



Client Portal Security Overview

October 2011



Institute of IT Training
Gold Standard
Accredited Training Provider

*



INVESTOR IN PEOPLE

*



**



FS75484

*



This document aims to provide an overview of the security controls that are inherent in the implementation of the Avelo Client Portal. We have taken a mature approach to the implementation of an appropriate data security model in line with our experience of providing and supporting the industry standard Avelo Exchange Portal. Following our client engagement programme we are providing a solution that meets the security and usability needs of you and your clients.

During the development of Client Portal we worked closely with Microsoft, who provided expert based reviews of the software in respect of identifying any potential security issues. Once Client Portal was complete we then commissioned a leading third party penetration testing company to review the application for security weaknesses, issues or concerns. The outcome of that testing was confirmation that they found the application to be secure and in line with industry standards, further Penetration testing will take place on a regular basis to ensure that your data is protected.

We believe that this document demonstrates our commitment to delivering a Client Portal which is secure both now and in the future. If you have any further questions please contact your account manager who will be happy to facilitate a more detailed discussion as appropriate.

1 Website access

The following features ensure that client data is only available to the client or their adviser:

- All client data is protected by a combination of username and password
- All passwords must meet our password complexity requirements (at least 7 characters including at least one digit, lowercase letter, upper case letter and symbol) to ensure that insecure passwords cannot be chosen by users
- The transfer of data over the internet is protected by HTTPS SSL/TLS this ensures that all communication between the client's web browser and the web server is private and ensures protection from eavesdropping or 'man-in-the-middle attacks', this security is common place for internet payment transactions and / or internet banking
- If a client is inactive for a preset amount of time they are automatically logged out to prevent another user gaining access to their account if their machine is left logged in
- Key security operations within the website, such as changing password are protected by CAPTCHA technology (to prevent automated attacks) as well as asking the user to re-enter their password, this combination ensures that these operations can only be carried out by a real user
- Anti-forgery tokens are used throughout the site to protect against cross site request forgery attacks



- Repeated attempts to guess a client's password will result in the account being locked out and this can then only be unlocked by you on the customer's behalf
- All files uploaded to Client Portal are automatically checked for viruses using two malware scanners
- All access to the database is via stored procedures to prevent SQL Injection attacks
- Cross Site Scripting (XSS) attacks prevented by input validation, where HTML input is allowed Anti-XSS tools ensure no cross site scripting vulnerabilities

2 Adviser Office connection to Client Portal

Adviser Office uploads and downloads data using Avelo developed Web Services, these Web Services are protected by an authentication mechanism with all transmitted data being protected by HTTPS SSL/TLS encryption. In addition any document uploaded to Client Portal from Adviser Office is automatically checked for viruses using two malware scanners.

3 Data Security

All data transmitted over the internet is sent over HTTPS (encrypted using SSL/TLS) all data transmitted within the data centre is encrypted with IPsec which provides secure internal authentication and encryption protection for all traffic. Within the data centre we operate our systems within a separate and secure location (room) to provide physical and logical network separation. Lastly we ensure that all sensitive data stored within the Client Portal database is held in an encrypted format.

4 Data Centre

The computers providing the Client Portal website are situated in a tier 3 / 4 data centre at IBM Warwick (Tier 4 is the highest level of capability commercially available and typically provides 99.995% infrastructure availability).

Our data centre operator monitors its internet connectivity 24/7 for attacks such as Denial of Service or Distributed Denial of Service attacks.

We ensure that regular penetration testing takes place (by an external third party) and furthermore weekly scans are performed by the security team to ensure that that Client Portal is not susceptible to new security exploits.

Access to data centre equipment and data is limited to specific named individuals within the technical operations team.

4.1 Physical security

Access to the data centre is tightly secured to ensure that the Client Portal service is available and secure. Our data centre provides the following features:

- Biometric access (fingerprint) to machine rooms
- 24/7/365 CCTV coverage with live security monitoring
- Tiger Traps (airlock type access) - monitored by security to manage personnel access to server rooms
- Tiger Trap vehicular access controls to cover goods inwards areas

4.2 Business continuity

Our data centre provides the following business continuity features to help ensure Client Portal is available:

- At building level
 - Dual building UPS (Uninterruptible Power Supply)
 - Dual Electrical feeds
 - Backup diesel generators – with five days fuel contingency
 - Multiple machine rooms
 - Redundant cooling
 - Redundant power distribution boards
 - Dual internet connectivity
- At rack or room level
 - Dual path power distribution
 - Redundant power supplies
 - Redundant network paths
 - Redundant SAN connectivity
 - Redundant Switches SAN and Network
- N+1 servers for the service (to provide redundancy)