BC LEGAL

BRINGING CLARITY

Web Application Software - Security Policy

January 2018

Owner: Terry Smith & Aden Fraser

Authors: Boris Cetnik — Director

Chris McCrudden — Head of Client Operations

Terry Smith — Head of Development

Aden Fraser — Lead Developer

Approver: Boris Cetnik

Signed:

Date: 03/01/2018

Implementation

Date	Version	Implementation Notes
03/01/2018	1.0	All implementation outlined in this document is pre-existing. Suggestions for additional implementation are clearly outlined and to be reviewed at the next review date.

Approval and Amendment History

Date	Version	Notes of Approval & Amendment
03/01/2018	1.0	First version of Software Information & Security Policies. Amalgamates previous internal-only IT and Software specific policies.

Review Date: 03/04/2018

Contents

1. INTRODUCTION

This document provides the policies in place for BC Legal's Software Information & Security and, in addition, notes the key objectives and the approach followed in order to manage information security and integrity.

BC Legal will keep all IT policies current, relevant and document controlled. All key objectives and the implementation approach will be reviewed at minimum every quarter and, where appropriate, modified or amended.

Any changes made will be communicated to and adhered to by BC Legal's staff. A copy of this policy is available to all third-parties using BC Legal's software.

Previous versions of this document will remain available in an archive. Physical copies of superseded documents should be destroyed.

2. SERVER HOSTING AND PHYSICAL ENVIRONMENT

At BC legal we need to deliver high availability products that are built to a high security standard, starting with the 'physical' equipment on which to deploy, run and test applications.

Traditionally, a physical infrastructure to achieve such a standard would require specialist teams and equipment. Maintenance of such an infrastructure is highly specialised and introduces many security challenges. To mitigate against any complications / issues as far as practicable, BC Legal use a 'hosted' solution.

When choosing a hosted solution, a priority was to ensure our existing standards were not compromised, including compliance with all appropriate national and international computer security accreditations. In addition, we required solutions providing industry leading security standards whilst maintaining high availability and transparency.

To satisfy our internal demands, our current products are hosted with Amazon Web Services (AWS) at their London, UK datacentre launched in 2016.

There are several security advantages to using AWS that gives the ability to ensure that our products are secure, compliant and demonstrably so.

2.1 NATIONAL AND INTERNATIONAL ACCREDITATIONS

AWS as the 3rd largest hosting company in the world and the leader in cloud computing solutions and as such has transparent accreditations for information security, data handling and organisation management.

As a global company the hosting options are split into regions. For compliance reasons we need to ensure that data is held within the UK mainland. AWS launched the UK London region in 2016 which is used for all our applications, as such we ensured that the following accreditations also specifically apply to said UK data centre.

AWS accreditations include ISO 27001 for security management, ISO 27017 cloud specific control and PCI DSS Level 1 (although BC legal does not process financial transactions online). It also holds ISO 27018 for personal data protection in storing PII data in the cloud.

It also holds the UK Cyber Essentials Plus and has been award the G-Cloud standard for specific infrastructure provided for the UK government to process data.

It complies to UK and EU data protection policies. Specifically, the EU data protection directive which will not apply to UK after Brexit but is essential for current platforms and the UK DPA - 1988 [1]

2.2 INDUSTRY LEADING SECURITY PRACTICES

When using any cloud provider, the key parts of the security stack we require they implement and secure are:

1. Physical computing resources
2. Networking internally and connectivity to the public internet with appropriate logging and auditing.
3. Designated entry points to physical hardware.

AWS provides high quality transparent practices to handle each one of these points. These are designed to comply with many international policies as well as UK ones such as PCI DSS Level 1 and ISO 9001 / ISO 27001.

Beginning with good physical environments with modern fire prevention and detection, UPS 24-hour power, high capacity for maintenance and device decommissioning AWS uses some good standard for device and security to the site, including 2 Form Factor Authentication, background checks, security monitoring and access logs.

The fault tolerant design and high uptimes is something that is very attractive about the platform and is a driving factor in choosing them as supplier.

