FIA Tech – Production Management Standards

Information Security

FIA Technology Services, Inc. is a wholly-owned subsidiary of the Futures Industry Association that collaborates with the global futures industry to improve operational efficiency via its web-based software systems. In the past, FIA Tech has operated three platforms: the Electronic Give-Up System (EGUS), the Electronic Give-Up Automated Invoicing System (eGAINS), and FIA Tech's Reconciliation Software (eRECS). Recently, FIA Tech developed a new OCR Data Service that has been included in its suite of applications since the third quarter of 2014.

FIA Tech's Data Centers

FIA Tech leverages best commercial practices, tools, and policies to ensure the security and recoverability of data that FIA Tech processes on behalf of its customers.

Towards this end, FIA Tech has employed in data centers that maintain high security standards and are audited annually to ensure that their high standards are met. Remote sites used by the data centers for disaster recovery purposes are also required to conform to the production data centers' security requirements.

Data center controls that ensure the security and recoverability of data processed by FIA Tech on behalf of its customers derive from a broad framework of organizational and operational dimensions:

- Control Environment – Organizational culture and approach towards security.
- Physical Environment – Security governing access to the IT assets that are hosting FIA Tech applications.
- Environmental Controls – Physical data center conditions that ensure safe, secure, and resilient equipment operation.
- Data Center Operations – Processes governing the management of the hardware, software, and procedures required for production operations.
- Information Security – Design and practices required to maintain the integrity of confidential information.
- Storage management – Practices required to keep physical media and documents secure.

All of these control dimensions are validated and verified by FIA Tech's data center hosts during the course of regular, required audits.

FIA Tech Information Security Practices

FIA Tech's internal processes have also been designed to conform to the same high security standards of its data center hosts. These processes include the following control points that have been established and tested to ensure the robustness of FIA Tech's information security approach:

- Security policy – Policy, documentation and internal assessments are maintained.
- Network access – Practices restricting access to data and infrastructure assets are established, maintained and monitored. These practices include password management, user rights management, server access privileges, etc.
- Production environment access – Procedures and controls that restrict production access and monitor production networks and applications are established and reviewed.
- Application security – Rules governing administrator and user access rights are documented, implemented, practiced and monitored, and all user access is logged.
- Data communications – Policies that govern the secure transmission of data (including encryption methodologies, certificate usage, internal and external network access methods, firewalls, WIFI policies, etc.) are established, maintained and monitored. Network monitoring for malicious software, intrusion detection, Dos/DDos attacks are in place according to standard practice.

Availability of Audit Documentation

All of FIA Tech's data centers undergo annual audits to ensure the conformity of their information security practices against of SSAE 16 audit standards. FIA Tech reviews and evaluates these audits annually in the context of its vendor assessment program. In addition to these independent audits, FIA Tech also performs its own separate vulnerability tests against the application's infrastructure and code to ensure that the application layer is secure. A summary of FIA Tech's most recent SSAE 16 audit of its data center host is available upon request.

FIA Tech will also be subject to annual attestations by an independent audit firm to ensure that its processes are sufficiently robust to support confidential information at all times. Documentation from the latter may also be obtained upon request.

Recent Assessments

FIA Tech conducted first annual vulnerability assessment of the OCR Data Service platform in December 2014. The assessment included two independent penetration tests, one as part of the data center host's procedures and a second from an independent security assessment firm. The assessments found no significant vulnerabilities; two low-level risk items were discovered and will be scheduled for remediation at a future date. An independent assessment will be performed on the internal application code in January 2015.

FIA Tech also performed its first annual OCR Disaster Recovery test in November 2014. It successfully recovered its data center at its recovery site within 3 hours, and proceeded to run its production schedule the remainder of the week at the alternate site with no issues. While attempting to return back to the production site, a configuration issue on the disk file system was discovered, and was corrected at the conclusion of the test. These measures helped FIA Tech confirm its recovery strategy and helped it correct factors that could have possibly hindered a smooth recovery in the event of a disaster.