Data Security and Privacy

User identify, user data privacy and user data security are strictly maintained at all times.

Security is provided in multiple layers: a) at the gpu server level, via user allocated unique gpu server name/location/ip-address, b) at user level, via authentication and authorization of user, c) system level security token(s), d) encryption of user data via SSL(256 bit encryption), e) continuous virus scanning, f) de-identification of user identity and g) de-identification of user data combined with fragmentary view of user data. Any gpu server instance contains information limited to only the sole contractual user or for shared situation the set of contractual users. Security monitors all login attempts, date, time, logon information and ip-address.

Web server hardening protocols are updated, enforced and monitored. Server vulnerability tests are periodically conducted for validation.

User access to web app models is controlled via pre-arranged Login, Password and Service Level available from IHA Consultants (www.ihaconsultants.com) or by calling (919) 260-3291. A total of 5 logon attempts is allowed. Upon an unsuccessful 5th logon attempt, the user account is permanently disabled for all web app models and requires the user to contact IHA Consultants. A successful logon resets the unsuccessful logon attempt counter. User web service job: date, time and web service name are logged to a central repository and debited against the user account authorized maximum count.

Enhanced security is provided by way of running each user initiated model as single/sole execution on available GPU card(s) combined with “no disk touch” – all user data remains in server memory at all times and is destroyed upon report transmission.

The possibility of data security breach is possible, however, remote due to additional timing requirement that perpetrator know date and exact time contractual user submits jobs. Security breach origination is more likely to occur due to “casual or seemingly harmless sharing of login, password, service level” information which will have the effect of accelerated debit of utilization count which for capped contracts with pre-arranged maximum utilization over a time period will “result in server busy messages for no apparent reason to contractual user and gain the interest/attention of the contractual user with probability 100% as the debit web app model counter increases towards the maximum sunset service access and result in higher gpu cloud runtime charges over shorter period of time.” [1] [2] For contractual users with uncapped maximum utilization count, the main effect is server busy messages for no apparent reason to contractual user (which require many re-submissions e.g. service access delay(s)), higher short-run gpu cloud service provider charges and subscription status queries that show increasing or high utilization web app model counts.

[1] Contractual user retains responsibility for user logon information security.
[2] See Web App Model Account section for details.