CLIENT PRIVACY & DATA SECURITY

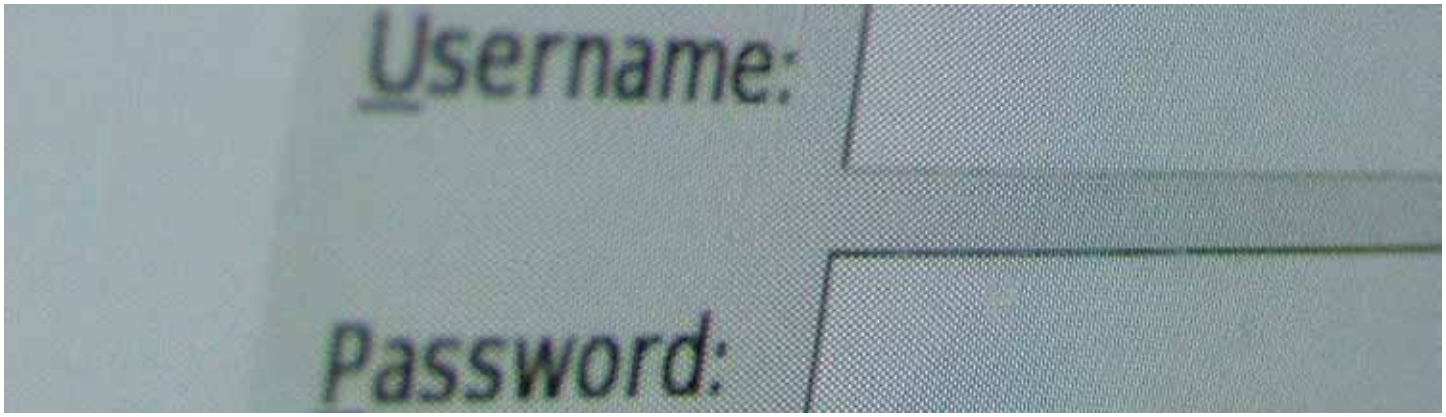
CLOUDFORCE
BUSINESS SUPPORT

PRIVACY AND DATA SECURITY

CloudForce takes client Privacy and data Security very seriously. Our priority is making sure your information is kept safe and secure at all times.

To prevent unauthorised access and ensure the correct use of your data, we have implemented appropriate physical, technical and administrative measures to safeguard and secure the data we receive from you.

We are always looking at ways to improve security systems and we will continue to invest in new security capabilities into the future. As technology changes and new threats emerge, we aim to keep ahead of any new risks.



CLIENT PORTAL SECURITY

CloudForce uses Nimbus Technology to provide its secure client portal.

Nimbus Physical Security

- Nimbus hosts your files using high performance, fault tolerant servers replicated across multiple, widely separated, world class data centres to ensure the best possible physical protection of data designed to achieve a 99.985% up time.

- Access to the server floor in these data centres is strictly controlled and limited to data centre technicians holding electronic pass cards. Buildings are under 24/7 continuous monitoring, internal and external video surveillance, with additional external surveillance by security guards.

- Connectivity is assured at each data centre via multiple backbones to independent transit IP providers, using Border Gateway Protocol (BGP4) to determine best case routing.

- Live server replication over long distances, coupled with a third stage backup regimen, ensures that your data is protected against any form of natural disaster that could take out an individual data centre. In the unlikely event of a data centre going off line, hosting switches to an alternate data centre.

Nimbus Electronic Security

- Nimbus servers are protected behind industry leading firewalls and locked down to only the secure protocol used to communicate with Nimbus. There is no FTP access to Nimbus hosts, no publisher services enabled, no directory browsing through standard web protocols, no user or guest account access to the server OS and data centre staff have no electronic access to the servers.

- All user communication with Nimbus servers is via https, an encrypted and secure protocol, thus preventing data taps, electronic eavesdropping or data siphoning en-route between user and Nimbus hosts. As a further safeguard, firewalls, routers and switches within the data centre are continuously monitored electronically for abnormal activity.

- Nimbus servers are continuously monitored with several levels of error and activity logging, including SMS and email alerts to Nimbus Technology support staff.

Nimbus Business - Safe, Secure and Simple to use

All business and client files hosted on Nimbus servers are encrypted with a sophisticated state-of-the-art algorithm, uniquely keyed to each Business account, thus uploaded files are not readable by Nimbus Technology support staff, nor would be readable to other Businesses or any other persons gaining authorised or unauthorised access at the server directory level.

User Access Security

- In Nimbus, each Business is allocated a unique high precision identifier, which is used to encode the URLs for both the Business site and Client portal. Thus, knowledge of one Business or Client Nimbus URL does not provide a URL to any other Nimbus Business site or Client portal, as the chances of correctly guessing another businesses' ID is infinitesimal.

- Even if an unauthorised person acquires knowledge of a Business URL, they still need a valid login and password to gain access. All passwords in the Nimbus database are stored with a "one way" encryption, thus even perusal of database tables cannot yield login credentials.

