EXHIBIT S

UNIVERSITY AT ALBANY, SUNY
SECURITY, NON-DISCLOSURE AND CONFIDENTIALITY

The Contractor shall maintain the security, nondisclosure and confidentiality of all information in accordance with the following clauses in performance of its activities under the Contract. Contractor shall ensure that its personnel, agents, officers and subcontractors, if any, are fully aware of the obligations arising under this Exhibit and shall take all commercially reasonable steps to ensure compliance. The Contract may be terminated by the University for cause for a material breach of this Exhibit.

A. Security Procedures:

Contractor warrants, covenants and represents that it shall comply fully with all security procedures and policies of the University, which procedures and policies are communicated to the Contractor by the University during the performance of the Contract. Contractor shall hold the University harmless from any loss or damage to the University resulting from the violation of such security procedures or policies by the Contractor, its officers, agents, employees, and subcontractors.

The Contractor shall comply with the following specific security procedures:

1. Data Access – The Contractor must ensure that all data related to this project is stored in a controlled access environment to ensure data security and integrity. All facilities proposed for use must have adequate security systems in place to protect against the unauthorized access to the facilities and data stored therein. Adequate security systems must be in place to control access into the facilities. Access into and within the facilities must be restricted through an access control system that requires positive identification of authorized individuals as well as maintains a log of all accesses (e.g., date, time, who). The Contractor shall have a formal procedure in place for granting computer system access to the data and to track access by its own employees. Access for projects outside of those approved by the University is strictly prohibited.

2. Location of Data – Unless otherwise noted in the contract, all University data exchanged with the Contractor must be stored, housed, processed, backed-up, archived and otherwise retained on systems physically located in the continental United States. This requirement extends to any subcontractors of data storage service.

3. Data Exchange – Except as otherwise stipulated in the contract, Contractor shall make arrangements to receive or exchange all University supplied or designated electronic information via the University's systems of record. University information in other formats must be exchanged via an official contact identified in the contract.

4. Physical Transport of Data – The Contractor shall use reputable means to transport data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the University.

5. Electronic Transport of Data – The Contractor shall use reliable means of electronically transferring data between the University and its offices and facilities. Such means must assure the confidentiality and integrity of the data while in transit.

6. Data Protection – The Contractor shall use appropriate means to preserve and protect the University data. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. The Contractor shall encrypt data identified by the University, as requiring encryption and it shall use encryption methods that have Federal Information Processing Standard (FIPS) 140 validation.

7. Data Destruction – At the end of this contract, the Contractor shall employ the technical measures necessary to assure the secure, irreversible erasure or destruction of all data storage formats to eliminate any and all data collected or generated by the Contractor and/or provided by the University unless explicit provisions for the retention of some data sets have been stipulated in the contract. The destruction process must receive written approval by the University.

8. Return of Data – Upon written request of the University, at any time during the term and upon expiration or termination of the contract, the Contractor shall promptly return to the University, in the format and on the media requested by the University, all or any part of University data collected during the term of the contract.

9. Data Breach Notification – In addition to Section D below, Contractor agrees that it shall immediately report to the University the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information [See Section B: Nondisclosure and Confidentiality] directly to the University.

The terms of this section shall apply equally to Contractor, its agents and subcontractors, if any. Contractor agrees that all subcontractors, if any, and agents shall be made aware of and shall be made contractually bound to the terms of this section.

Upon request by the University, Contractor may be asked to provide a recent independent audit report on security controls. The University shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the
facilities and operations used in the performance of any work under the Contract. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be non-compliant with Contract safeguards.

B. Nondisclosure and Confidentiality

Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its officers, agents, employees, and subcontractors, if any, shall maintain strict confidence with respect to any Confidential Information to which the Contractor, its officers, agents, employees, and subcontractors, if any, have access. This representation shall survive termination of the Contract. For purposes of the Contract, all University information of which Contractor, its officers, agents, employees, and subcontractors, if any, becomes aware during the course of performing Services for the University shall be deemed to be Confidential Information (oral, visual or written, in paper, electronic or any other format). Notwithstanding the foregoing, information that falls into any of the following categories shall not be considered Confidential Information:

1. information that is previously rightfully known to the receiving party without restriction on disclosure;
2. information that becomes, from no act or failure to act on the part of the receiving party, generally known in the relevant industry or is in the public domain; and
3. information that is independently developed by Contractor without use of Confidential Information of the University.

Contractor shall hold the University harmless, without limitation, from any loss or damage to the University resulting from the disclosure by the Contractor, its officers, agents, employees, and subcontractors of such Confidential Information.

C. Federal or State Requirements

In the event that it becomes necessary for Contractor to receive Confidential Information, which Federal or State statute or regulation prohibits from disclosure, Contractor hereby agrees to return or destroy all such Confidential Information that has been received from the University when the purpose that necessitated its receipt by Contractor has been completed. In addition, Contractor agrees not to retain any Confidential Information which Federal or State statute or regulation prohibits from disclosure after termination of the Contract.

Notwithstanding the foregoing, if the return or destruction of the Confidential Information is not feasible, Contractor agrees to extend the protections of the Contract for as long as necessary to protect the Confidential Information and to limit any further use of disclosure of that Confidential Information. If Contractor elects to destroy Confidential Information, it shall use reasonable efforts to achieve the same and notify the University accordingly. Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of Confidential Information, which Federal or State statute or regulation prohibits from disclosure.

Contractor agrees that it shall immediately report to the University the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information directly to the University. The terms of this section shall apply equally to Contractor, its agents and subcontractors, if any. Contractor agrees that all subcontractors, if any, and agents shall be made aware of and shall be bound contractually to the terms of this section.

D. Information Security Breach and Notification Act

In accordance with the Information Security Breach and Notification Act (ISBNA) (General Business Law, §899-aa; State Technology Law, §208), Contractor shall be responsible for complying with the provisions of the ISBNA and the following terms contained herein with respect to any private information (as defined in ISBNA) received by Contractor under this Contract (Private Information) that is within the control of the Contractor either on the University’s information security systems or the Contractor’s information security systems (System). In the event of a breach of the security of the System (as defined by ISBNA) Contractor shall immediately commence an investigation, in cooperation with the University, to determine the scope of the breach and restore the security of the System to prevent any further breaches. Contractor shall also notify the University of any breach of the security of the System immediately following discovery of such breach. Except as otherwise instructed by University, Contractor shall, to the fullest extent possible, first consult with and receive authorization from University prior to notifying any individuals, the State Consumer Protection Board, the Office of the Attorney General (OAG) or any consumer reporting agencies of a breach of the security of the System or concerning any determination to delay notification due to law enforcement investigations. Contractor shall be responsible for providing the notice to all such required recipients and for all costs associated with providing such notice. Nothing herein shall in any way impair the authority of the OAG to bring an action against Contractor to enforce the provisions of ISBNA or limit Contractor’s liability for any violations of the ISBNA.