www.bglcorp.com
info@bglcorp.com.au
1300 654 401

SECURITY WHITE PAPERS

1. Overview of BGL's Web Applications

BGL Corporate Solutions Pty Ltd (BGL) is Australia's leading developer of corporate compliance and self-managed super fund (SMSF) administration software solutions. BGL's cloud solutions include CAS 360, the next generation cloud corporate compliance software solution, and Simple Fund 360, Australia's leading cloud SMSF administration software solution.

BGL's award winning Simple Fund 360 and Simple Fund Desktop solutions are currently used to administer over 60% of Australia's 600,000 self-managed super funds. While CAS 360 and CAS Desktop are used in over 45 percent of Australian companies. BGL has over 8,000 clients in 15 countries using its product suite of compliance solutions for superannuation, company secretarial and general ledger. Our clients include all major accounting firms, law firms, many listed and private company groups, accountants, financial planners and many individual SMSF trustees.

CAS 360 has changed the way ASIC corporate compliance work is done in Australia. CAS 360 automatically downloads Annual Company Statements and Company Debt reports from ASIC each day. The Annual Review process compares ASIC and CAS 360 data automatically and then prepares the Annual Reviews for clients. Debt is managed and deadlines for lodgement of documents are all controlled through smart alerts.

At same time, Simple Fund 360 has revolutionised the SMSF administration space, with intelligent algorithms that significantly reduce the amount of time required to process an SMSF, Simple Fund 360 is the complete SMSF compliance solution that automatically matches bank, broker, corporate action and dividend data overnight by using BGL's SmartPost technology. BGL has been providing software solutions to accountants, SMSF administrators, lawyers, financial planners and professional firms for over 30 years. The economies of scale that BGL's services, in collaboration with our cloud hosting provider Amazon Web Services (AWS), make it possible for BGL to provide higher levels of physical and digital security than many of our clients have on their own systems.

From sophisticated data matching, artificial intelligence, deep learning technology and big data analytics to seamless document delivery, digital signing and two-way integration with over 350 ecosystem partners, BGL eliminates manual data entry, ensure businesses are compliant with ASIC and SMSF laws as well as gives accountants back time to focus on delivering remarkable moments to their clients while boosting their productivity, profitability, growth and team satisfaction.

2. Data Security

BGL's cloud solutions, CAS 360 and Simple Fund 360, successfully achieved ISO 27001 certification in January 2020. This is testimony that delivering efficient, reliable, and secure cloud solutions is BGL's highest priority. BGL's infrastructure and online software security is regularly reviewed by external security specialists. These highly trained specialists run penetration tests every six months to systematically identify and exploit any security flaws in the CAS 360 and Simple Fund 360 web applications. This testing is done in accordance with OWASP Application Security Verification Standard 3. OWASP is a worldwide not-for-profit charitable organisation focused on improving the security of software. In addition to running regular external tests, CAS 360 and Simple Fund 360 servers run the latest UNIX based operating systems, firewalls, and have perimeter based security policies applied which protect against unauthorised service access. Requests to internal hosts are logged and monitored continuously to ensure that only authorised internal clients are accessing the services.

3. Data Backup Control

CAS 360 and Simple Fund 360 have been designed to support mission-critical databases. Databases are replicated across multiple servers and across multiple Availability Zones (AZ's). BGL performs complete backups of data every hour and each night, to ensure the Recovery Point Objective (RPO) is not greater than one hour. BGL also ensures the implemented storage solutions are highly scalable, durable, and reliable for backups.

4. Security Standards are used

BGL's CAS 360 and Simple Fund 360 applications are signed by an Secure Socket Layer (SSL) certificate, which means that all data transferred between the Internet Browser and the applications is encrypted.

The CAS 360 and Simple Fund 360 Secure Socket Layer (SSL) connections utilise the latest perfect Forward Secrecy. This security feature uses a derived session key to provide additional safeguards against the eavesdropping on encrypted data. This prevents the decoding of captured data, even if the secret long-term key is compromised. In addition to that, the application load balancer uses the latest Elliptic Curve Cryptography (ECDHE) cipher suites, which most internet browsers currently support, in order to ensure that newer and more secure cipher suites are available for our clients. For that reason, we always advise clients to use the latest versions of their browsers to make use of these stronger cipher suites for communication.

In order to secure end user access, credentials with complex passwords and MultiFactor Authentication (MFA) is required to login. For password resets, end users receive password reset emails directly to their email address. Users can only access information they have permission to view. Access in CAS 360 and Simple Fund 360 are role-based, where the Practice Administrator can create accounts and assign permissions depending on the role of the user. He/she has complete control on who can access which data in the application. All User accounts have an audit trail with logs that include the performed action and the IP address from where the action was performed.

5. Hosting

All CAS 360 and Simple Fund 360 data is hosted and stored in AWS in Australia using multiple Availability Zones (AZ's).

5.1 BGL uses world class Hosted Data Centres

BGL's chosen Data Centres are located in Australia and isolated from BGL's own internal office networks. Only strictly controlled BGL staff with authorisation can remotely access the servers which house the data. BGL regularly reviews access control and when an employee no longer has a business need for these privileges, his or her access is immediately revoked.

