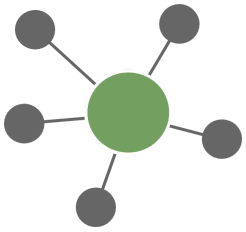

AccountingHub.io Ltd.

Information Security Policy

Author:
Kieran Fitzsimons (CTO)

Last updated:
04/10/2017

Introduction

Security is a core element of our solution. We have designed our application to protect both your clients as well as your own data at all times. Furthermore, the General Data Protection Legislation (GDPR) directive has been considered as part of both this policy and our application architecture.

Definitions

- ‘Administrator’ is a user that is part of your practice and has admin permissions
- ‘Staff’ is a user that is part of your practice but does not have admin permissions (cannot edit subscription, remove Administrator users etc.)

Policy

- All communication via our website, backend servers and database are protected using SSL (Secure Sockets Layer) encryption. You will always see a padlock in your browser when using our application which ensures it cannot be intercepted by anyone else
- Documents are stored on European servers, the data is not replicated outside of the EU. This is important to comply with data protection regulations but also provides the best performance for our customers in UK/EU. This applies to any practice who did not register via our U.S. suppliers
- Access to documents is based on the following principles:
    - If you uploaded a document, you should have access to it
    - If your company uploaded a document, you should have access to it (e.g. a client uploads a document, any other user that is part of that client account can also see the document)
    - If your accountancy practice uploaded a document it could be publicly shared with all clients or private (just for other members of staff). A warning is shown to ensure you do not wrongly set the permissions. Uploaded documents are private by default. This is a GDPR consideration.
    - If a document is deleted, we will continue to store it temporarily to ensure it has not been deleted by mistake. This is important from a data retrieval and compliance perspective. You must contact us to restore a deleted file.
    - If your accountancy practice account is ever permanently deleted, this will erase all related records including users, documents, forms, invoices and tasks. Cancelling your subscription will not immediately trigger this permanent deletion
- Only a user with administrator access can cancel or modify your AccountingHub.io account. Likewise a member of staff has access to client records and most features but cannot remove an administrator user or view/modify many of the account settings.

- During development we use a completely isolated environment, including a different database to ensure we do not interfere with the production application or your data
- Our production database is regularly backed-up and we run a disaster recovery drill every year to ensure we can restore this data promptly if ever required
- The architecture of our systems is always reviewed and approved by an Amazon Web Services Solutions Architect
- Data such as Stripe API keys are encrypted in our database, all passwords are also hashed (stored in a format so they can never be read)
- All payments are made via Stripe (including client invoices), we never store or handle payment information ourselves, both for security and compliance reasons.
- Documents are uploaded, stored and retrieved directly from Amazon S3. We provide authorised users with a temporary link to the document (generally a few minutes)
- Emails sent via our servers always use SSL encryption to protect information (e.g. invoice / document link)
- Activity is tracked and can be seen on the practice dashboard, this provides an audit trail of activity. We can produce ad-hoc reports over a specific time period for a fee, should this ever be required
- When logging in from a new IP address (e.g. new device/location) we will email you to make you aware
- We will never ask you to tell us your password. If we need to verify who you are we will ask a number of security questions regarding your activity, user details and payment information. In addition you may be asked to verify your identify using an emailed security code
- Your account will be locked out temporarily when entering your password incorrectly five times. This helps reduce the threat of a brute force attack (where an attacker enters a large number of passwords in the hope one will work).
- An administrator can suspend any staff account instantly (and unlock again). Any member of staff can suspend a client account instantly (and unlock again). This helps ensure only the correct people can login / access data. Attempting to login with a blocked account will show an account disabled error message
- Updates are regularly released to improve usability, fix issues and add new features. Each release must pass our test plan, unit tests and code review before being released. We can rollback to a previous version in under ten minutes if required
- All code for both the website, application and backend are kept under source control. Only developers who require access are able to read/write to the relevant areas
- In the unlikely event of a data breach we will follow GDPR policies.
- Computer related: Anti-virus software is installed and running on all staff machines. The latest operating system updates are applied regularly (e.g. monthly). Only operating systems that are supported by their developers will be used (e.g. Windows XP is end of life). We will only use supported versions of Internet browsers for security (and recommend the same to customers)