CASSIE The Consortium for the Analysis of Student Success through International Education

Data Privacy and Security Overview[1]

CASSIE is led by the University System of Georgia (USG) in coordination with the Institute of International Education and funded by the U.S. Department of Education's International and Foreign Language Education Office. It is a research project to study the impact of international education experiences (e.g. study abroad, taking a foreign language, Title VI program participation) on a variety of student success outcomes.

The project will create a database in the USG data warehouse of de-identified student-level data from both USG and non-USG colleges and universities that includes information on student demographics, academic characteristics, international experiences, and educational outcomes. The USG data warehouse currently securely stores student data for the 26 institutions of the USG and grants access to designated role-based users. Data are not stored on local devices or within computer tools/applications.

Data security is foundational to CASSIE and will be assured through the following operational processes and technical, physical, and administrative cybersecurity safeguards:

- USG data warehouse personnel will utilize current warehouse loading, storage, and access procedures and technologies to provide services for the CASSIE project.
- Data are stored in an Oracle 12.1.02 database managed and monitored with Oracle Enterprise Manager 13C.
- The database is protected by a next-generation Palo Alto firewall that allows connections only to defined and authorized IP address ranges.
- Individuals (no shared accounts) access the warehouse with Active Directory accounts associated with designated role-based security. All accounts are re-certified on an annual basis.
- Oracle Transparent Database Encryption (TDE) is used to encrypt all sensitive data at the database table level.
- Oracle SQLNET Encrypted connections are used and required to encrypt all data during transport across the network.
- The USG environment is actively being monitored by the enterprise security operations center.
- The data warehouse is protected through enterprise backup and recovery operations.
- The data are physically protected in a secure data center using biometric controls to restrict access to only authorized personnel.
- Protection of sensitive data is fostered through administrative controls in the form of comprehensive actions, policies, and procedures.

Transmission of datasets from participating institutions will be carried out by the USG's secure file transfer utility system, MoveIT. Secure access to the CASSIE databank is in place through Toad database administration software. Statistical analyses will be carried out via STATA and SPSS software.

[1] Prepared by USG Information Technology Services personnel Alfred Barker, Assistant Vice Chancellor and Chief Information Security Officer, with contributions from Dr. Gregory Shutz, Assistant Vice Chancellor for Strategic Business Intelligence, and Greg Turmel, Director Data Warehouse.