AMS
by Catapult

HOSTING

AMAZON WEB SERVICES (AWS)

Catapult data is hosted on industry-leading cloud services provided Amazon Web Services (AWS). The AWS network provides significant protection against traditional network security issues and customers can implement further protection. Refer to the AWS Overview of Security white paper (available at **amazon.com/security**) for additional details.

Amazon assets are configured with anti-virus software that includes e-mail filtering and malware detection. AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm. For more information please refer to this **link**.

All data stored by Catapult on behalf of customers has strong tenant isolation security and control capabilities. Catapult retain control and ownership of their data, thus it is our responsibility to choose to encrypt the data.

AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. Refer to AWS Risk and Compliance Whitepaper for additional details - available at **aws.amazon.com/security**.

The AWS environment that Catapult uses is a virtualized, multitenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.1 published in April 2015. Refer to AWS Risk and Compliance Whitepaper for additional details - available at **aws.amazon.com/security**.

Automatic alarms are in place which alarm key Catapult support staff in the case of problems.

Partners can also log support requests to their regional support teams via email and our support staff from the different regions are able to assist the partners.

We also use two factor authentication to ensure only eligible staff from our partners are able to access the system.

In case of acute issues we also are able to request the partner to provide us temporary access to their account which we can diagnose. The access is automatically terminated for data security after a pre-determined period of time.

We are also able to revoke access to partner employees who no longer work for the partner upon request from the authorised account holder of the partner.

AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures.

Catapult will use commercially reasonable efforts to implement back-up and recovery procedures to protect and preserve information you transfer to Catapult or that your use of the software and equipment generates (your 'data') while your data is stored on Catapult's computers.

This will include at least daily back-up to a separate hard disk and weekly off-site back-up, or a back-up schedule that provides adequate equivalent security against data loss.

Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means.

The AWS SOC 1 Type II report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.