Finally, the account security and access management are also to a high standard and well trusted. Each admin user must not only enter a password but a secondary form of identification such as short access generated on special apps linked to user specific mobile phones. This ensures that even if credentials are stolen they expire as soon as they are entered.

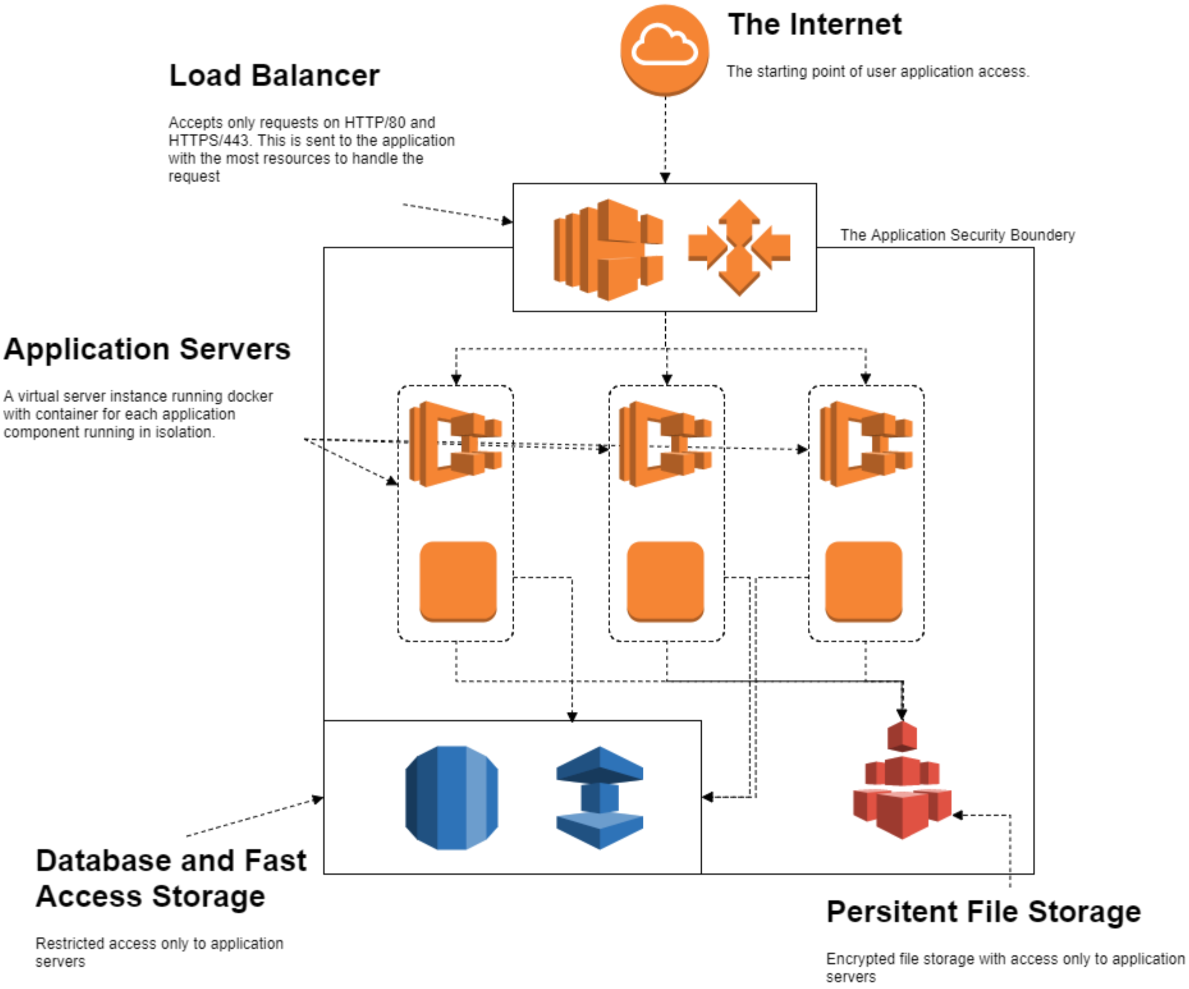
- Full details of the security practices are detailed in the whitepaper produced by AWS here.

