ChildCarers Security Statement

We pride ourselves on the security provided..

Our hosting environment was selected particularly because of it's scalability and robust security. Companies like Department of Education Employment and Training in NSW, Curtin University in WA, NASA, Verisign along with 1000's of others also share our view. ChildCarers's security vision is formed around a multi-layered security strategy that provides controls at every level of data storage, access, and transfer.
We break down the security into compartments to build a total secure platform. These components are

* Organisational security
* Personnel security
* Physical and environmental security
* Operational security
* Access control
* Systems development and maintenance
* Disaster recovery and business continuity

Secure Login

All logins are secured via Secure Socket Layers (SSL) technology.

SSL (Secure Sockets Layer) is the security technology for establishing an encrypted link between a web server and a users browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

For more information go to http://info.ssl.com/article.aspx?id=10241

Login User name and Password

Each user has a unique username/password access control for protection.

Fine Grained Permissions
This allows you to specify permissions at a user level so you can control what staff can view. The can be changed on a user by user basis so some staff can view some parts only whilst other can view all but not modify or view all and modify all. Examples of this maybe child care educators can view content but not change whilst Room Leaders or Regional Managers can view all and Centre Directors, Principals, Licensee's or Portfolio Managers have complete control.

Password Policy
We have adopted a password policy that allows you to specify the complexity of passwords and how when passwords should expire. Examples of this maybe when a family, employee leaves you simply disable their login.

One-way Encryption For All Passwords

There is only one entity that knows their password and that is the user it is intended for. All passwords are encrypted in the system and cannot be decrypted. Nobody can look up any password.

IP Based Security

This tightens our security even further. You can grant quick and easy access to those who need it, and keep your business information safe from those who shouldn't grant access. This functionality works by assigning one or more IP addresses or IP address ranges to an allowed list. For example you can allow access to the system only from the centre or regional office or you can grant access to some users from external locations.

Firewalls

Our state of the art firewalls further protect access to data to authorised hosts only. They are constantly being upgraded to shut down new threats.

Reliability

Our solution and data is hosted in top-tier, world-class data center. The system is fault tolerant, redundant servers for high availability Data is backed up routinely for peace of mind For compute, we have external connectivity at least 99.95% of the time. Additionally, we will monitor all of your individual role instances and 99.9% of the time we will detect when a role instance's process is not running and initiate corrective action.

For storage, at least 99.9% of the time we will successfully process correctly formatted requests that we receive to add, update, read and delete data.