PeopleMetrics

PeopleMetrics Security Standards

Security/Access Control Standards

1. All of our data is hosted at a SSAE 16, SOC 1 Type II secure hosting site through Windstream Communications.
2. Our systems at Windstream are protected by Cisco ASA Firewalls allowing access only for the needed ports to perform our services.
3. All of our systems are behind A10 Network Accelerators which provide common SSL (https) to encrypt the client's data as well as attack vector protection. All data transfers are performed using SSL (SCP and SFTP).
4. All web traffic to our SaaS application is forced to use SSL (https) by the A10 Network Accelerators.
5. All web servers are running patched versions of Microsoft Server 2008. Security patches are reviewed and applied within two weeks of issue date for production systems and one week of issue date for test systems.
6. The hard drives of our database and file transfer servers use self encrypting disc drives to prevent data loss from failed drive replacement.
7. Only our system administrators have access to the systems at Windstream. All access is by secure IPSEC VPNs. All VPN access is logged by user and time of access.
8. All accounts require secure passwords. We use Microsoft Active Directory and only our system administrators have Domain Administration privilege and can create accounts.
9. All default passwords are changed on both software application and hardware device levels.
10. Password controls are implemented using Group Policy to ensure consistency throughout the organization. Password controls are:

    - The password has to be at least eight characters in length
    - It must contain at least one number and at least one upper case letter and one lower case letter
    - Password history is set to the last five passwords
    - Invalid logon lockout is set to five attempts
    - Password expiration is set to 90 days

11. All access to the client software requires user names and passwords. The system uses Role Based Access control to limit the data available to the user. Only their survey data is accessible.
12. The database is backed up several times per day to disc and then copied to encrypted tape drives nightly.
13. The database backup is encrypted using private encryption keys and stored in the cloud daily.
14. Disaster Recovery - Windstream provides multiple hosting centers, and should anything happen to the center in Conshohocken, we would be re-located to another of their centers. All data is backed up to the cloud for quick access for remote site recovery.

15. All user and administration accounts are unique and justified based on 'least privilege.' User permissions are restricted to accounts and systems required by their job responsibilities.
16. Account administration change requests including account additions and deletions is performed electronically using request submission form.
17. Emergency account disablement is provisioned by the Incident Response Plan.
18. All users login with their own usernames for audit and review purposes.
19. Security/access logs are reviewed weekly to track authorized access and monitor activity against all accounts.
20. All PeopleMetrics servers have virus protection with periodic scanning and virus signature updates.
21. Perimeter vulnerability and application vulnerability scanning is performed nightly by a third party service.

Code Deployment Standards

1. An entirely separate system is used, not at the co-location center, for development. Access to these systems is not provided outside of the PeopleMetrics offices.
2. Cisco ASA Firewalls are used to protect the PeopleMetrics office network. Only IPSEC VPN access is allowed from off-site.
3. All code is kept under Perforce Source Code Control.
4. Code for release is tested in the development environment, upon successful testing it is promoted to a test environment at Windstream.
5. The code is tested at Windstream on separate systems in the production environment using the same standards as the production environment. Upon successful test it is promoted to production.
6. Management signs off on releases to Test and to Production before they occur. The changes are tracked both in Perforce on a file by file bases and in SharePoint or Google Docs at a project basis.

Physical Access Standards

- Co-Location Center
  PeopleMetrics Data Center is co-located with Windstream Hosted Solutions, a part of Windstream Communications. Windstream's Conshohocken Data Center is audited under SSAE 16 SOC 1 Type II standards annually. The Data Center facility falls into a Tier Three (3) standard from a power and cooling standpoint and are in an N+1 configuration as required. SLA covers network availability at 99.995%, which matches the Tier Four (4) criterion.

  1. ***Power***
     - N+1 UPS system
     - Independent diesel fuel generator 48 hours of runtime
     - 24x7 contract for service and immediate fuel delivery from multiple vendors

  2. ***Cooling***
     - N+1 Cooling

- All units are double compressor units and can run at half capacity, regardless of N+1
- Preventative maintenance and capacity monitoring is performed routinely to ensure operating efficiency
- Water detection system under HVAC units

3. ***Connectivity***
   - Diverse fiber connectivity using SONET architecture
   - Tier 1 Peering with Multiple Internet Upstream Providers

4. ***Security***
   - 24 x 7 onsite personnel
   - Card-reader access system
   - Biometric identity access system
   - Video surveillance and capture to DVR
   - Electronic verification by Windstream personnel
   - Key and lock access to all equipment cabinets

5. **Fire Protection**
   - The data center is equipped with a network of water sprinklers and water detection alarms around the doors. There is a manual shutoff for the sprinkler in the event the mechanism is inappropriately triggered. The water sprinkler system is monitored and inspected by the landlord on continual basis. Fire extinguishers are in place next to each door in the data center.

Application Access Standards

We utilize a DMZ configuration with multi-layered firewalls that include stateful inspection, as well as advanced application and protocol inspection and intrusion monitoring. All web services are protected by the A10 Networks devices which support automatic denial of service and attack mitigation.

Only two ports/services open for application access:

- HTTPS – for 256-bit SSL encrypted survey and eFocus pages
- SFTP – for data transfer to a dedicated file transfer server, as required. All SFTP access is limited to only the directory for that client using virtual mount points.

- **E-Focus**
  eFocus participants can access an eFocus group using an individually assigned URL with encrypted PIN information. The URL and PIN are valid only for the duration of the eFocus group, which is typically 2 days, but can be extended to any period of time as determined by the client.

- **Survey Taking**
  Survey participants access their survey using an individually assigned URL with encrypted PIN information, or a generic landing page that generates a survey specific pin.

The URL and encrypted PIN are valid only for a single survey, and do not allow access to any other areas of the application.

- **User Access**
  Hub users have individual user accounts with passwords and access the system via https (SSL). Their login restricts their access to only data within the surveys assigned to their account. Role base access control further restricts their access to data within that survey.

- **Single Sign On**
  Windows AD users may opt on a client by client basis for use of Single Sign On. A trusted web service at the client site validates the user using Windows AD and passes a private key encrypted time limited token to identify them to our system. Our system validates that the token was received from a valid IP address for that client and decrypts it using the client's public key. This token, when decrypted properly and within its time limit, is accepted as if it was the user name and password for that validated user.