

# AN AUDITORS GUIDE

Prepared by  
BGL Corporate Solutions Pty Ltd  
March 2018

# CONTENTS

- 1.0 Overview of BGL's Web Applications**
- 2.0 Data Sources and Services**
  - 2.1 Bank Data
  - 2.2 Dividends / Distributions Received
  - 2.3 Contract Notes (for security purposes and sales)
  - 2.4 Wraps and Platforms
  - 2.5 Registry Data
- 3.0 Audit Features in Simple Fund 360**
  - 3.1 Gaining Access to Simple Fund 360
  - 3.2 Audit Reports
  - 3.3 Other Functions and Reports
  - 3.4 Audit and the Documents Screen
  - 3.5 Using Document Tags to Help the Auditor
  - 3.6 Integration with Third-Party Audit Software
- 4.0 Overview of BGL Web Application Infrastructure and Controls**
  - 4.1 Policies
  - 4.2 Physical Data Hosting and Security
  - 4.3 Data Backup Controls
  - 4.4 AWS Access Control
  - 4.5 Change Control Process
  - 4.6 Infrastructure Monitoring
  - 4.7 Transport of Data
  - 4.8 Internal Security Assessments
  - 4.9 External Vulnerability Assessments
  - 4.10 Sensitive Database Fields
- 5.0 User Security**
  - 5.1 User Access
  - 5.2 Logging of User Activity
- 6.0 Privacy of Data**





# INTRODUCTION

The purpose of this guide is to assist auditors in gaining a better understanding of BGL's web applications and how auditing in the Cloud can streamline the audit process.

This guide is divided into six sections:

**Section 1** provides an overview of BGL's web applications.

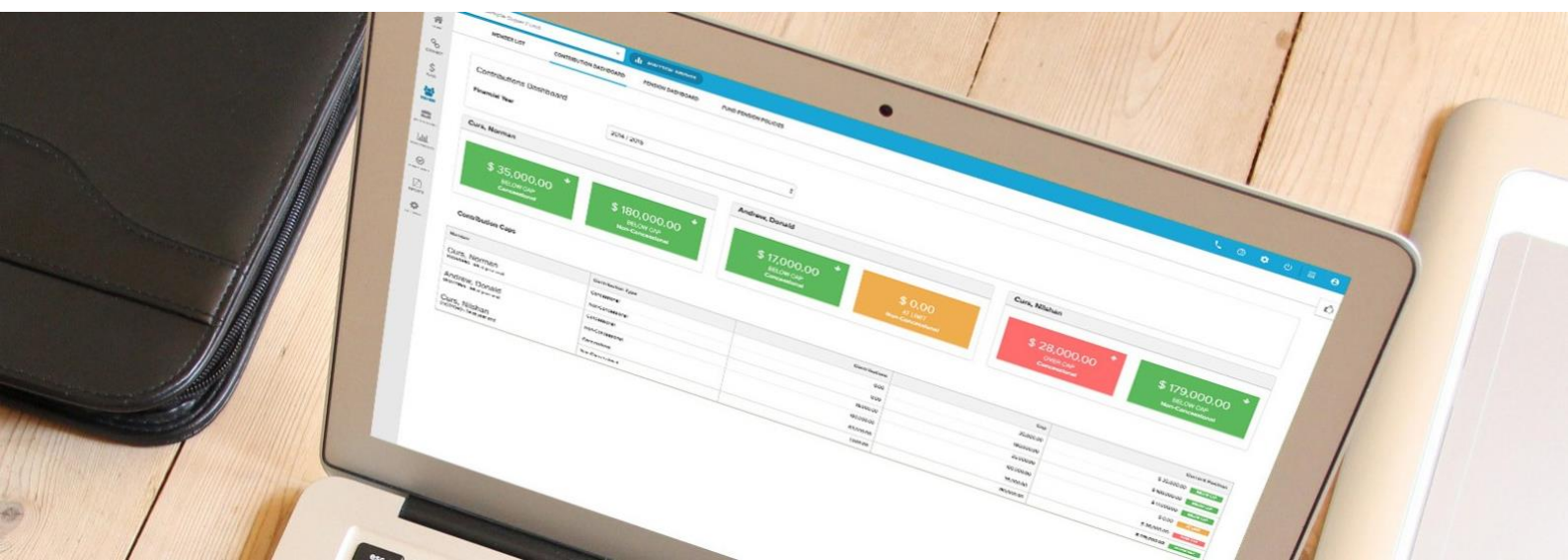
**Section 2** contains an overview of BGL's data sources and how the data is used in each BGL application.

