Review360 is a Pearson hosted application. Following is information pertinent to its technical requirements, data security, network security, facility security, data center security, disaster recovery processes, server security, and backup & recovery processes.

Review360 Technical Requirements

Computer Requirements

Review360 is a web-based application. To access and use Review360, a user's computer must meet the following requirements:

Operating Systems

- Windows 98, 2000, XP, Vista, 7, or 8 (XP or Higher Recommended)
- MAC OS X Tiger, Leopard, Snow Leopard, Lion, or Mountain Lion (Leopard or Higher Recommended)

Internet Browsers

- Internet Explorer 7 or above
- Google Chrome (Any Version)
- Safari 4 and above
- Android 2.2 and above (Safari or Chrome)
- iOS 4.0 and above (Safari or Chrome)

An Internet Connection

- A high-speed Internet connection is recommended.

512 MB of memory (RAM)

- 1 GB of memory or more is recommended.

Cookies and JavaScript Enabled

Additional Notes

- District network should allow for all e-mails from the domain psiwaresolutions.com to be allowed through.

Data Security

Encryption

Pearson utilizes encryption protocols in many of its standard services, and can provide specific solutions based upon program requirements. Some of the more relevant uses of encryption would be:

- **Secure FTP** – for encrypting sensitive data between our customers and Pearson
- **HTTPS** – Secure Socket Layer (SSL) encryption on websites to protect all user transactions
- **Encrypted Backup Tapes** – All backup tapes generated for offsite storage are encrypted using hardware layer encryption to prevent data exposure through loss or theft of offsite media
- **Virtual Private Networks (VPN)** – for secure remote access to the Pearson network, and for secure point-to-point network connections when necessary.
- **Database Encryption** – to protect data at rest from unauthorized access

Working with our customers, Pearson can provide the technical resources necessary to implement the correct encryption protocol for any customer data.

Data Destruction/Chain of Custody

Two critical components of end-to-end data security are proper disposal of data at end-of-life, and secure transfer of media containing sensitive data in circumstances where the data cannot be removed. Pearson provides policy guidance through the Electronic Media Disposal Policy, which is implemented with specific processes for degaussing all media before it is removed from secure Pearson Technology locations, such as the Iowa City Data Center. In the instances when systems or media must be transported with data still resident, a strict chain of custody process is followed to assure proper handling and protection of all data. This process requires written signatures at each stage of the transfer process, as well as acknowledgement of the Data Security Officer.

Network Security

Firewalls/Intrusion Prevention System (IPS)

The internal Pearson network is isolated from the public Internet by a layered firewall approach that creates a secure LAN environment, with web, application, and database DMZs for publicly accessible services. Stateful, packet inspection firewall devices are used, with only business required ports and protocols enabled across the network boundaries. All firewall traffic also traverses an in-line IDS\IPS system to protect against network based attacks, such as Denial of Service (DOS), and other known malicious traffic (See Vulnerability Management). Internal LAN segments are structured to optimize performance as well as controlled access.

Facility Security

Access Controls

All Pearson facilities are secure, and closed to the general public. Physical access to each facility is controlled by an access card reading system. Employees are required to wear a company-issued photo ID badge. This Security Identification Badge is to be worn in unobstructed view at all times on the front upper part of the body on outer clothing. Pearson employees are required to sign a statement regarding proper badge usage when receiving a new or updated security badge. All facility's entrances are monitored actively by security officers, receptionist staff, or via closed circuit television (CCTV) systems.

Further access to restricted areas such as the Iowa City Data Center requires additional authorization, which is both programmed into the employee's badge and illustrated on the badge. Access is pre-approved on a business need basis by the authorized manager.

Visitors may only enter Pearson facilities at designated entrances. Manager authorization is required for visitors, and they must remain under the control and escort of an authorized employee. Visitor badges must be worn in unobstructed view (same requirement as employees). Escorts are required to communicate visitor responsibilities to the visitor.

Monitoring

Closed-circuit TV cameras monitor all entrances, and uniformed guards regularly patrol the premises 24 hours-a-day.

Data Center Security

Pearson's core IT infrastructure resides in the Iowa City Data Center. Access to the Data Center is strictly controlled and managed. If an employee has a business need to access the Data Center, the employee's manager must complete a request for extended access. The employee's manager, the Pearson Administrative Services manager, and the Data Center manager must sign the completed form before access can be granted. To enter, an individual must pass through three access card readers, with separate authorization required for access at each level.

