EXHIBIT "E"

DATA SECURITY REQUIREMENTS

Provider will, at a minimum, implement the following types of security measures:

A. Physical access control

Technical and organizational measures 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 Student Data are Processed*, 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.);
- Surveillance facilities, video/CCTV monitor, alarm system; and

*Note: Student Data is stored at our Service Provider - currently AWS - and the above applies to their technical and organizational measures. In addition, we secure decentralized data processing equipment and personal computers.

B. Virtual access control

Technical and organizational measures to prevent data processing systems used for Student Data from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password); and
- Encryption of archived data media.

C. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Student Data in accordance with their access rights, and that Student Data cannot be read, copied, modified or deleted without authorization, 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;