- Nimbus also prevents employees and clients from sharing login codes, thus ensuring that all logins are unique within each Business database. Similarly, unique Client login prevents inadvertent access to another Client's files.

CLOUD ACCOUNTING SECURITY

How is Cloud Accounting more secure than desktop software?

With Cloud Accounting, your data is not stored on your computer – if your PC or laptop crashes, gets lost or is stolen, all of your data remains completely safe and unaffected.

By allowing your accountant or bookkeeper to have secure access via Cloud Accounting, it is much more secure than sending your data via email, disc or USB.

At CloudForce we are set up to use all Cloud based accounting software, however Xero, MYOB and Reckon are our preferred partners. If your preferred software is not on our list, we have the systems and expertise in place to use any Cloud Accounting Software.

Each one of these Cloud accounting software suites has been carefully chosen for their functionality and also their comprehensive security features.

Xero Security

Xero software has never been breached and they have never lost any client data.

System Security

Xero's hosting and service delivery infrastructure ensures the highest level of security. This is supported by a world-class network, data and physical security environment.

SSL

Xero servers have SSL Certificates signed by global leaders with certificates in Entrust & GTE Cybertrust, so all data transferred between the users and the service is encrypted. The encryption is the same as that used for Internet banking.

User Access

No one has access to your organisation's data file unless invited by you and with your selected level of user permission. You can remove any invited users whenever you want.

User Passwords

Users must choose a strong password and automatic lockouts are enforced when incorrect passwords are repeatedly entered. Xero does not allow the browser to save your login and if you leave your computer unattended for an extended period, you will be automatically logged out.

Physical Security

Xero's servers are located within Rackspace tier-4, enterprise grade hosting facilities. Access is restricted to authorised Rackspace staff by a combination of biometric systems and 24/7 onsite security guards and is continually audited to meet SOC 1 Type II standards.

Firewalls and Network Security

External access to the Xero servers is controlled by multiple layers of firewalls, intrusion protection systems and routers.

Third Party Audits and Inspections

Xero's security is reviewed regularly and audited by external specialists. This includes penetrative testing and automated server port security scanning.

Data Protection and Backup

Xero service availability performance stands at over 99.99% since launching the service in 2007.

All client data is backed up daily. Xero also runs a continuous off site data back-up service into a second Rackspace facility for further real-time data protection.

MYOB Security

Keeping your business information safe and protected is vital. That is why MYOB uses industry best-practice security protocols to keep your data safe, secure and private. MYOB understand you are entrusting them with your business data and they take it seriously.

Your data is stored and protected in high security facilities which MYOB monitors 24/7. Although you can access and read your data or private information wherever and whenever you like, no-one else can without your authority.

System Security

To ensure their systems are secure, MYOB have worked closely with information security specialists such as

Appsecure to apply the recommended protocols to protect your business data.

In addition to providing industry-best practice protocols, MYOB also undertakes extensive security testing. This includes detailed analysis on their applications in line with the Open Web Application Security Project (OWASP), the Payment Card Industry data Security Standard (PCI-DSS) and industry-recognised privacy standards.

Reckon Security

Physical Security and Infrastructure:

- Reckon's servers are in a purpose built data centre (in the south of Sydney) provided by one of the largest data centre providers in the world.
- The data centre has dual power supplies to all the server racks, with dual UPS, dual independent air conditioning towers, diesel generator backup.
- Physical access to the data centre is controlled using biometric security.
- Reckon has dual high availability fibre optic internet connections that are sourced from the north and south of the data centre so they are physically in separate trenches.
- All the Accounts Hosted hardware is based on a high availability (HA) design (auto fail over).
- Reckon has a second disaster recovery data centre in North Sydney.

Data Security:

- The data is stored in Sydney subject to Australian law i.e. it is not stored in the US where the US Patriot Act means that the US government has complete access to all data stored in all locations globally by any US corporation.
- The data is stored in data base servers that have highly controlled access.
- Reckon cannot decrypt your login passwords (either to the entire service or your Accounts Hosted data files) which is why they have to ask you for your password if they think that they need to access your data to help in a problem resolution.
- The security system they use is based on Microsoft Server 2008 R2 with Active Directory control with the highest level of security enabled.
- The client's data is backed up every night.
- A second backup is taken to tape, the tapes are stored in a secure vault in Sydney but a long distance from the data centre.

CLOUDFORCE OFF-SHORE PROCESSING CENTRE SECURITY

Team Members

- CloudForce only recruits professionally qualified candidates for our Managers and Accounts Associates as they have a professional responsibility to comply with their Institute's code of ethics.
- We have a strict privacy and confidentiality clause in our employment contracts.
- We perform regular security checks and background checks on all of our team.
- We conduct awareness programs and audits to ensure every employee is fully trained on confidentiality.
- We have a strict password policy to ensure that team members regularly change and do not share passwords.