[1] Full detail including certifications can be downloaded from https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/

- Details of Identity and Access Management program is here.
- Detail of Access log product is here and I have attached a sample log - event_history.csv
- Details of server log product is here and I have not attached a log as it contains IP address and other personally identifiable information.

3. ENVIRONMENT AND BACKUPS

To aid in the following section, please regard the below diagram using a high-level perspective of the application environment.


The Internet
The starting point of user application access.
Load Balancer
Accepts only requests on HTTP/80 and HTTPS/443. This is sent to the application with the most resources to handle the request
The Application Security Boundery
Application Servers
A virtual server instance running docker with container for each application component running in isolation.
Database and Fast Access Storage
Restricted access only to application servers
Persitent File Storage
Encrypted file storage with access only to application servers

3.1 OPERATING ENVIRONMENT AND SECURITY HARDENING

We have several methods to ensure the integrity of our systems in deployment. We have two security environment types, normally one per product:

1. Staging or UAT – A final testing environment that is a duplicate setup to the live environment. No PII or “real” data can be stored here.
2. Production – The live environment with customer data.

For the purposes of this section, both environments have the same security controls unless otherwise specified.

Each application is confined using the AWS security groups to its own environment. This includes database instance, static file resources and caching (if required). It defines the allowed entry and exist points. Our software allows public access to two ports HTTP/80 which redirects HTTPS/443.

Databases

Each database is given its own instance MySQL 5.6 RDS instance (RDS). This is the latest MySQL version available in the London, UK data centre. There is no external access to the database to read or write data. Database access is only through the application interfaces provided for updates/reads/writes and through defined database “migrations” as part of the application development process.

These allow us to tightly control any other access to these servers. For this purpose, the remote access via SSH or other access means is disabled at operating system and firewall level. Updates are performed using rolling updates to replace servers with new instances.

Security updates for this are scheduled weekly on a Wednesday at 23:00-01:00. This is after the AWS update notification that would be generated during the day. The uptime of the instances is maintained during the upgrade by applying updates to a “Stand by” instance and then replacing the existing “Primary” instance. This primary instance is then updated ready for the next update cycle.[2]

Our databases are encrypted within the instance itself. This ensures that any data “at rest” is un-obtainable other than through programmatic access. Access for the is control through application keys stored and backed up on AWS and are not for any other use[3].

Database backups can be either on demand or on a schedule and are stored as “snapshots”. Snapshots are also encrypted and are taken from the shadow copy database so that no impact is felt on the live system.

[2] Details of the RDS database maintenance cycle can be found here: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html

[3] Encryption techniques outlined in more technical detail here: https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#enveloping

There are two triggers for a database snapshot, one is when a new version of the application is deployed (to aid in roll backs) and also daily between 06:30 and 07:00.

These are stored using four different retention policies:

1. A daily snapshot is held for one week
2. Once a week a snapshot is captured that is held for 12 months
3. Once a month a snapshot is held for a year
4. Once a year a snapshot is create and held for 6 years.

This mean we can always restore from any point in the last 6 years by applying incremental difference in snapshot until we are back to the current position. If any snapshot(s) are deemed invalid, they can be skipped, and systems still be rebuilt to the last known good configuration.

Application Servers

BC Legal systems operate in a load balancing cluster. This means that new server instances are brought online as needed to meet customer demand. This "stateless" environment has some distinct security and data integrity benefits by design.

There are no physical servers but representations in the form of virtual machines referred to as "Instances". This give us the flexibility to deploy more instances as needed to handle demand and to update the core platforms as security patches are required.

Even though the instances are virtual, they still need to be secured and monitored as any operating system. There are still vulnerabilities, known and unknown, that may cause the server to become breached with a rootkit or other hard to detect system penetration.

We have two different approaches for updating server software, depending on the type of update:

1. Minor and Patch updates – Updates that are to a specific major version of the software [4]. These are applied weekly on a Tuesday to Staging Environments to allow for testing before they are rolled to Production environments on a Wednesday.
2. Major Software update – Major software updates normally involve more detailed research and risk assessments before they can be considered and would normally require more detailed manual testing and a custom structured release.

