Product Data Sheet: Intelligentcontract.com Data Security

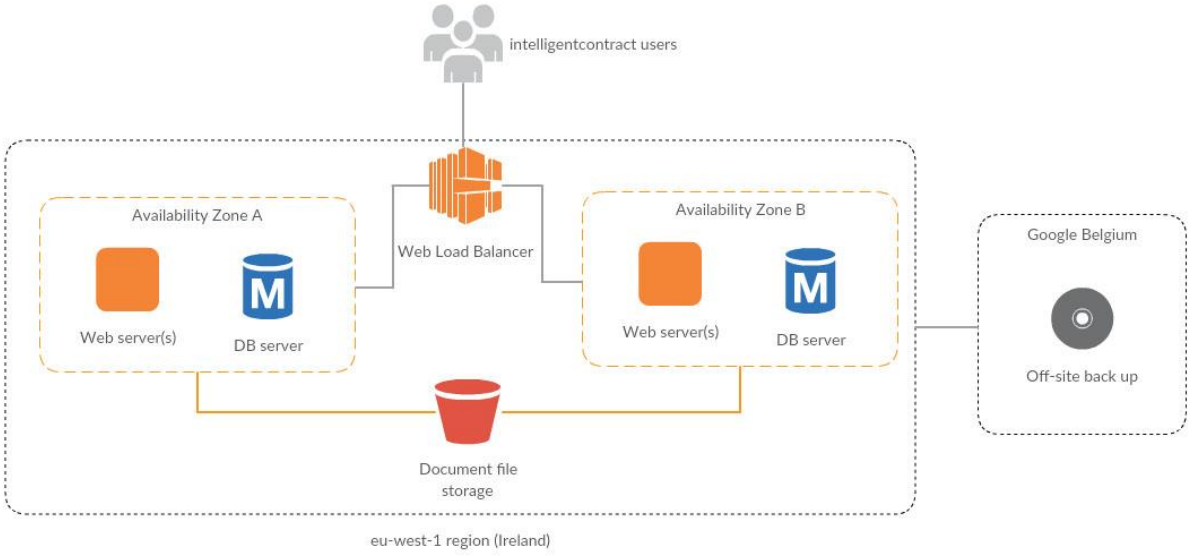
The use of Cloud-based solutions is becoming more prevalent, predominantly due to the substantially lower cost of ownership and flexibility offered when compared with traditional "installed" software. However, there is a key concern for customers surrounding the security of their data: both the unauthorised access to data and the loss of any data.

At Cloud9 Software (C9S) we realise the importance of data security to our customers, so we have taken measures so that we and our partners have policies, procedures and systems in place to reduce the security risks relating to your data.

We are committed to ensuring that your information is secure and prevent unauthorised access, disclosure or loss of your data. In this product data sheet, we describe the **application level security**, **hosting partner policies and procedures** and **backup and recovery** procedures we have put in place to safeguard and secure the information we hold on your behalf.

Overview of our Platform Architecture

Intelligentcontract.com is hosted by Amazon Web Services (AWS). AWS is a tier 1 web hosting service. Intelligentcontract.com is hosted out of AWS' Dublin facility in Ireland. There are two physical locations (availability zones) which provide a level of redundancy within our architecture. The diagram below provides an overview of the intelligentcontract.com technical platform.



Application Security

We take the security of our application very seriously. We employ an external party on an annual basis to review our application security arrangements. The annual penetration test is completed in the first quarter of each year and the annual results can be provided upon request.

The intelligentcontract.com application has built-in security measures that provide peace of mind to our customers. The table below provides information on the key measures that have been implemented.