Physical and environmental protection controls in place include:

- Card key access for building and work area entrances
- Twenty-four hour security officer coverage: (Note: Coverage is for entire North Dodge facility and is not specific to the Data Center)
- Raised floor in Data Center, to protect against water damage
- Dedicated, redundant cooling system with humidity control
- Conventional raised floor
- Emergency lighting in Data Center
- Fire extinguishers rated for electrical fires
- B/C rated fire extinguisher
- Smoke, water, and heat detectors
- Emergency power-off switch by exit door
- Surge suppressor
- Zoned dry pipe sprinkler system and chemical fire suppression system
- Uninterrupted power supply for all equipment
- Power strip/suppressors for peripherals
- Power strip/suppressors for computers

Significant system improvements in 2008 include a mainframe upgrade that supports hardware-level encryption. Time-tested mainframe technology gives us extraordinary capacity and computing power, and provides additional security benefits for sensitive student information.

Physical Structure

The Iowa City Data Center is independent of the main facility except for a passage link. This passage link seals off the passage from the main facility in the case of a fire. If a fire occurs in either facility, the fire alarm automatically causes two-hour-fire-rated steel doors to close. These steel doors are spring-loaded and held open electromagnetically. The doors also close automatically in the event of a power failure due to a loss of current to the electromagnets.

The Data Center is at an elevation of 23.1 ft. above the 500-year flood plain of the nearest waterway, thus protecting the facility from natural flood. The building is located on a sloping hill; water runoff during periods of heavy rain is rapid and complete. The under floor is protected by a continuous-from-center sloped sub floor with multiple drains positioned at the four corners of the facility. In addition, a corner sump pump provides a second level of protection.

Iowa is located in Zone 1 of the Seismic Risk Map of the United States. Zone 1 is defined as an area where distant earthquakes can cause minor damage to poorly designed structures. The Data Center meets building code requirements for earthquake resistance for a Zone 1 structure.

Iowa has an average of 4.5 tornadoes per 10,000 square miles per year. Damage assessments by cooperating federal and state governments estimate the strongest tornado winds to be approximately 150 mph. The Data Center was designed and constructed of poured-in-place steel-reinforced concrete specifically to protect against the positive and negative air pressures from winds exceeding 150 mph. In addition, the Data Center facility has no windows and each door is specifically designed with 3-point latches to guard against these significant wind pressures.

Access Controls

Pearson applications are served from a data center that is physically secure. Access to the data center is restricted to a controlled list of Pearson staff and key vendors. Access requests are reviewed and pre-approved by the Data Center operations manager on a case-by-case basis. Verbal requests made through the network operations center are authenticated against a contact list to verify that they are authorized to make the request.

Any digital connections to the data center are authenticated using digital encryption and one-time passwords to verify that only authorized users are granted remote access. Our host data center has fully redundant power supplies as well as UPS backups and diesel generators. Multiple carriers provide network connectivity at multiple points of demarcation to isolate the data center from issues associated with a single provider.

Monitoring

We monitor Pearson systems seven days per week, 24 hours-a-day. Our staff continually collects and analyzes metrics indicative of capacity and performance from the end-user perspective. Our monitors will cover the operating systems, applications, databases, and networks, and automatically notify staff when performance thresholds are exceeded. This allows the staff to proactively address problems before the end-user is impacted.

In the event that the load on the system impacts performance or assessed capacity of the system, each tier in the architecture is scalable, allowing additional capacity to be added to the system to alleviate any performance constraints.

Fire Suppression

Fire detection in the facility consists of ceiling and under-floor detectors of optimum type, spacing, and cross zoning to recognize early, reliable fire detection. Detectors are linked to an alarm control and building map display that provides specific detector operation location so fires can be located rapidly.

The detection system sounds an audible alarm, flashes a visual building-wide alarm, readies the fire suppression system, and charges the sprinkler system with water. To allow data center personnel time to determine the cause of the alarm and either abort the discharge or exit the facility, there is a two-minute delay between the time that the fire suppression system is armed and its discharge. Direct heat is required to activate individual sprinkler heads to the fire's direct location, localizing the impact of water discharge.

Power Back Up

Pearson is protected against utility company power fluctuations and interruption by a sophisticated system of components including redundant Uninterruptible Power Supply (UPS) battery back-up system and a diesel generator. The battery system can run the entire data center for short power failures. The battery is also used during transfer to the diesel generator that supplies power to the data center indefinitely throughout long-term power outages. Upon resumption of utility power, the system switches back automatically. The back-up power systems are tested monthly. Regular maintenance is performed on the batteries every three months, on the diesel generator every four months, on the UPS every six months, and on the power distribution units every year.

