As described by the U.S. Department of Education's Privacy Technical Assistance Center, it is imperative that any computer-based product establish and maintain **rigorous security processes** to protect privacy and confidentiality.[113] As with our current SEL games, the proposed software will be FERPA-, COPPA-, and HIPAA-compliant and meet the strictest data security standards, including compliance with Title 21 Code of Federal Regulations Part 11. Protected sections will be encrypted during transmission using strong 256-bit SSL transport layer security and trusted certificates for both browser and mobile access. No protected information will be stored on local devices; all data will be housed on our multi-server cloud environment with two independent backup systems and protected using best practice algorithms for sensitive data, including 3DES encryption and separation of encrypted data from keys. Globally Unique Identifiers (GUID) with expiration schedules consistent with government industry standards will be used for all accounts.

To ensure the security, privacy, and confidentiality of data entered into the software system, several physical, network, hardware, and software safety precautions are in place. For example, access to servers requires a special password known only to IT staff involved in launching and capturing data. In addition, the firewall restricts access to these data from outside of 3C's offices. Lastly, 3C uses SSL encryption for data entry pages during transmission.

Lastly, access to the computer network is restricted to staff with valid usernames and passwords. Individual network and database passwords are changed on a regular basis. All staff members are trained to close password-protected applications or lock their workstations when they are away from their desks.