

Overview of Administrative Security Controls - Supplement I.

Rigorous Security

Pearson systems and components employ the appropriate protocols and design features necessary to neutralize known threats.

- **Component-to-component** – All sensitive communication between application components that crosses the Internet is encrypted using SSL/TLS. This does not apply to assessment item content delivery, because these are encrypted as described below; the different method is required to enable proctor caching, which many customers opt to use to reduce their overall bandwidth requirements.
- **User authentication and authorization** – Users are only created when there is a business need and are granted a user role in the system based on job requirements. User accounts are only authorized to access the data specific to their role and organization. Users are removed as part of Pearson's overall Termination Process initiated by our Human Resources policy.
- **Assessment item-level security** – When a test is marked "secure" during publishing, each individual item is encrypted using AES and a 128-bit key. Test items remain encrypted until they are downloaded to the TestNav client, decrypted, and presented to the student during testing.
- **Student response and score data security** – Student responses are encrypted using an AES 256-bit key. Score data are communicated between components using SSL/TLS.
- **Data storage** – Database backups are AES encrypted using a 256-bit key using Amazon's S3 Server Side Encryption functionality.

Overall Approach to Security

Whether the setting is one with high capacity or low capacity, Pearson's overall approach to security involves several facets:

- **Security and audit management** – Pearson undergoes regular audits from both our internal corporate audit function as well as third-party audits from companies like PriceWaterhouseCoopers and Deloitte. Identified gaps are inserted into our Information Security Management System (ISMS) where a remediation plan is identified, responsibilities are assigned, milestones are created, and follow-up documentation is stored. This allows for the necessary visibility at all levels of the business and mitigates gaps, reducing or eliminating risks.
- **Update processes** – Pearson calls this "change management," which is the process of managing changes to optimize risk mitigation, minimize the severity of any known impact, and to be successful on the first attempt. This includes additions, modifications, and removals of authorized components of services and their associated documentation. The process includes raising and recording changes; assessing the impact, the cost, the benefit, and the risk of proposed changes; obtaining approval(s); managing and coordinating the implementation of changes; and reviewing and closing requests for change.
- **System behavior monitoring** – Both during test-taking and at other times, Pearson monitors for anomalous activity throughout the entire system, not just at the application layer. Special care is taken during student testing. Should activity trigger one of our behavior alerts, the test is halted and the proctor is alerted. Our system monitors may be triggered, which will generate an alert to the appropriate team for further investigation.
- **Compliance with state policies** – Pearson will comply with all reasonable policies.

- **Features that prevent infiltration** – Pearson employs several methods to mitigate the risk of uninvited access to our systems. All external traffic is encrypted. All item content payloads are encrypted end-to-end using AES-128. All student responses are encrypted using AES-256, using a different key than the content payloads. Students receive a one-time password to take a test. Account and password controls meet accepted standards for length, complexity, lockout, re-use, expiration, and so on.

TestNav Security

A high-stakes, large-scale assessment like PARCC requires specific software features to protect data from threats both inside and outside the testing location. These standards and protocols are designed to thwart anyone seeking to steal test content or personal data, as well as test-takers trying to gain an unfair advantage. The primary method of stopping external threats is encryption of data, while test security is accomplished by “locking down” the computer from unauthorized activity.

Data Security

Pearson's vigilance in securing the online testing environment will provide PARCC with the confidence that Pearson will protect the integrity of each student's test and the confidentiality of each item's content. We use AES encryption and HTTPS to provide encryption and security for online testing by creating a secure channel on the network with the Secure Socket Layer (SSL) protocol.

Test Security

The TestNav system requires just a standard browser and uses existing security features to put the testing computer in "lockdown" mode, also known as "kiosk mode".

While using TestNav, PARCC students cannot print, cut, or copy test content. If a student tries to access the desktop or any other application, TestNav prevents moving, minimizing, or resizing the window in order to use any functions other than testing. They cannot open another browser, visit websites, or access other installed resources, such as a thesaurus, spellchecker, or encyclopedia that isn't approved for use during the test. Using key combinations to switch applications, such as ALT+TAB or CTRL+ESC, returns a warning that leaving TestNav will terminate the test. Once a student exits a test, he or she cannot return to the test without intervention by the test administrator.

PARCC test administrators control authorization of individual students by printing and distributing test tickets with each student's information and a unique URL. The student enters the URL in a browser window on the testing workstation to gain access to the test. Administrative user IDs and passwords do not provide access to test content. Only an authorized TestNav session, accessed with a specific student's test ticket, will provide access to PARCC.

PearsonAccess Tasks and Data

PARCC educators will have access to information and tasks that are appropriate for their individual PARCC duties. PearsonAccess provides administrators with a rules-based system of permissions by role, so users can perform their assigned duties and access appropriate data -- and only their assigned duties and data. Without a hierarchical permissions system, data are at greater risk of accidental damage or exposure.

To manage each user's access to sensitive data, PARCC will use PearsonAccess to establish a hierarchy of user roles. After the top level of PARCC users is established, they can authorize state and district users to grant permissions to personnel who are lower in the hierarchy. Thus each level of users oversees the roles of the users below them. PARCC can specify:

- The organizations that each user level and role can access, from statewide down to a specific school.
- Each user role's access to functional areas, such as enrollments, student data management, order tracking, and viewing reports.
- The data that each user role can access, edit, modify, and delete.

For example, PARCC might specify that users with the School Administrator role are authorized to edit and delete data, while the Teacher role might enable the user only to view data. Checkboxes allow for easy selection of user permissions, and the changes are effective throughout the system, immediately after saving them.

Authentication and Authorization

PARCC data will be guarded by the PearsonAccess security module, which restricts access based on the user's role and level in the hierarchy. Each authorized user has a unique ID and must create a secure password after agreeing to a confidentiality agreement that PARCC will review in advance.