Access to individual instances is totally removed for any live environment and is granted to key individuals within BC Legal for the purposes of debugging and testing staging environments and deployments.

Individuals are granted access through a public keys exchange. These keys are generated via the AWS IMR control panel. Each key is recycled annually, and logs are kept defining the access rights of each key. Keys are then assigned to instances where access is allowed.

[4] For definitions of Major, Minor and Patch updates and software version numbers see here https://semver.org/

There are two individuals within BC Legal currently with this level of access:

1. Terry Smith – Head of Development
2. Aden Fraser – Lead Developer

Both are senior and well trusted individuals with clear background security checks and good references (these checks are carried out by our own internal fraud team).

Application Environment

To mitigate possible access to the core operating system through approved access points for software usage (i.e. The webserver), each instance installs "docker" as the only software directly to the instance. No web server or application logic can run directly on the actual instance. Instead it must run inside a "container".

This offers logical separation of the application code at the very core of the operating system with other benefits[5]. It raises the bar considerably to obtaining access or compromising the core instance as the core application files that are used to create the webserver or application are immutable (un-editable) inside the container.

We offer two file systems to the container, one with the application code needed to run and a writable storage layer.

No application code can be modified or removed by the web server or application. All application code is "read only" when presented to the docker containers with specific locations setup to store writeable data (documents or other uploads) in the system. As such, even with a fully compromised web server or application, the only data that can be edited is information that could be updated by a user in normal operation on the application.

User data is stored in a writeable storage layer that is contained within the application security group provided by the AWS Elastic File System (EFS). This is mounted by the instance and is offered as the only writable space to the application inside the container. Both metadata and the core data are encrypted so that no "data at rest" can be compromised outside the application access.[6]

This writable storage layer is backed up using an "EGS-to-EFS"[7] backup solution as recommended by AWS. This a daily backup between 06:30 and 07:00. Different projects have different size requirements and backups are dictated by that, but a minimal retention policy we use:

1. A daily archive is held for one week
2. Once a week an archive is captured that is held for 12 months

[5] Technical Detail of the security benefits of docker https://docs.docker.com/engine/security/security/

[6] For general FAQ's on file system encryption see here: https://aws.amazon.com/efs/faq/ for more detailed technical notes see here: https://docs.aws.amazon.com/efs/latest/ug/encryption.html

[7] Detail on the efs-to-efs backup solution https://docs.aws.amazon.com/solutions/latest/efs-to-efs-backup/welcome.html

Web servers are nginx v1.13.8 configured using the OWASP "Secure Configuration Guide" specifically as it pertains to nginx servers. This guide forms the basis of ensuring that correct headers are applied to each request where applicable, SSL certificates are configured correctly with the correct protocols and hashing algorithms, mitigation is taken against buffer overruns and otherwise.

PHP version is currently 7.1 with configuration based on current best practice. This is an evolving process through conjunction developer knowledge with Pen Testers as there is no default standard to PHP application hardening at the language level. The core language features, such as "safe_mode", is enabled and session handling is handled at application layer away from any default session language features. The restricted file access to the read only container means we can take a blacklist approach to disabling PHP features and functions. Currently there are no functions available to interpret code on the fly e.g. "eval" and "curl_exec" functions. We do not allow access to the core shell by disabling functions such as "passthru" and "shell_exec" to web requests and reflection functions designed to reveal source such as "show_source" are also disabled.

No third part PHP application, such as database managers or deployment tools, are installed on the web application. This reduces the attack surface and reduces burden on maintenance.

Application Deployment, Health checks and Configuration Updates

Finally, there is a gated application deployment method. When the application is deployed it must be by an approved staff member through the "Elastic Beanstalk" API using a dedicated deployment key[8] for each application. This sparks a series of automated steps that control application deployment. These are tested during the staging phase of deployment.

Sensitive information, such as database login details or application encryption keys, is stored in "environment variables" as part of the deployment. At no point is sensitive data written or stored in application code or in file format on the server. This ensures that compromised system is not vulnerable and access to application code cannot reveal sensitive information.