**Section 3** contains an overview of the Simple Fund 360 audit functionality.

**Section 4** contains an overview of BGL Web Application Infrastructure and Controls.

**Section 5** contains an overview of User Security.

**Section 6** contains details of BGL's Privacy Policy



## 1.0 Overview of BGL's Web Applications

---

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

BGL software solutions are used to administer over 70 percent of SMSFs and over 45 percent of Australian companies.

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 using BGL's **SmartPost** technology, while Australian Securities Exchange's (ASX's) managed funds and international share prices provide daily portfolio valuations.

BGL has been providing software solutions to accountants, SMSF administrators, lawyers, financial planners and professional firms for over 25 years. The economies of scale that BGL's services offer, together 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.

## 2.0 Data Sources and Services

---

### 2.1 Bank Data

All BGL bank data is received directly from the banks. Eighteen financial institutions are currently supported, with more added on a regular basis. Simple Fund 360 ensures the bank balance in the bank data file received from the bank reconciles with the balance in the software each day. Balances are displayed on the Fund Dashboard screen, with any differences highlighted.

### 2.2 Dividends / Distributions Received

Dividends / distributions received in cash are matched with the ASX dividend / distribution data. Simple Fund 360 ensures the dividend / distribution amount per share x units on hand agrees with the dividend / distribution amount. If not, the cash dividend / distribution transaction is flagged for user review. If Simple Fund 360 does not receive a cash dividend / distribution, a corporate action for a potential dividend reinvestment plan (DRP) is automatically created.

### 2.3 Contract Notes (for security purchases and sales)

BGL's Contract Note Service extracts the buy / sell data from the PDF formatted contract notes received from brokers. Over 110 brokers are supported. The data is matched against buy and sell cash transactions. The contract note PDF is then attached to the Simple Fund 360 transaction and can then be viewed on Transaction List and in Document Management. Simple Fund 360 will automatically match unlimited, multiple buy and sell transactions against a single cash amount on a single day.

### 2.4 Wraps and Platforms

All wraps and platform data is received directly from the wrap or platform. Simple Fund 360 ensures the wrap / platform balance in the wrap / platform file received from the wrap / platform provider reconciles with the balance in the Simple Fund 360 software each day.