Measure	Purpose
Application is only available over HTTPS (additionally HSTS is enabled and cookies are flagged as HTTPS only)	Prevents attackers from accessing sensitive data by sniffing network traffic
Application is hardened against XSS, clickjacking, CSRF and SQL injection attacks (verified by penetration testing)	Prevents attackers from executing harmful code on the server or tricking legitimate users' browsers into giving away login credentials or data
Customer-configurable login session timeout	Customers can optionally specify a time after which inactive login sessions should time out
Customer-configurable password strength	Customers can switch on a "strong passwords" setting which forces users to use complex passwords
5 failed login attempts allowed in 5 minutes before Captcha image is presented. The account is locked if there have been 10 failures in the last 5 minutes	Prevents non-authorised people (maybe who are using brute force attacks) from attempting to guess passwords.
Customer -configurable password options to expire users' password after specified length	If a customer doesn't restrict access to an ex-employee's login, after the specified period access will automatically be revoked
Forgotten password functionality requires users to confirm password reset via a link sent to their email account	Prevents attackers from resetting users' passwords without their consent
IP address and time/date of most recent login displayed to user on login	Alerts users if their account has been logged in to from an IP at a time and date they don't recognise
Read/write access to entities within the system (Contracts, documents etc.) can be locked down to specific users and groups of users	Allows Customer to control who within their organisation can access which data
User file uploads are restricted to specific file types	Prevents users from uploading harmful files including as viruses

Hosted Environment Security

Our hosting partner has security measures in place that adhere to the data security standard ISO270001. A detailed copy of AWS' security white paper can be obtained on request. In addition to AWS hosted environment security measures, we have implemented further security measures designed to prevent

Measure	Purpose
2-factor authentication required to access back-end C9S administration portal	Prevents attacker who's acquired a password to the system from gaining access
Access to live servers and database administration interface restricted to C9S office IP address	Prevents anyone outside the C9S network from accessing the hosting infrastructure
Firewall and load balancer in place	Clients cannot connect directly to the live servers or database but must come through a load balancer. Only the ports that strictly need to be opened (HTTP/HTTPS) are accessible.
Staff with access to the C9S administration portal have signed Non-disclosure agreements, are back ground checked annually (Disclosure Scotland) and are made aware annually of the consequences of breaking the terms of the Non-disclosure agreement.	Because employees have access to data it is important that those staff are able to demonstrate they are trustworthy and also for them to be aware of the consequences of unauthorised disclosure The NDA agreements apply after an employee has left the business
It is our policy that customer data should not be downloaded to local computers or any type of portable media	By having a policy that customer data only ever resides in the data centre we are able to minimise the risk of unauthorised access of customer data.
The C9S office is physically secured with a combination lock. No one is allowed into the office unless a background checked member of staff is present.	Removes the risk of opportunistic individuals accessing machines which may have access to the data centre
We are able to demonstrate that we comply the UK data protection (acting as a processor)	To give our clients piece of mind that personal data is treated in line with the stipulations of the UK data protection act.

Backup and Recovery Strategy

Customer Meta data

SQL databases in AWS are backed up on an on-going basis with backups retained for 30 days. Point-in-time recovery is available with these backups so we can restore to any point in time within the previous 30 days.

Additionally, the databases are converted to text files once a day and these are backed up to a file storage area within our AWS account.

Customer Uploaded files

Files uploaded by Customers (for example, contract documents) are incrementally backed up on an hourly and daily basis to the file storage area within our AWS account. These incremental backups cover a period of 2 weeks so in the event of data being lost from our primary file storage, we can restore to the nearest hour at any point within that period.

On a weekly basis, the database dumps and file backups are archived to a weekly backup directory within the AWS file storage area, and these weekly backups are retained for two years.

Finally, all data stored within the AWS file storage area (including historical backups) is incrementally backed up on a daily basis to a secure storage area within a separate storage (Google Cloud Storage) account. This is also retained for 2 years

Note that the AWS file storage is located in Dublin, Ireland and the Google cloud storage is located in Belgium.

Disaster Recovery

Customer data is primarily located our AWS facility in Dublin Ireland. We have reserved space in two physically separate locations – should there be an issue in one location, service will automatically switch over to the other.

We have a documented disaster recovery procedure which covers both the CS9 office location and the AWS data centre. The plan is rehearsed on an Annual basis and alterations made if required. A copy of our disaster recovery plan is available on request.

For more information about how we protect your data please visit our product website at www.intelligentcontract.com or call us on 0800 756 9711