Each application deployment is stored in an S3 bucket in the London UK centre-this is the only file storage not encrypted. This is just application code as described before and does not contain sensitive information. This not encrypted as it needs to be launched to instances before the encryptions keys are available to read it. Access to this bucket is only through the application management console to responsible people inside BC Legal.

The application is not launched straight away to running servers, instead a separate load balancer is brought online with new instances added that match the existing load in the live system. Once the application is deployed, a series of health checks are performed to ensure that the status of the application is secure and ready for users. These are defined at application level as they change from product to product. This ensures that the application can run and has mitigation against security risk in the environment.

[8] Key access is maintained AWS Key Management with annual expiry

These final checks are to ensure application integrity and the environment has not been altered. The checks ensure:

1. Correct file/directories are not-readable
2. Correct files/directories are readable but not editable
3. Correct files/directories are readable and writable
4. Application keys and language specific items are available (i.e. application is using correct versions).
5. Database structure matches the current versions definition

If these final environment checks pass on all instances, then the system will switch to the new load balancer and decommission and destroy the old application version. This can be aborted until the final health check has passed.

Each application version is stamped with the user that deployed the application, the GIT SHA reference that identifies exactly which version from source control was updated (see Software Versioning Process), and date and time it was deployed.

If any additional monitoring alerts subsequently fail, or user issues are brought to light in the new environment, it can be rolled back to any of the previous 200 versions using the control panel or further using the GIT versioning system.

3.2 MONITORING AND LOGGING

To be able to react to threats in a timely fashion, detail the impact of any potential breaches and for customer compliance and confidence, logs are kept of the system activity, errors and access.

This logging applies to:

1. Any use of AWS credentials to access or configure the system or configuration either using programmatic or web panel access.
2. Access to any instance using ssh
3. Output of deploy scripts and docker logs from all instances
4. Any access via the web server
    a. Captures requested time
    b. Requester IP address
    c. Requested path or resource
    d. Requester method (http/https)
    e. Requester User agent
    f. Http Response code
5. Any web server error
6. Database access, error and slow query logs
7. Application errors and logging

Web application access is logged at application level. Please see section 5.7.

In addition to this several health metrics are also stored:

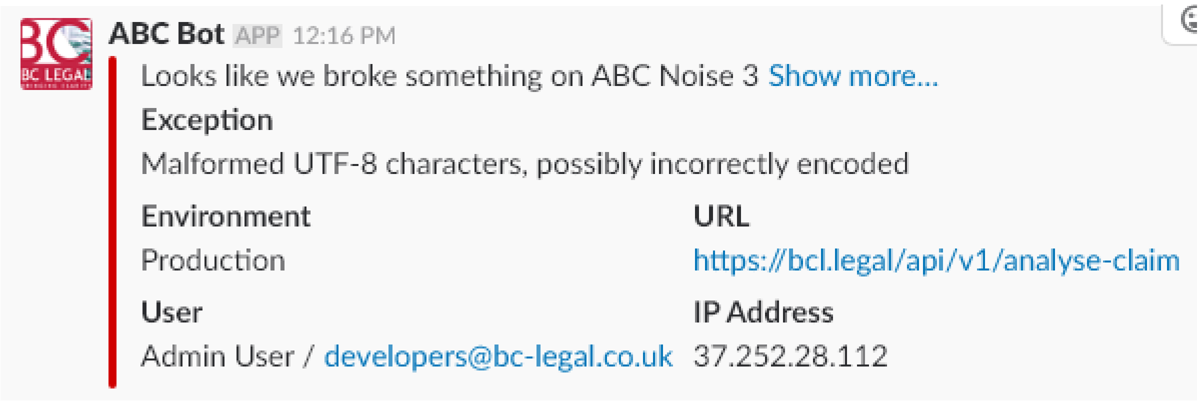
1. Network through put and response times
2. Instance CPU and memory usage
3. Application health (is the correct code version on all instances and is the correct number of instances ready for the number of uses).

Logs Management and Alerts

Logs from all instances are collated using AWS software "Cloud Watch". This enables to set alerts for specific log errors or warnings or environmental issues.

