Data Security Statement for Hosted Applications Service for SIMS, FMS & PS Financials

Protecting, securing and managing access to customer data are critical aspects of the Scomis Hosted Applications service. Some of the key measures utilised to ensure data security are detailed below:

ISO 27001 Accreditation

Scomis' accreditation to the internationally recognised standard for Information Security demonstrates our commitment & ability to protect our customer's data. This provides assurance to our customers that your data is safely hosted by us following processes and procedures that adhere to established best practice.

Backup and Recovery

The backup processes for the service provide six months of retention with 30 daily points and 5 monthly rollups. This is protected by our managed remote backup service, which mirrors the information to our second offsite data centre - see http://faq.scomis.org/kb4499 for further details.

We are currently migrating to an industry leading virtual server backup solution to further enhance this aspect of the service and significantly reduce recovery time for customer requests to restore data.

Resilient Connectivity

To provide the most reliable service possible, Scomis have recently released v5.3 of our connector which incorporates connectivity through multiple Internet Service Providers to remove any single point of failure in our infrastructure - see http://faq.scomis.org/kb16871 for details.

External Security Assessment and Penetration Testing

Data confidentiality is of paramount importance to us, as is safeguarding the integrity and availability of our Service from any potential threat or disruption. The Scomis Hosted Applications Service has been proactively penetration tested to address any such security vulnerabilities and issues.

Compliance with Industry Standards

Scomis maintain compliance with current security and industry standards and best practice. As a Hosted Service provider our purpose is to ensure we protect your information with confidentiality, integrity and in accordance with current laws and codes of practice.

Reacting to Vulnerabilities

The Scomis Hosted Applications service utilises Microsoft Server products which are robust, industry standard assets under constant review by the Internet community at large. Comprehensive monitoring of the platform is performed; updated security patches and fixes are applied on a rolling programme. Scomis will always react to any vulnerability in accordance with its impact and urgency.

Creating, Suspending and Deleting Accounts

Scomis offer subscribers of the Hosted Application Service the ability to undertake certain user management and user access tasks. This allows our customers to be in charge of who has access to their data and when.

Scomis provides additional functionality (for nominated users) to create, disable and suspend users' access to the Hosted Application Service via a suite of user management tools. Alternatively, the Scomis Service Desk is on hand to provide assistance with immediate requests for user management tasks.

Data Deletion and Retention

Scomis agrees to manage data for customers for the purpose of providing the Hosted Applications Service only, as detailed in our Service Level Agreement and our Terms and Conditions. Scomis retain secured backup copies of a customer's data for a period no longer than 6 months. All hardware used to hold data is securely wiped and disposed of in accordance with recognised industry practice and standards.

Audit Trail

Each user accessing the Hosted Application Service is recorded in Scomis' activity logs which are retained for 6 months. Subsequent activity within applications is recorded in accordance with the respective software vendors audit methods.

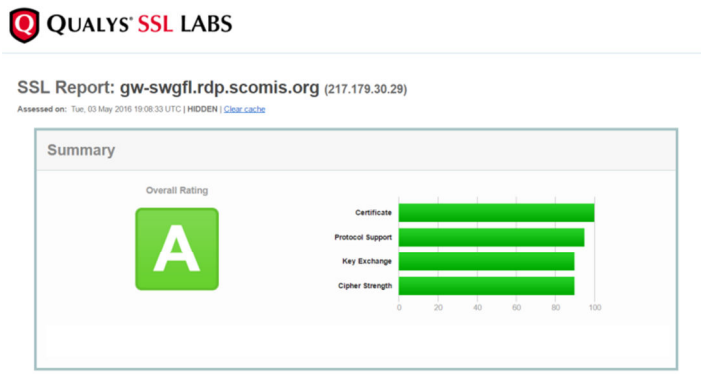
Data sharing

Scomis will never share customers' data unless expressly requested or authorised by the customer, and only for such purposes as are compatible with providing the Hosted Application service (i.e. sending copies of SIMS data to Capita for support purposes).

Customers often utilise Third party applications (VLE's and parent communication tools) which transfer data to and from their MIS dataset that is hosted with Scomis. It is the customers responsibility to ensure that they undertake their own due diligence and risk assessment checks (as data owner) to ensure that the data is held secure and encrypted at all times whilst in transit or at rest and that sufficient access controls are in place to prevent accidental data loss.

Security of data in Transit

Customers of the Hosted Application Service can rest assured that all data transmissions are securely encrypted using up-to-date variations of SSL and other encryption technologies. For further technical information on the measures employed please contact the Scomis Service Desk.



Information correct as at 05/05/16