confidential, during and after termination of their activity;

(c) using, copying, reproducing or distributing personal data only for the purpose(s) set out in the Agreement or otherwise as permitted by applicable laws and not for any other purposes;

(d) minimizing, to the fullest extent possible, the disclosure of personal data to third parties (such disclosure shall be strictly necessary to enable IAS to discharge IAS's obligations to Customer under the Agreement); and

(e) using reasonable encryption methods for securely storing personal data according to its sensitivity and proportional to the risk that the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.

In addition, IAS has implemented the following technical and organizational measures:

1. Physical access control

These measures are designed to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, and include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

These measures are designed to prevent data processing systems from being used by unauthorized persons and include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of **one** master record per user, user master data procedures, per data processing environment;
- Encryption of archived data media.

3. Data access control

These measures are designed to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, and include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

These measures are designed to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic) and that it can be verified to which companies or other legal entities Personal Data are disclosed, and include:

- Encryption/tunnelling;
- Logging;
- Transport security;
- Due diligence process to ensure that any companies or other legal entities which receive personal data can comply with data protection obligations.

5. Entry control

These measures are designed to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, and include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

These measures are designed to ensure that, where IAS acts as a processor, personal data are processed solely in accordance with the instructions of the controller, and include:

- Unambiguous wording of the contract;
- Formal commissioning (request form/statement of work);
- Criteria for selecting any sub-processor.

- Due diligence process to ensure that any sub-processors provide sufficient guarantees that they can comply with their obligations.

7. Availability control

These measures are designed to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) and include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

These measures are designed to ensure that Personal Data collected for different purposes can be processed separately and include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

9. Security Incident Management

- Procedures to identify actual or suspected security incidents;
- Notifying Customers of any confirmed personal data breach (as defined in the Standard Data Protection Terms);
- Security incident management plan in place;
- Co-operation with Customers and governmental authorities, as applicable, in relation to management of security incidents.