Rev. 12/18

PERFORMANCE SUPPORT SYSTEMS, INC.
20/20 Insight and WebResponse
Privacy and Security Statement

Performance Support Systems, Inc. (PSS) provides desktop and web-based survey services, which includes the collection and storage of survey data, in an online repository known as WebResponse. WebResponse is the online survey data collection component of 20/20 Insight GOLD (20/20 Insight).

The following privacy statement discloses the privacy practices for 20/20 Insight and WebResponse and applies solely to information collected through the use of 20/20 Insight and WebResponse.

Information Collection, Use, and Sharing

Only the User's survey Administrator and authorized PSS technical personnel who maintain 20/20 Insight and WebResponse have access to personal information. This Privacy and Security Statement applies to all PSS employees, restricts the use of User information and requires that it be held in strict confidence.

PSS will ask for only the information that is needed to provide the services requested.

Any personal information entered will be used only for the services requested.

PSS will never give, rent or sell any item of User's personal information to any person, organization or web site for any reason.

Types of Information Collected and Stored

Cookies

Cookies are used to maintain a link between User's login session and the PSS server. PSS does not use cookies to collect personally identifiable information or to track usage.

Name and Email Address

Names and email-addresses are the only personal information that is used by 20/20 Insight and WebResponse. It is used solely for the delivery of invitations from the 20/20 Insight and WebResponse to survey Participants.

Individual Username and Password

Survey Participants receive a link to a log-in page where they enter their Username and create their own password to enter the survey.

To re-enter the survey Respondents must use the correct username the password.

Anonymous Ratings and Comments

Respondent scaled ratings and comments are stored on 20/20 Insight and WebResponse.

Respondent ratings and comments are confidential.

Neither the User nor Subject can view a specific Respondent's ratings and comments.

Respondent names are never directly linked to individual ratings and comments. Scaled responses and comments are associated with an ID number, never directly with the Respondent or Subject's names.

Respondent scaled ratings are combined anonymously with other ratings to produce average scores, which are summarized in a feedback report.

Written comments are also combined anonymously with other written comments to produce a feedback report.

Only the User and PSS technical support personnel have access to raw data. PSS technical support personnel will NOT access the data unless handling a technical support issue for the User, and then, only with expressed permission from the User.

PSS will not intentionally disclose scaled ratings and comments from Respondents about a particular individual.

PSS will not disclose to any third party any information stored on 20/20 Insight and WebResponse or allow unauthorized access to sensitive records for any reason.

Details of 20/20 Insight and WebResponse Data Protections

Web Security

WebResponse data is stored on a Cogeco Peer1 Hosting server located in the U.S. and is accessible over the Internet only by the User. Cogeco Peer1 Hosting is a holder of the Safe Harbor certification in accordance with the U.S. - EU Safe Harbor Framework (http://www.peer1.com/hosting/compliance/safe-harbor).

PSS has in place appropriate technical and organizational measures to protect data on 20/20 Insight and WebResponse from loss, misuse, unauthorized access, disclosure and alteration and destruction. Information is protected through password protocols, internal procedures, a state-of-the-art firewall, and encryption programs.

Data encryption is used to protect sensitive information transmitted online. Users are encouraged to use 20/20 Insight GOLD 4.0.22 or higher, which implements encrypted transmission of data through Secure Sockets Layer (SSL) protocols. Users are also encouraged to use WebResponse 4.1 or higher, which implements additional encryption and security features online.

Only PSS technical support personnel, who need the information to perform a specific task for a User, are granted access to sensitive, personally identifiable information and only with the expressed permission of the 20/20 Insight and WebResponse User.

Physical Security

The WebResponse server is physically located at and serviced by Cogeco Peer1 Hosting, 2300 NW 89th Place, Miami, FL 33172.

A dedicated server is used for the 20/20 Insight and WebResponse database. Power backups are in place to maintain service and protect personal information during outages.

Physical access to the equipment, wiring and ports is denied except for authorized Cogeco Peer1 Hosting personnel or those accompanied by authorized personnel. Network connectivity to the facility is designed to provide high capacity and is fully redundant.

Data Security

Data may be secured with passwords at multiple levels of the program: Administration Software Level - to ensure that only authorized people have access to the program.

Project Level - where multiple administrators access the software, to ensure each individual project is protected.

A private, personal password created and known only to the Administrator enables login to the 20/20 Insight and WebResponse database server and prevents anyone else from accessing the User account or seeing any of the information on User pages.

The 20/20 Insight and WebResponse database server contains a state-of-the-art hardware firewall device with all non-essential ports disabled. As a result, the public Internet is denied access to the database.

The database server does not face the web and is behind a hardware firewall with an IP whitelist.

Only PSS technical personnel and Cogeco Peer 1 Hosting have access to the server.

SSL encryption (https) is available for the transmission of personal information and other data.

Virus protection and prevention programs are continuously upgraded.

Bi-weekly vulnerability and penetration assessments on PSS's servers are performed by Cogeco Peer 1 Hosting.

The entire server is backed up nightly and stored off-site by Cogeco Peer 1 Hosting.

Disaster recovery protocols are in place to protect personal information in case of a disaster.

Data Security Hygiene Protocols

Data is stored on a separate database server that does not face the Internet.

Everywhere on WebResponse, all data input is "sanitized." This means that any executable script entered into WebResponse is automatically changed to text to prevent hackers from inserting viruses or malicious programs and other database attacks.

Administrative access to PSS servers is behind a firewall that blocks all traffic except 20/20 Insight and WebResponse.

Client data is separated logically, not physically. The software application delivers data only to the appropriate authenticated User.

All Internet transmissions containing sensitive information may be SSL encrypted (https). 20/20 Insight GOLD release 4.0.22 and higher uses SSL protocols by default. The most current version of 20/20 Insight GOLD is 4.1.

Security Monitoring and Auditing

20/20 Insight and WebResponse data is professionally housed and monitored by Cogeco Peer 1 Hosting. Cogeco Peer 1 Hosting's complete Privacy Policy is available here:
https://www.cogecopeer1.com/en/legal/privacy-policy/

Cogeco Peer 1 Hosting's staff monitors the security from their data centers 24 hours a day, 7 days a week.

Cogeco Peer 1 Hosting's system is monitored by an advanced proprietary, SSAE-16-Type-II, CSAE-3416 and ISAE-3402 audited and documented system. More information about Peer1 Hosting's auditing and certification is available here:
https://www.cogecopeer1.com/en/?s=SSAE+renewal

In the event of a security breach, PSS's Chief Software Engineer Consultant is notified immediately by email.

All access to PSS's server is logged, including Windows and SQL login attempts. Logs are reviewed regularly by PSS's Chief Software Engineer Consultant and Technical Support Specialist.

In the highly unlikely event of any breach of the security, confidentiality, or integrity of User unencrypted electronically stored personal data, PSS will make any legally-required disclosures via email or conspicuous posting on this site in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of law enforcement or (2) any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Miscellaneous

Downtime

Downtime is rare. The server currently has an up time of 99.9% since 2004.

PSS subscribes to a third-party service that notifies PSS immediately if there are any outages or errors.

If PSS must take the server down for maintenance, it is performed on weekends when User usage is minimal and Users are notified in advance.

If you believe that PSS is not abiding by this privacy policy, you should contact us immediately:

Paula Schlauch
Performance Support Systems, Inc.
757-873-3700 x207
info@2020insight.net

The most current version of this document is always available at:
http://www.2020insight.net/support/documents.asp