PARC | knowledge management made easy

Security Summary

The PARC application and SQL database reside within the Microsoft Azure cloud platform, where both are protected by Microsoft-maintained firewalls, partitioned local area networks and physical separation of back-end servers and public-facing interfaces. (See details of Azure infrastructure security here.) Interrogation of the database by the application occurs only within the secure Azure environment. The database can only be accessed via the application by authorized users who present a valid account ID and password. Cross-client separation is maintained by application protocols that ensure that every user request is matched to the account to which the user is assigned. Communication to and from the Azure cloud is secured with SSL encryption, with a certificate by DigiCert. Optional two-factor authentication is available.

Files are parsed using Open XML in web context, a secure and less privileged context which prevents unwanted action. No macros are executed. Stored user files are not opened or executed. Stored procedures prevent SQL injection; in query creation, every input is sanitized.

Initial PARC passwords can and should be changed by users. Passwords require eight to 15 characters, at least one lower case, one upper case, one number and one special character. Accounts lock after five incorrect password attempts. Administrative and non-administrative IDs are available; only admin IDs have rights to create project folders and upload or delete files.

Standard user agreements require Langer Research Associates not to disclose confidential client information. We will access an account only upon written authorization by the user, only for the purposes specified, and will delete the access ID when the requested task is completed. Users who depart the system can receive their data file in CSV/Excel or text format.

Details: http://www.langerresearch.com/parc/
Questions: info@langerresearch.com