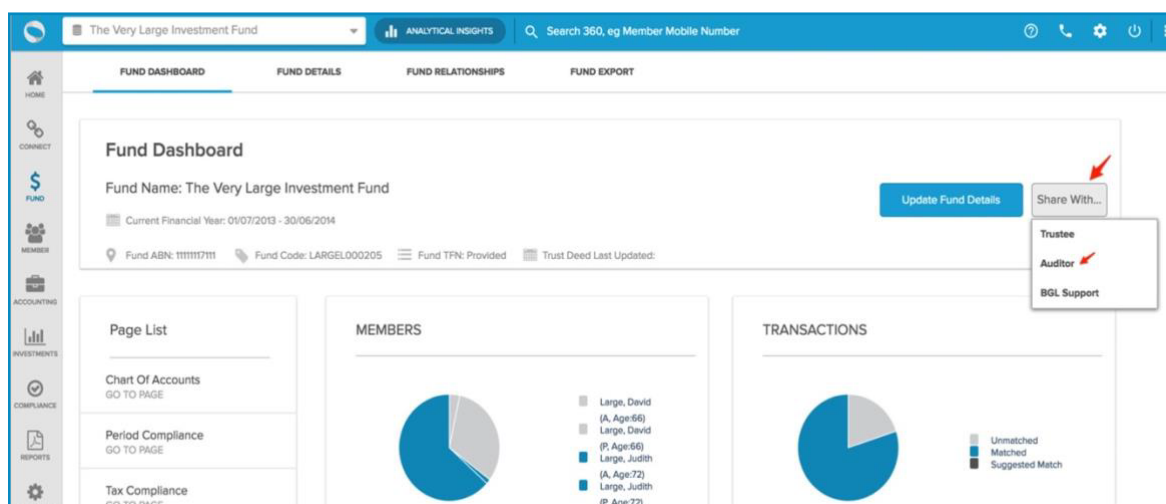
## 2.5 Registry Data

Simple Fund 360 provides a direct link for holding balances to the Computershare and Link registry data. On the Simple Fund 360 Investments | Balance Review screen, holding balance data received from the registries is compared with holding balances in Simple Fund 360 with differences highlighted. This data is obtained from input of the fund's HIN(s). The registry data cannot be accessed by Simple Fund 360 clients. The registry is the Source of Truth for all listed holding balances. These connections ensure holding balances in Simple Fund 360 are independently verified.

## 3.0 Audit Features in Simple Fund 360

### 3.1 Gaining Access to Simple Fund 360

Auditor access to Simple Fund 360 can be provided by the software administrator. The simplest way to invite an auditor is to go to the Fund | Fund Dashboard and select Share With | Auditor.



Complete the auditor's name and e-mail details and click Invite. This will provide the auditor with audit access to Simple Fund 360 based on the auditor's user role.

**Invite Auditor**

You can invite users such as Clients, Employees, Auditors and Advisors to review the information on this Portal. Fill in the details password when they first log in.

From the Administration | Setup menu, you can both edit permissions for the User Roles and the invitation email template.

**Auditor Details**

First Name:

Last Name:

Email:

The auditor will receive an e-mail invitation to log in and create a password.

The auditor then will be able to access:

- Some dashboards;
- Reports;
- Live reports;
- Documents.

The software administrator can provide the auditor with access to additional functions.

### 3.2 Audit Reports




Simple Fund 360 provides users with a full set of audit documentation and reports provided by TAG Financial Services Pty Ltd.

These reports are available from Reports | Audit Reports.

The settings available for these reports are:

- Audit Planning Memorandum;
- Audit Working Papers;
- Compendium Index;
- Engagement Letter;
- File Index;
- Management Letter;
- Trustee Representation Letter.




**Audit Planning Memorandum 2016**

Prepared by:	<input type="text" value="Ron Lesh"/>	
Date prepared:	<input type="text" value="03/11/2016"/>	
Completed by:	<input type="text" value="Ron Lesh"/>	
Completed date:	<input type="text" value="03/11/2016"/>	
Reviewed by:	<input type="text" value="Ron Lesh"/>	
Reviewed date:	<input type="text" value="03/11/2016"/>	

The settings available for these reports are:

- Compliance Checklist;
- Fraud Checklist.

**Compliance Checklist 2016**

Checklist Template:	<div style="border: 1px solid #ccc; padding: 2px;"> Please select... ▼  Please select...  Template  High  Medium  Low </div>	
Prepared by:	<input type="text"/>	
Date prepared:	<input type="text"/>	
Completed by:	<input type="text"/>	
Completed date:	<input type="text" value="03/11/2016"/>	
Reviewed by:	<input type="text" value="Ron Lesh"/>	
Reviewed date:	<input type="text" value="03/11/2016"/>	



### 3.3 Other Functions and Reports

In addition to audit reports, the following reports can assist the auditor:

- Fund Dashboard | Bank Statement Report: Provides a verified bank balance taken from the data file provided by the relevant financial institution;
- Fund Dashboard | Bank Balance;

DATA FEEDS				
<a href="#">View Bank Statement</a>				
ACCOUNT DESCRIPTION	FEED PROVIDER	FEED STATUS	BALANCE IN 360	STATEMENT BALANCE
Commonwealth Bank of Australia 067-167	BGLBankDataService	Feed Operating	\$30,529.64	\$30,529.64 19/10/2016

There are a number of reports to assist auditors in the Reports | Work Paper Reports and Reports | Investment Reports areas of Simple Fund 360.