Offshore Offices

- 24 hour CCTV cameras, security system and security guards.
- All documents and data are kept on the Nimbus or the Cloud Accounting Software Provider servers in Australia. No data is held offshore.
- CloudForce Accounts Associates do not have a local printer. All printing is via the Supervisor's office and we maintain a printout register. All printouts are shredded at the end of each day.
- We maintain a clear desk policy with every team member.
- At CloudForce we have strict IT controls with tight web, email and file access restrictions, which are constantly reviewed and subject to regular audits. Accounts Associates only have internal email access and can only access the approved websites required to perform their job.
- CloudForce only uses Thin Client Technology, so no data can be stored locally.
- All data ports on the Thin Client Terminals are disabled.
- We have a no USB, mobile phone and camera policy and all such devices must be handed in to security before entering the premises.

CLOUDFORCE PRIVACY PROTECTION

Responsibility

We understand that managing client information is a responsibility that includes important privacy obligations. This is particularly true for Cloud-based services such as CloudForce. We have a broad network of people and processes that implement our privacy standards and provide privacy guidance and training.

If a privacy incident occurs, we have rigorous procedures to address the problem, diagnose the cause and update clients in a timely manner.

Using Client Data Only for the Clients' Purposes

At CloudForce, we use our clients data only for what they pay us for—to provide Cloud based Accounting and Back Office Services. As part of providing a quality service, we will troubleshoot in order to prevent, identify or repair issues and to improve features that protect our clients. But CloudForce does not build advertising products out of our clients' data. We also don't scan our clients' email or documents for the purpose of building analytics, data mining, advertising or improving the service without our clients' permission.

Together, our privacy principles, data processing agreements and our corporate privacy policy govern the collection and use of all client and partner information at CloudForce Business Support and give our employees a clear framework to help ensure privacy compliance companywide.

We regularly review the privacy policies and codes of conduct that govern our online applications, and we update them periodically if changes are needed to address clients' evolving needs and expectations.

Techniques to Protect Privacy in the Service

There is a set of common techniques that CloudForce uses to protect data privacy as we operate the service. Data access controls fall into two categories: physical and logical. The physical side is described in the Security section of this document in relation to our major service providers, Nimbus, Xero, Reckon and MYOB as well as our physical security measures in our Offshore Facilities.

The logical side relates to the access of client data. Access to client data will be via either the Cloud Accounting Software providers' servers or via CloudForce's Direct Access Networks (including Nimbus). Access to client data is restricted based on business need. Access is restricted by controls such as role-based access control, two-factor authentication and logging and auditing of activities performed in the service environment.

CloudForce applies strict controls over who will be granted access to key client data. CloudForce and support personnel are required to have a legitimate business justification to request access to CloudForce clients' core data and the request must be approved by the person's manager prior to gaining access.

In addition, access levels are reviewed on a periodic basis to ensure that only CloudForce employees or support personnel who have an appropriate business justification have access to the systems.

Further, all CloudForce support personnel are accountable for their handling of client data. Accountability is enforced through a set of system controls, including the use of unique user names, data access controls and auditing. Unlike generic user names such as "Guest" or "Administrator," unique names connect the use of client data to specific individuals.

CloudForce will only provide Data to lawful requests for specific sets of Data

Regarding requests for client data from law enforcement or other governmental entities, CloudForce is firm in its commitment to protect your data. We will only provide data to lawful requests for specific sets of data. We will not disclose client data to a third party (including law enforcement, other government entity or civil litigant) except as clients direct or required by law.

Should a third party contact us with a demand for client data, we will attempt to redirect the third party to request it directly from our client. If compelled to disclose client data to a third party, we will promptly notify our client and provide a copy of the demand, unless legally prohibited from doing so.

Privacy Policy

CloudForce Business Support Pty Ltd is a wholly controlled division of Powers Financial Group Holdings Pty Ltd. The Group Privacy Policy outlines how CloudForce manages personal information. It applies to any personal information CloudForce collects, uses, discloses or otherwise handles. For further information on the Privacy Policy, please contact us for details.

CLOUDFORCE

BUSINESS SUPPORT

www.cfbs.com.au

mail@cfbs.com.au

Tel: 07 3906 2881

CloudForce Business Support Pty Ltd

ABN 92 600 068 844

A DIVISION OF

POWERS FINANCIAL GROUP est. 1968

ACCOUNTANTS & ADVISORS

BRISBANE
10 / 8 Metroplex Ave
Murarrie QLD 4172
PO Box 518
Cannon Hill QLD 4170
P 07 3906 2888
F 07 3906 2889

BILOELA
54 Callide Street
Biloela QLD 4715
PO Box 98
Biloela QLD 4715
P 07 4995 6677
F 07 4992 1787

MONTO
3 Newton Street
Monto QLD 4630
PO Box 69
Monto QLD 4630
P 07 4166 1366
F 07 4166 1343

ROCKHAMPTON
75 High Street
North Rockhampton QLD 4701
PO Box 5161
Red Hill Rockhampton Qld 4701
P 07 4928 1555
F 07 4926 1184

mail@powers.net.au

www.powers.net.au

www.lets-talk.net.au