Redundant Network

- Internet Redundancy
- WAN redundancy
- Redundant Server

Disaster Recovery

Disaster Recovery Structure

The Pearson Technology Services (PTS) Master Disaster Recovery Plan is specifically designed and structured to provide sustained business operations and recover all critical applications and data. Pearson's disaster recovery capabilities have been developed in recognition of the fact that our customer's IT services are essential to the effective operation of their business. Pearson's Disaster Recovery Planning (DRP) recognizes that to effectively recover from a disaster we must plan for replication and/or support of all critical resources — including IT, people, facilities and equipment.

The PTS Master Disaster Recovery Plan includes the organization, actions, and procedures to evaluate and recover critical and vital applications at an alternate (recovery) facility. It also includes the actions needed to announce the occurrence of a crisis at the PTS Data Center, a remote Pearson PTS supported site or remotely hosted Pearson environments supported by PTS, communicate implications to all customers, and disseminate any subsequent follow-up information deemed necessary.

Contingency preparedness also includes mechanisms to keep the plan current as the environment, personnel, equipment, legislation and business processes change. Physical and information environments on which the plan is dependent are monitored and modified to ensure they are available for recovery response, if needed. The DR Master Plan is reviewed semi-annually by the DR team and PTS management and updates are made as needed to ensure the plan remains current and accurate.

Disaster Recovery Plan Overview

The DR Plan includes specific detailed strategies that address interruptions impacting the Pearson Education Data Center, a remote Pearson PTS supported site or remotely hosted Pearson environments supported by PTS. Detailed plan components include:

- Damage Assessment Team structure
- Activation process and governance during the outage
- Recovery processes for computer systems, data communications and user access
- Ongoing processing at the Recovery Site
- Cold Site recovery if needed
- Emergency Command Center activities and communication processes
- Return Home strategy and processes

Recovery Process Overview

The recovery process allows for a restoration of the Iowa City Data Center, a remote Pearson PTS supported site or remotely hosted Pearson environments supported by PTS at the Disaster Recovery Site (DRS). Upon declaration of a disaster, the Recovery Site is notified as to Pearson's situation. PTS's Hot Site Recovery team will immediately begin restoration of servers covered under a PTS DR Service offering.

In parallel with Hot Site notification, PTS' off-site storage facility or hosting facilities help desk, which holds or can get a hold of the backup files needed to restore the environment, is notified. They will transport the specified tape files to the Recovery Site within predetermined time frames. These tape files will be staged and the system restores will commence immediately. Mainframe restoration and Remote PTS supported DR server environments will be restored from tape.

When the systems have been fully restored, database and application teams will then restore and restart the applications. Data communication links will be re-established to allow remote access to the recovered systems.

Detailed information and specifics as to Hot Site vendors can be discussed during oral presentations should Pearson be selected to continue in the bidding process.

Server Security

Standard Build

Pearson Technology Services (PTS) supports a wide variety of computer processing platforms, including the following:

- Sun Solaris on Sunfire and Dell/Intel Servers
- Red Hat Linux Enterprise Server on Dell Servers
- AIX on IBM P-Series Servers
- HP-UX on HP Servers
- Windows on Dell Servers
- IBM zOS on IBM Z Series Mainframe

Pearson keeps all standard builds current by monitoring emerging best practices for all supported operating systems – Linux, Windows, Sun, etc. and analyzing how developments can benefit our environments.

All production servers are highly available with redundant power supplies, RAID 1 disk subsystems for operating system volumes, RAID 1, 0+1 or 5 for application and data volumes, redundant and monitored SAN connections for large application/data volumes and redundant network interfaces.

The highest level of availability is achieved for large databases and file stores which utilize Oracle RAC Clustering Services to provide failover and redundancy. Web and application servers are built from standard images and scaled 'horizontally' using TCP/IP load balancing routers to distribute work over the entire server farm. In the event of a single server failure the load is balanced over the remaining servers until the failed unit is replaced.

For high transaction batch processing applications, Pearson leverages its expertise in building highly reliable and stable mainframe based solutions. These applications consistently process billions of transactions at very high resource utilization rates to meet the demanding contract deliverable timelines required by Pearson's customers. The Pearson mainframe environment utilizes dedicated high-performance DASD subsystems and an innovative StorageTek Virtual Storage Manager (VSM) 'virtual tape' subsystem which provides highly cost effective storage and long term retention of millions of data sets.

Patching

Security and vulnerability control is an essential component of world-class data center operations. Pearson's focus on automated patch and vulnerability management tools has put us a step ahead of other data centers. Our highly automated Intrusion Detection and Prevention systems identify and eliminate would-be virus attacks every hour of every day.