All alerts are forwarded as email to the developers@bc-legal.co.uk email address and instantly alerted in our team management tool "Slack". This enables us to move quickly to any errors or alerts from the system.

These are either "error" alert e.g.



ABC Bot APP 12:16 PM

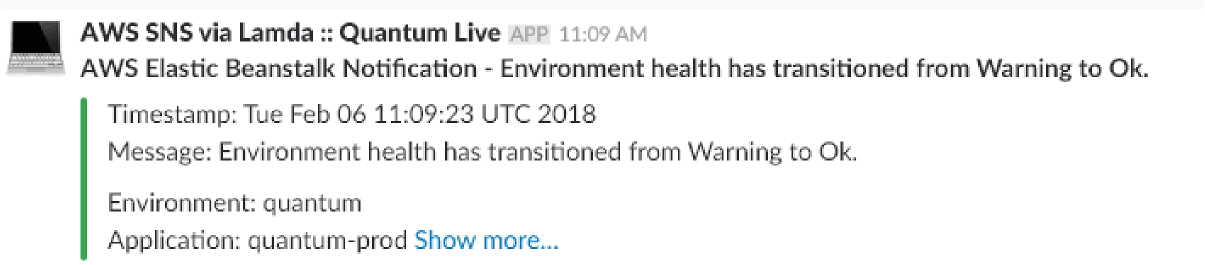
Looks like we broke something on ABC Noise 3 Show more...

Exception

Malformed UTF-8 characters, possibly incorrectly encoded

Environment	**URL**
Production	https://bcl.legal/api/v1/analyse-claim
User	**IP Address**
Admin User / developers@bc-legal.co.uk	37.252.28.112

Or an environmental or server log e.g.



AWS SNS via Lamda :: Quantum Live APP 11:09 AM

AWS Elastic Beanstalk Notification - Environment health has transitioned from Warning to Ok.

Timestamp: Tue Feb 06 11:09:23 UTC 2018
Message: Environment health has transitioned from Warning to Ok.

Environment: quantum
Application: quantum-prod Show more...

This can then be fed into either security response measures or development process. Security incident are always dealt with immediately.

Automated Vulnerability Scans

1. Trusted Advisor – A detailed look at how our configuration is currently setup and will advise us in real time to any setup or detected danger.
2. Amazon Inspector – A vulnerability scanner that can be configured to continually monitor your application externally. Sadly, this is not available to London, UK hosts but should be later next year.

We comply to all the current Trusted Advisor guidance. Please see the attached example report.

Trusted Avisor
Log.xls

4. APPLICATION SECURITY

Application security outlines the use of software, hardware and procedural methods to protect BC Legal's Software Applications from internal and external threats.

In order to stay up-to-date with the ever-changing security landscape and new and evolving attack vectors, the following procedures are in place as a requirement for all software developed and maintained.

It is not an exhaustive list of all methods used or guidance followed, as this is continually updating and is typically implementation specific.

4.1 OWASP

All software development undertaken by BC Legal's in-house software development team follows the guidance provided by OWASP (Open Web Application Security Project). OWASP is a non-profit group which provides impartial, practical information about application security used by individuals, corporations and government agencies worldwide.

The OWASP developer guidance provides major insight into the foundation, architecture, design, build, configuration, and operation considerations during the SDLC (Software Development Lifecycle). OWASP also provide a Testing Guide, Code Review Guide and the 'OWASP Top Ten' — which provides an insight into the top ten most critical Web Application security risks.

4.2 SOFTWARE VERSIONING PROCESS

BC Legal's software development team utilise GIT version control with pull requests and a two-member approval process to ensure a high-quality codebase.

This review process provides an 'extra pairs of eyes' to ensure the security and integrity of data within systems, whilst also providing a means of identifying and preventing malicious cyber-attacks, such as any attempted backdoor additions by a staff member.

4.3 DEVELOPMENT ENVIRONMENT

All BC Legal Software Developers work on local machines with either fake 'seeded' data in their local software databases or, where appropriate, an anonymised version of a production database.

BC Legal Software Developers store any form of PII or any form of data or information on their local machines. They also do not have access to this data (as outlined in the Access Control section) except in the format of an automatically anonymised version.