The reports provide the General Ledger – Audit View and many other reconciliation and comparison reports covering most Operating Statement items.

The Reports | Documents screen provides access to all source documents and reports created and uploaded for the fund. Tags can be created to classify documents by audit year.

Simple Fund 360 also provides a transaction drill down tool for all ledger accounts. This is accessed through Reports | Live Reports. This tool is available for Accounting Performance, General Ledger and Trial Balance Reports.

### 3.4 Audit and the Documents Screen

The Reports | Documents screen allows the trustee, administrator and auditor to store and share the fund's documents. Trustees can upload permanent documents, such as trust deeds or annual documents, including dividend, distribution and tax statements. The accountant can add working papers and other documents to support fund transactions. The auditor can then log in, view and / or download documents.

### 3.5 Using Document Tags to Help the Auditor

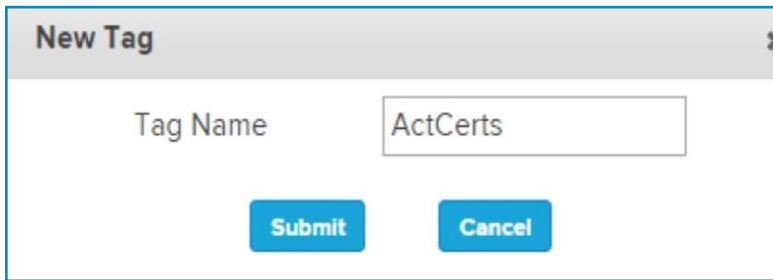
BGL recommends that the accountant create document tags for group documents. Tags are similar to folders on a desktop computer except multiple tags can be applied to multiple documents, whereas a document only can be placed in a single folder.

To add a new tag, select Add Custom Tag on the left of the software screen.

[Add Custom Tag](#)



The New Tag screen will appear. Input the tag name and click Submit.



To apply the tag to the document(s), select the checkbox to the left of the document(s) and select Tag As at the top of the screen. Select the appropriate tag(s) and then select Apply Tags.

BGL recommends creating a Permanent tag and an Audit (Year) tag for each financial year.

Audit Reports including Engagement, Representation and Management letters can all be stored in Simple Fund 360.

### 3.6 Integration with Third-Party Audit Software

Simple Fund 360 also provides integration with [Caseware](#), [Cloudoffis](#), [Evolv White](#) and [MyWorkpapers Audit](#). Audit integration with Simple Fund 360 is implemented through the BGL Application Programming Interface (API).

While the process is different in each package, the data extracted through the API consists of:

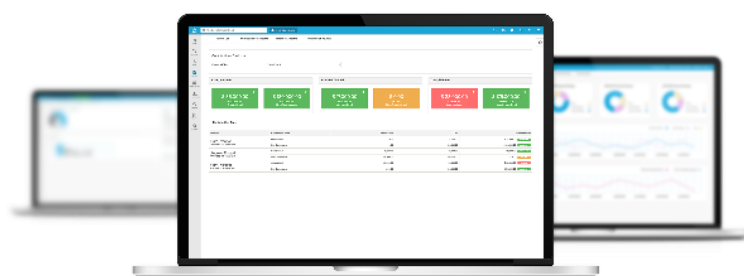
1. Import of the Simple Fund 360 fund list: Fund, member and trustee data is loaded.
2. Import of the Trial Balance: The audit application dynamically creates and populates folders, lead schedules and lead schedule summaries.
3. Report data and Report PDFs

For more information on the data extracted by each supplier and how to integrate, refer to website of each software supplier.

## 4.0 Overview of BGL Web Application Infrastructure and Controls

### 4.1 Policies

BGL has documented policies and procedures for risk assessment, data security, release management, security operations, incident management, privacy, visitor policy, confidential trash, new employment, employee conduct and termination of employment. Background screening, professional credential checks and police checks are conducted on team members. Policies are reviewed as required. BGL has employment contracts with all team members that comply with the Fair Work Act.



## 4.2 Physical Data Hosting and Security

All BGL client web data is hosted in Australia by Amazon Web Services (AWS). Data is stored across multiple zoned replicas. AWS services are isolated from BGL's own internal office networks. No BGL staff can physically access any of the servers.