Pearson maintains a quarterly patch cycle. Security patches are promoted through development and test cycles before being pushed out to production server environments. One of the tools Pearson uses to monitor and manage Data Center operations is called System Insight Manager, or SIM. This tool, built internally by Pearson, centralizes significant amounts of disparate data into a graphical, summary-based dashboard view. Using SIM, Pearson Data Center personnel have at their fingertips comprehensive data on backup and recovery, maintenance schedules, patch management, obsolescence planning, system policy compliance, security and authorization, contact information and issue resolution, and performance monitoring. Our patching process and insight has regularly gained accolades from third party auditors.

Access Auditing

Pearson has taken a number of steps to ensure that access to/changes made to network components are tracked including:

- Access logging features all implemented on all applicable components
- Logs are written to a centralized management server (the Cisco Works server for Cisco devices) where they are backed up and protected from unauthorized access or modification.
- Baseline configuration files are maintained on the centralized management server. Comparison scripts are executed weekly against currently running configurations to ensure that all changes are recognized/authorized.

Pearson provides a security management audit trail by enabling operating system (Windows, AIX, Solaris, HPUX, Redhat…) audit features. The operating system records each attempted user-resource interaction with the password and user ID, which permits the audit of each individual's actions. Audit trails provide records for each activity in the system, including actions such as when a user attempts to read, modify, add, create, or delete information as well as attempting actions that require administrator-privileges. For each recorded event, the audit record identifies:

- Date and time of event
- User
- Type of event
- Success or failure of the event
- Name of the object being used or deleted
- Log-on and log-off activity
- Database administrator activities
- Database modification activities and reasons for modification

An automated host based assessment tool mines systems logs on a nightly basis. These logs are reviewed by Pearson Help Desk staff on a weekly basis. Any anomalies or suspicious behavior is immediately reported to support staff for review.

Due to the fact that system logs are reviewed on a regular basis and can become unmanageable over time, logs are rolled to tape backup and stored offsite on a ninety- day basis. This provides an audit trail of system and individual access attempts that can assist in forensic and incident handling processes. The Pearson Help Desk reviews the logs weekly with the primary emphasis on unsuccessful access events (computer security incidents). The operation system security features protect these audit logs from unauthorized read or modification access, granted only to administrative-level operators and not to general project staff. Back-up procedures help mitigate risk of losing an audit trail from remote tampering or system failure.

Backup and Recovery

We provide for daily backups of all critical business data to allow for full recovery in the event of hardware failure or other incident requiring data recovery. Each day, our Tivoli Storage Manager software creates backup copies of critical business data to multiple locations, ensuring the data is protected from loss due to hardware failure or other incidents. Each day, application data is copied to AES256 bit encryption standard encrypted backup tapes. These tapes are stored in a secure off-site vault.

We protect your data from loss with a thorough backup and recovery system:

- **Data Storage Pools.** Our primary (disk), offsite (tape), and disaster recovery (disk) storage pools provide triple backup for your data.

- **Nightly Server Backup.** We support quick and reliable data restoration by using a best practices approach to increase efficiency when we back up our servers to the primary disk storage pool each night.
- **Backup Timeframe.** To keep systems operating smoothly during peak hours, we complete major backups during non-peak hours.
- **Running Backups.** We provide added security by performing database log backups, additional ad-hoc backups, and restores as needed.
- **Database Backups.** We backup your databases while keeping them accessible to you with industry proven tools such as Tivoli Data Protection agents and Oracle RMAN backup software.
- **Monitoring.** Our 24/7x365 day a year operations staff monitors and verifies that all backups are completed successfully.

While our standard retention policy is based on industry best practices, we can customize it to meet any specific requirements you may have. Typically, it includes the following:

- **File Redundancy.** We store a copy of each version of every backup file in three locations: the primary (disk), off-site (tape), and disaster recovery (disk) storage pools.
- **Changed Files.** We store 3 inactive backup versions of changed files up to 65 days or until a new version causes the oldest version to be removed from backup storage due to the version limit.
- **Unchanged Files.** If you have not changed a file in 65 days, the storage pools will retain the latest version.
- **Deleted Files.** If you delete a file from the host file system, the storage pools retain the latest version of it for 65 days before deleting it from the backup storage pools.
- **Incident Records.** Our Command Center staff generate a problem record if a system backup fails during backup and escalates the failure to the support staff.
- **Efficient Restores.** While the size of the file(s) determines the duration of a restore, our disk-based backup architecture makes restoring data efficient and timely.
- **Additional Capability.** We can provide disaster recovery services using the Tivoli Storage Manager suite of products.