ABOUT ITP ONLINE TOOLS

ITP Online Tools is a site for Iowa school personnel. The functionality on this site includes: Registration and Orders for Scoring Services; eITP interactive reporting; and IBCV bar code submission and validation.

ITP STUDENT DATA CONFIDENTIALITY

ITP (and the University of Iowa) are subject to and adhere to the Family Educational Rights and Privacy Act, or FERPA. All educational records and all information concerning student names, performance information, test results, test results analyses and any other student or school-identifying information and personal data belong to the customer; deemed to be the Superintendent of a public school district, or the person holding an equivalent position in a private school (e.g. Dean, Chancellor, Executive, Headmaster). Iowa Testing Programs (ITP) will keep the customer information confidential and customer information will not be disclosed in any manner, in whole or part, by ITP or by its officers, directors, partners, employees, affiliates, agents, subcontractors, or representatives unless specifically provided for by written consent and approval.

ITP TECHNICAL OVERVIEW

ITP and our vendors take all reasonable precautions to protect information and data, both paper-based and digital. We use the latest software protection and encryption techniques to protect our customers' data and meet regulatory compliance.

All of our sites are hosted on a secure, encrypted server. Our Database server meets the highest security standards for data integrity and related processes. This includes maintaining restricted physical access to the data center and other sensitive areas; logical authentication and access to networks, programs, and data; monitoring to proactively identify and fix system vulnerabilities; and systems implementation to ensure infrastructure changes are accurate and logged.

Physical Security

All production servers are hosted at a secure hosting facility and physical access is limited to approved personnel only.

Restricted Access

ITP has created and maintains a set of roles to access its website. Access to various areas of the site is restricted based on a user's assigned roles. What users are able to view, and actions they can perform, are determined by the roles to which they are assigned. Local user roles and access privileges may be updated or revoked at any time by the district Superintendent (or equivalent).

Login

Only Iowa school personnel are eligible to have a user account. Users are assigned unique ITP usernames and password to access our sites. Upon successful log in, a cookie is placed on the local computer to keep the user logged in for the next 60 minutes. After 60 minutes of inactivity, users are automatically logged out of the site. This is a rolling expiration. (Note: Users must have enabled cookies in the browser to use any secure ITP site.)

Data Security

As all our sites are hosted on a secure, encrypted server, every attempt has been made to maintain the security of our site/data as well. Users can help maintain the security of their district's data by observing the following:

- Never write ITP passwords down in a non-secure location.
- Never reveal passwords to anyone or share login information with others.
- Change passwords on a regular basis (at least yearly).
- Use passwords with at least 9 characters, and a mixture of letters, numbers, and symbols.
- Always use the "Log Off" link when the session is completed and close the browser.

Operating System

ITP recognizes that the data in our system is of immense value to customers. To ensure that our customers' data is safe not only during day-to-day operations but also during releases of updates to the application, we ensure that all update and maintenance procedures meet the highest standards of quality.

Software Updates

We regularly patch our software to ensure our operating systems and any other software running on our servers contain the latest security patches.

Permissions and Privileges

Only personnel with the appropriate authority will have controlled access to the application and data file servers. This is enforced through the use of permissions, passwords, and unique IDs.

Monitoring and Anti-Virus

System Center Endpoint Protection® is used to monitor and protect both our servers and the local computers used to access student data. This software expands our operation visibility with delivery of a more effective IT security standard on all ITP servers that protect our systems from the following:

- Ensures complete protection against all known malware, including viruses, Trojans, rootkits, spyware, and adware.
- Provides additional layers of defense against zero-day malware through sandboxing and exploit detection technology.
- Provides granular settings to ensure endpoint performance and user productivity is not impacted by anti-virus scans.
- Delivers a scalable and efficient defense against well-known and fast-spreading malware.
- Application role level security.

- ITP will work with schools to ensure that the appropriate level of access for an individual role is configured (for example, ensuring teachers can only see their assigned student data or administrators at a school level can only access data pertaining to their school.)

Only ITP employees who need the information to perform a specific job are granted access to personally-identifying information and data, and all certify annually that they will adhere to FERPA regulations while handling such data.

Network-Intrusion Detection and Prevention

All traffic is carried on secure VLANs, passing through a firewall to access physical networks.

Firewall Services

Each server and person who access the data has their own dedicated firewall appliance.

File Integrity Services

Our partnered vendors securely access files from us.

Please direct any concerns to David Henkhaus, Director of Operations, Iowa Testing Programs at david-henkhaus@uiowa.edu.