Squad In Touch Information Security and Data Protection Notes

Information Security in the cloud

The *Squad In Touch* solution is delivered to schools from the cloud servers located in Ireland. We host our solution at the Amazon Data Centre (Amazon Web Service, AWS) fully compliant with security standards and requirements according to:

- UK Government Cloud Security Principles published by National Cyber Security Centre under the Cloud Security Guidance - https://www.ncsc.gov.uk/guidance
- UK Cyber Essentials Requirements dated June 2014 - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

NCSC published the Cloud Security Guidance documents for public sector organisations that are considering the use of cloud services for handling official information on 23 April 2014. Under this guidance, HM Government information assets are currently classified into three categories: OFFICIAL, SECRET and TOP SECRET. Each information asset classification attracts a baseline set of security controls providing appropriate protection against typical threats.

NCSC Cloud Security Guidance includes a risk management approach to using cloud services, a summary of the Cloud Security Principles, and guidance on implementation of the Cloud Security Principles. Additionally, supporting guidance documents are included on recognised standards and definitions, separation requirements for cloud services and specific guidance on the measures that customers of Infrastructure as a Service (IaaS) offerings should consider taking.

See https://d0.awsstatic.com/whitepapers/compliance/AWS_CESG_UK_Cloud_Security_Principles.pdf to learn more about how AWS complaints Cloud Security Guidance.

Cyber Essentials Plus is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organizations demonstrate operational security against common cyber-attacks.

It demonstrates the baseline controls AWS implements to mitigate the risk from common Internet-based threats, within the context of the UK Government's "10 Steps to Cyber Security". It is backed by industry, including the Federation of Small

Businesses, the Confederation of British Industry and a number of insurance organizations that offer incentives for businesses holding this certification.

Cyber Essentials sets out the necessary technical controls; the related assurance framework shows how the independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor. Due to the regional nature of the certification, the certification scope is limited to EU (Ireland) region.

See AWS certificate here - http://www.cyberessentials.org/validator/verify.php?certificate=2864877880893798

AWS provides a highly reliable, scalable and secure cloud based infrastructure meeting the requirements of an extensive list of global security standards, including:

- ISO 27001;
- SOC;
- PCI Data Security Standard.

Personal data protection

SquadInTouch LTD is developing their software as well as business process according to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (EU Data Protection Directive).

SquadInTouch LTD use the approaches stated in AWS EU Data Protection Whitepaper (https://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf) to use AWS services in compliance with EU Data Protection Directive.

SquadInTouch Ltd is registered with the Information Commissioners Office (ICO) and its registration number is ZA190536.

Members of Squad In Touch development, support and administrative teams has no access to schools data. If we need an access for the school data for support team member for particular data-related issues, our support team member ask school admin for temporary permission that can be revoked by school admin at any time.

Our technical maintenance staff has very strict requirements for access into the database and are regularly instructed to maintain and support measures for preventing unauthorized or unlawful access or use of schools data. We do ensure that all technical maintenance team members having access to whole database are fully aware of their responsibilities with regards to the schools data protection including requirements of confidentiality and non-disclosure of any personal information.

To provide higher individual users data protection the Service uses an increased strength-level for user passwords. We check user contact details (email, mobile phone number) when the new user is enrolled. Every time the user wishes to change their personal contact data he needs to confirm changes using codes sent to his mobile phone and/or email address to verify his identity. The user passwords stored in the data base irreversibly encrypted, thus we completely prevent harm in case of passwords stealing.

Squad In Touch service supports high secure multi-level role model of access to schools data. System admins team member can only grant permissions for school admins and revoke any permissions of any user in the system for emergency reasons. Nobody of system admins team can grant any permission to the school data. Only school admins can grant permissions to school data for their PE teachers, coaches and parents. School admins are able to revoke any permission to their school data at any time for any reasons.

Squad In Touch server supports secure https connection which provides high level protection of the privacy and integrity of the exchanged data.

Squad In Touch server supports strong authentication mechanisms based SHA1, SHA256 and RSA cryptography algorithms.