BGL uses Amazon Web Services (AWS) world-class, highly secure data centers utilizing state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards and access is authorized strictly on a least privileged basis.

5.2 Storage Device Decommissioning

When a storage device has reached the end of its useful life, a decommissioning process - designed to prevent customer data from being exposed to unauthorized individuals - is employed. The chosen data centre uses the techniques detailed in DoD 5220.22M ("National Industrial Security Program Operating Manual") or NIST 80088 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry standard practices.

5.3 Security Controls

The Data Centre built on an environment with extensive and validated security and controls, including:

- Service Organization Controls 1 (SOC 1) Type 2 report (formerly SAS 7011 Type II report), with periodic independent audits to confirm security features and controls that safeguard customer data.
- ISO 270001 Certification, an internationally-recognized security management standard that specifies leading practices and comprehensive security controls following the ISO 27002 best practice guidelines.
- PCI DSS12 Level 1 compliance, an independent validation of the platform for the secure use of processing, transmitting, and storing credit card data.
- Relevant government agency and public sector compliance qualifications, such as an ITAR-compliant environment.
- AWS Security Compliance Programs: **https://aws.amazon.com/compliance/programs/**

5.4 Service Availability

Whilst BGL intends the Software will be available 24 hours a day, seven days a week, 365 days a year, it is possible on occasions the Software may be unavailable for reasons within the control of BGL (ie: for scheduled or unscheduled Software updates) or for reasons outside the control of BGL (ie: the data centres have power outages and all backup generators fail).

BGL uses reasonable endeavors to notify you in advance of any planned outages and will notify you as soon as possible of any unplanned outages. BGL will use commercially reasonable efforts to make the Software available with an uptime percentage of at least 99.9%.

The BGL Service Status page is - **https://status.bgl360.com.au/**

6. Privacy of my data

It is BGL's priority to ensure the security and privacy of data. BGL continuously ensures all its employees handle and treat data with the utmost privacy. In addition, BGL applies the least privilege access principle on its employees and controls all access to the AWS cloud storageservice (Simple Storage Service (S3) buckets) and databases through well-defined Identity and Access Management (IAM) policies- **http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html** BGL's Privacy Policy can be found at **http://www.bglcorp.com/about-bgl/privacy-policy**

12. Disaster Recovery

All CAS 360 and Simple Fund 360 are multi-tenanted applications using AWS Multi-Availability Zones, hence the applications span across multiple distant data centres. Redundant instances for each tier (e.g. web, application and database) of an application are placed in distinct Availability Zones thereby creating a multi-site solution. The Database and the cloud storage resource (Simple Storage Service - S3 bucket) are also backed up to the AWS Tokyo Region. In the unlikely case that all three AWS data centers in the Sydney Region are unavailable, BGL would utilise the AWS Tokyo and manually bring the applications back online. The replicated data to AWS Tokyo is encrypted in transit and at rest.

Disaster Scenario	Expected RTO
AWS EC2 Failure in Single Availability Zone	Zero - No Impact
AWS EC2 Failure in Multiple Availability Zones	4 Hours

13. Cloud Subscription Agreement

BGL's cloud software subscription agreement can be found **here**.

7. Monitoring

For monitoring, BGL utilises:

- Amazon services utilised to monitor server and database health
- Third party software for additional monitoring of servers and of BGL 360 applications
- Email and SMS alerts to keep relevant BGL staff notified of critical alerts

8. Data management lifecycle (creation, storage, retention, removal)

BGL retains customer data for 5 years after a subscription expires. Customers are able to delete their own data at any point before the 5 years expiration date. Management of the physical servers is handled by AWS. When a storage device has reached the end of its useful life, AWS destroy data as part of the decommissioning process - ***For more information please refer to 5.2***

9. Encrypted connections between BGL and Amazon

The infrastructure of all BGL cloud solutions are located and hosted at AWS. BGL employees access the infrastructure either through the AWS management console with a web browser or through a secure Virtual Private Network (VPN) connection. A connection with a Web Browser is encrypted through the 256-bit Secure Socket Layer (SSL) certificate and a connection through the Virtual Private Network (VPN) is encrypted with the Virtual Private Network (VPN) certificate to ensure a secure tunnel connection to the infrastructure.

10. Encryption of data

CAS 360 and Simple Fund 360 are Web Applications accessible through Internet Browsers. To ensure protection and confidentiality of the data flowing between the end user and Web Application, BGL uses a 256-bit Secure Socket Layer (SSL) certificate to securely encrypt the transmitted data.

BGL also ensures critical or identifiable fields such as TFN's are encrypted at rest using 256-bit Advanced Encryption Standard (AES) encryption keys.

To find out more about data encryption read - Encrypting Data at Rest - **https://d0.awsstatic.com/whitepapers/AWS-Securing-Data-at-Rest-with-Encryption.pdf**

11. Data Backup

BGL utilises the AWS database called the Relational Database Service (RDS). There is a default scheduled backup, operated by AWS, for the Relational Database Service (RDS) that occurs once every 24 hours. In addition, BGL has scheduled another Relational Database Service (RDS) backup/snapshot to run on an hourly basis, which shortens the reversible point-in-time to one hour.