BGL employs team members who maintain the data and servers housed at AWS. These team members are appropriately authorised to remotely access the servers. BGL regularly reviews these access controls.

AWS's data centres are state of the art, utilising innovative architectural and engineering designs. AWS has many years of experience in designing, constructing and operating large-scale data centres throughout the world. This experience has been applied to the BGL Hosting Platform and Infrastructure.

The Australian data centres are housed in nondescript facilities. Physical access is strictly controlled, both at the perimeter and building ingress points, by security staff utilizing video surveillance, intrusion detection systems and other electronic means. Authorised staff must pass two factor authentication at least twice to gain access to the data centre. All visitors and contractors are required to present identification, are signed in and then escorted by authorised staff. When an employee no longer has a need for access, this is immediately revoked, even if the individual continues to be employed by AWS. All access to the data centres is logged and routinely audited.

When a storage device reaches the end of its useful life, a decommissioning process ensures data is not exposed to unauthorised individuals. AWS uses techniques detailed in DoD 5220.22M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("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 standards.

AWS is built in 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 to safeguard customer data.
- ISO 270001 Certification, an internationally-recognized information security management standard that specifies leading practices and comprehensive security controls that follow ISO 27002 best practices guidelines.
- PCI DSS 12 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.

More information on AWS security can be found at:

[https://d0.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Whitepaper.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf)

No BGL client web data is hosted at BGL's offices. BGL's offices are protected by card controlled entrances and monitored alarms, with all actions logged.

BGL clients can share data with BGL support consultants. This can be authorised when a user logs a support call with BGL and selects the appropriate option in the software. This option provides the BGL support consultant with access to fund data for five days. After five days, access is automatically revoked. The client can revoke access at any time.

## 4.3 Data Backup Controls

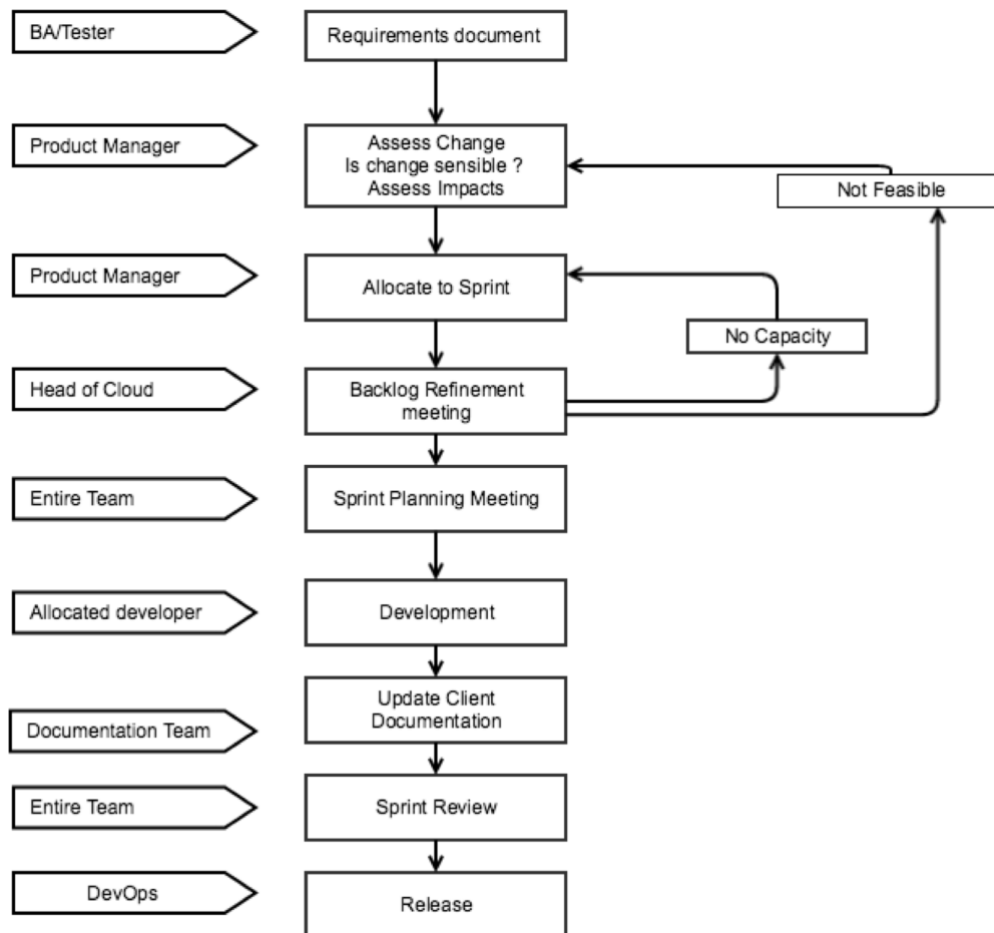
BGL web applications use mission critical databases. Databases are replicated across multiple servers and multiple AWS availability zones. Data backups occur every two hours during the day. Full data backups are also taken each night. BGL has a documented disaster recovery plan.

