Data and Functional Security

Area of Concentration	LinkIt! Current State
Business Application Security	In 2016, a third party firm was engaged to conduct penetration testing on the LinkIt! platform (Administrative Portal, Student Test Taker). At the conclusion of the testing, additional safeguards were implemented to enhance security.
Policies & Procedures	Two independent third party vendors conducted ISO 27001/2 pre-certification audits to assist LinkIt! in the pursuit of full ISO 27001 certification. The policies and supporting documentation used to prepare for and satisfy these audits can be made available upon request.
Information Gathering	Information leakage of technologies used by the web application is avoided in order to reduce possible attacks.
Configuration Management	The application hosting environment is patched to the latest version on a periodic basis.
Identity Management	Complex user credentials to protect and prevent discovery and exploitation of user identities are enforced through the LinkIt! platform.
Authentication	Rigorous requirements are in place to prevent brute force and other malicious attacks (including industry standard password reset rules and CAPTCHA).
Authorization	Enforce rigorous entitlement policies defined by the customer so only authenticated users can securely access specific data and functionality associated with the role in the district.
Session Management	Control session information to prevent unauthorized access to data or functions.
Cryptography	Restrict use of outdated and insecure internet protocols, including but not limited to file and data transmissions.
Business Logic	Restrict file types which can be uploaded or downloaded on the LinkIt! platform and restrict storage and access to these files to protect against attacks.
Client Side Experience	Prevent client side unauthorized access to data and functionality via known exploits (hacks).