Our machines used for software development are encrypted and are part of the companies' AD (active directory). It is not possible to access the machine without a company login and the source code cannot be committed and changed to version control without the developer's SSH key and passphrase. The source code committed would then still be subject to the review process outlined previously.

The current development environment implementation prevents against both the possibility of leakage of information through accidental or purposeful means.

4.4 APPLICATION ACCESS

Access to BC Legal Software is restricted to the IP Addresses of organisations' that have registered for use of our software. Furthermore, an access policy exists which outlines the IP Addresses whitelisted for each organisation, preventing access from outside of defined constraints agreed by the organisation during the enrolment process.

This provides a multi-layer access approach as there is then a requirement for any malicious access attempt to be made from the internal network of an organisation enrolled in BC Legal's Software Suite.

All users who have access to BC Legal's Software receive an account which they can use to access all of the software that has been agreed to during the enrolment process. Their account is provided by BC Legal's Authentication System — BC Passport — which is an SSO (Single Sign-on) platform shared across all the software suite.

The SSO platform provides:

- A single email address and password combination shared across all software.
- Immediate revocation of access from all software, when required.
- An audit log of all access attempts, profile changes and action performed on all software by each individual.
- The ability to log-out of all software simultaneously from one location.
- A user lockout after a number of failed login attempts.

BC Legal intends to further its SSO platform's security offering with:

- 2FA (Two-factor authentication)
- LDAP Integration

All HTTP requests made by BC Legal Software during operation, once a user has been authenticated, are verified by the possession of a 'bearer' token provided by the software (as per OAuth 2.0 specification[9]) which can be revoked at any time. This results in:

- A 403-forbidden response being provided to the HTTP request.
- A log of the request attempt being stored.
- The request counting towards the 'rate-limit' (outlined later in this document).

4.5 USER PASSWORD POLICY

Users of BC Legal's Software must adhere to the password policy that has been outlined. All passwords must be:

- At least 8 characters long
- Must contain three of the following character types:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols

In order for a user to change their password, they are required to enter their existing password, preventing any malicious access change requests from occurring. All users' credentials expire every 90 days. If the uses goes beyond 90 days without resetting the password they must complete a password recovery option to confirm they have access to the original email account.

4.6 PASSWORD STORAGE

All passwords managed by the BC Legal SSO Platform are currently stored using the Bcrypt password hashing functions, based on the Blowfish cipher. Currently, all hashed passwords are stored with 10 rounds of hashing.

BC Legal's IT team has discussed the possibility of moving to Argon2i as their password hashing function of choice in the future, in order to keep up with the changing cyber-security landscape. Argon2i (vs BCrypt) is further optimized to resist side-channel attacks and is more difficult to attack.

At this time there is no decision made to transition from Bcrypt, which has been widely tested for 15 years and no known vulnerabilities exist, and there is no urgent requirement to make any change.

[9] The OAuth 2.0 Authorization Framework: Bearer Token Usage — https://tools.ietf.org/html/rfc6750

4.7 AUDITING AND LOGGING

BC Legal's Authentication System for all of its software logs all changes that a user creates chronologically. This is in addition to the aforementioned logging provided by the server's software security stack.

Through the combination of all available logs, access attempts can be identified and pinpointed to certain IP ranges, times and areas of the software. Any malicious attempts can be filtered out and blocked from the system, whilst audit logs also provide the opportunity to ensure data integrity should any suspicion arise.

4.8 ENCRYPTION & DATA TRANSPORT

All data transmitted to or from a client's machine with any piece of BC Legal Software is transported via HTTPS with a Qualys' verified `A Grade` SSL implementation.

Data that is transmitted between the different components of the BC Legal Software Suite is having its integrity verified using MAC (message authentication codes).

BC Legal would advise that any data to be transmitted programmatically between BC Legal's infrastructure and that of a third-parties, such as when implementing a technical integration between two systems, should follow the same transport security and integrity measures as outlined above.