#### 4.4 AWS Access Control

Access to the AWS production environment is available to authorised BGL team members via a virtual private network (VPN). A list privilege model determines who has access. BGL follows AWS security best practices and rotates access keys. All activity is logged and accounts are reviewed on a regular basis.

#### 4.5 Change Control Process

BGL uses mixed Agile methodologies to releases updates every three weeks. The release cycle for application changes is described below



BGL has three environments: User Acceptance Testing (UAT), Staging, and Production. A Configuration Management Tool confirms that patches and updates have been successfully applied to the servers. BGL's continuous integration deployment will not commit unconfirmed changes to production servers until integration tests are passed.

BGL has a separate policy for updating Amazon Relational Database Service (RDS) instances. All minor upgrades to RDS are done in test environments before being placed into production. All major updates reside in the UAT environment for at least two sprints.

#### 4.6 Infrastructure Monitoring

AWS tools are utilised to monitor server and database health, in addition to third-party software utilised for additional monitoring of application servers. These services send e-mails and SMS messages to notify team members of any critical alerts. All access and changes to the database are tracked and logged.

#### 4.7 Transport of Data

BGL's web applications are signed by a secure sockets layer (SSL) certificate, meaning all data transferred between AWS and the Internet browser is done with strong encryption and authentication, the same certification as Internet banking.

The SSL connections utilise the latest Perfect Forward Secrecy. This security feature uses a derived session key to provide additional safeguards against the eavesdropping of encrypted data and prevents the decoding of captured data, even if the secret long-term key is compromised. The load balancer utilises the latest industry standard cipher suites. Most major browsers now support these newer and more secure cipher suites. BGL encourages clients to use the latest browser versions that include these stronger cipher suites for communication.

#### 4.8 Internal Security Assessments

Regular security training is conducted by necessary BGL team members. Open Web Application Security Project (OWASP) methods for security testing are conducted by BGL testers and developers. The application code is regularly scanned for vulnerabilities.

#### 4.9 External Vulnerability Assessments

BGL's infrastructure and online software security are regularly reviewed by external security experts. These highly trained specialists run penetration testing to identify and exploit any security flaws in BGL's web applications. The testing conforms with the Application Security Verification Standard 3.0 Open Web Application Security Project.

#### 4.10 Sensitive Database Fields

All sensitive database fields, such as tax numbers and bank account details, are encrypted using the latest cryptographic algorithm method.

## 5.0 User Security

### 5.1 User Access

A user role and identity system prevents users from accessing data that is not their own.

Users can access the system by invite only, with access to information determined by user roles. Access is username and password protected. Access to BGL web applications is role-based, meaning the BGL client administrator has complete control over who can access data. Users are required to change their password at the first log in, with the new password sent to the user's e-mail address. BGL enforces complex passwords. Users are automatically logged out due to inactivity after a set period of time.

### 5.2 Logging of User Activity

All user access is logged, including IP address, log-ins, failed log-ins and activity in the application.

## 6.0 Privacy of Data

BGL treats all data with the utmost privacy.

BGL's privacy policy can be found at: <http://www.bglcorp.com/about-bgl/privacy-policy>.