4.9 RATE LIMITING

All access requests to BC Legal software are subject to rate limiting in order to prevent DoS (Denial of Service) and brute-force attacks. If a user or system attempts to make too many requests to any system without a certain amount of time, they will receive a 429 – Too Many Requests response and will subsequently be locked out until the number of requests is reset.

4.10 SESSION HANDLING

Most of BC Legal's software does not rely on session handling since a RESTful API is used. This API authenticates the user using an Authorization header with a bearer token. In the rare instance software sessions are used, they are stored in secure, encrypted cookies. It is not possible to reverse-engineer or fake these cookies.

4.11 SQL INJECTION

The framework within which the BC Legal tools are built has several layers of security and abstraction to prevent SQL injection. In addition to this, BC Legal's IT team avoid using raw SQL queries wherever possible, utilising the built-in in ORM instead. Where raw SQL is used, data is both validated and sanitized before a query is executed. Any interaction with the database is via prepared statements only which ensure parameter sanitation before the query is committed.

4.12 CSRF (CROSS SITE REQUEST FORGERY) PROTECTION

CSRF is an attack which performs an unwanted action on a website or piece of software that a user is authenticated with. The platform and framework that all of the BC Legal Software is written on provide protection against CSRF attacks.

This is achieved using a single use non-transferable code attached to every request. This must be parroted back to the server for the correct session to be approved. After each request a new access token is provided. This ensure that any session that may be stolen are invalid as soon as the user performs any action on the software.

4.13 XSS (CROSS-SITE SCRIPTING) ATTACKS

XSS attacks are a type of injection, in which malicious scripts are injected into a trusted website in order to perform an attack on an end-user. All of BC Legal's software is developed in a way to prevent these attacks from occurring, and two rounds of testing are performed in order to verify this:

- In-house Penetration Testing using Automated Tools
- Third-party Penetration Testing is undertaken by Accredited Security Experts

4.14 SECURITY HEADERS

All of BC Legal's web-based software regularly has its headers verified by a tool sponsored by Sophos, a leading security software and hardware group. These regular checks ensure that the proactive measures made during the development process following the guidance provided by the OWASP Secure Headers Project is adhered to.

The reason this is undertaken is to ensure that the correct headers are being set — those that provide security benefit — whilst also checking that any headers which would disclose software versions or other sensitive metadata are not included.

4.15 PENETRATION TESTING

BC Legal understands the importance of not just the rigorous internal security methods outlined above, but also the need for a third-party to audit the security measures in place, to perform penetration testing on its software and ultimately ensure an independent report is provided on BC Legal's obligation to ensure Information Security and Integrity.

Therefore, BC Legal has all of its software penetration-tested by a UK-based security consultancy once every quarter. The consultancy provides a wealth of experience with their CHECK Team Leader and a team of individuals with qualifications such as CCIE, CISSP and CEH, in order to identify any vulnerabilities or risks. BC Legal is then able to undertake a risk treatment plan.

Current approved suppliers are NCC group and Pen Test People.

A detailed up-to date list of current credentials for NCC group can be found here:
https://www.nccgroup.trust/uk/about-us/what-we-do/accreditations/

The company overview for Pen Test People with accreditations can be found here:
https://www.pentestpeople.com/company-overview/

5. BC LEGAL – PROFESSIONAL STANDARDS AND CERTIFICATIONS

BC Legal is working towards two business wide certifications at the moment- ISO 27001 and ISO 9001.

In the meantime, these standards are to be adhered to at all times.

5.1 STAFF DEVELOPMENT AND TRAINING

Staff and developers are trained on the most secure methodologies for the tools they use. Training is updated at least annually.

Each year developers must attend OWASP refresher training and at least one other certification. This year it will be the recent Laravel Certification[10] . It is at this application level the developers have most exposure and more efficient use of the framework helps boost security and speed up application development.

The development team will enrol on the Laravel Certification program and at least one member of staff must be Trained to AWS Systems Architect[11] and look to take the security exam as soon as the course is out of beta.[12]

[10] Laravel Certification - https://laravel.com/certification/

[11] https://aws.amazon.com/certification/certified-solutions-architect-associate/

[12] https://aws.amazon.com/certification/beta-exam/