Webrecs IT infrastructure

The Webrecs IT backend explained and how we store, backup, protect and deliver your documents to you

Sunday, April 21, 2013

Contents

Introduction

Webrecs provides a fully hosted document management system for use by third parties.This hosting is commonly referred to as being “in the cloud” or “Saas - Software as a service**”.**

This document covers how we manage and store your data and documents, and importantly, how we back it up (and of course where necessary restore) , secure, protect and deliver the data to your desktop or mobile device.

Data storage

Data Centres

Webrecs is committed to storing your data locally, in Australia. We currently use Web24 as a hosting provider, who make use of the Fujitsu Nobel Park data centre in Melbourne. This highly secure, well regarded data centre has the following capabilities :

- Datacentre is ASIO T4 and ISO 27001 compliant
- 24 hour monitoring
- Separate secure server cages
- CCTV
- Security-screening for service technicians
- Backup generators for 72 hours operation in the event of power failure
- Multiple redundancy with data-communications and providers including Vocus Connect, Pipe Networks, Verizon and UECOMM

Servers

Webrecs has its own servers which are separated into virtual machines which can be thought of as flexible “mini” servers. Virtualisation allows us to very easily scale according to your requirements - increasing the power to your system is as easy as allocation more memory, CPU or disk space to your system. And virtualisation has huge benefits in terms of Relocatable User Backups (see RELOCATABLE USER BACKUPS*) .

The servers are fully monitored for faults and/or device degradation and have a hardware-fault turnaround time of less than a day

Control of data and data access

All data is controlled by Webrecs. While access to the raw data bytes is possible by qualified , security-screened service technicians, the fact that the application which is able to make sense of this data is password-controlled by you alone means that the risk of someone being able to assemble and read your data is negligible. And this is the same as ANY cloud service provider unless all your data is fully encrypted (which we can do, but it makes sharing of documents awfully hard and slow with the passing of keys and passwords around)

Webrecs support staff can and do need access to your application to resolve issues or help you, often with administrator privilege. They will always get you to set up access for them and they recommend that you remove it as soon as they are done.

In effect, no user can access your documents unless you allow them to. And the built in audit-trail capabilites means that you can see exactly who has accessed which document and when.

Transfer of data and encryption

All data to and from the Webrecs servers is encrypted with 256 bit SSL encryption which is the same as most online banking sites.

Data ownership

All data is owned by you. Webrecs does not use any data stored on your system for any purpose other than provide the service to which you have subscribed eg. store, transform, deliver and find documents. Webrecs will not make this data available to anyone other than you except to comply with a legal warrant issued by a court under whose jurisdiction Webrecs is bound (and even then Webrecs cannot guarantee that we can provide the data in a usable format without your password – and we do not know your password).

Data Backups

It is in the area of backups where Webrecs outshines all other cloud service providers. We provide 3 levels of backup, each with a different purpose :

Daily backups

These are performed automatically overnight and are covered by the subscription cost. At least 15 days of backed-up data is available. So if something bad happens and you contact us within 15 days we can get it back for you. Backups are stored offsite in a physically distant (>10km) location so that in the event of a data-centre catastrophe (flooding, fire) the backups are safe. Backups can be restored in their entirety or individual files can be selectively restored. Data restoration carries a cost of $120 per restore.

User-initiated server backups*

These can be done at any time from the user's control panel, depending on the subscription type. They are typically used by users for backing up your Webrecs subscripion prior to a significant configuration change so that the restore process can be quick and easy should you wish to back-out the change.

Relocatable user backups*

These backups are ordered through the subscription control panel and are your insurance policy. They contain all your data, plus the software needed to make sense of the data - in fact the entire contents of the virtual machine, for you to keep on your premises. They come with the Webrecs "magic CD" which allows you to run your entire system on any PC completely independently of Webrecs, the internet or any political, infrastructure or legal disruption. So in the event of something really bad happening like the web going down or Webrecs going out of business, you still have all your documents with their complete contexts (including audit trials, workflows, properties and versions) . These are typically delivered on USB drives through the mail, and carry a cost of $100 plus $1 per gigabyte of data. Most customers take one every 3 months or so - the decision is how much data can you afford to lose in the event of the worst possible scenario (note that this is not necessarily fire, flooding or destruction of the data centre - we have disaster recovery to take care of this - see DISASTER RECOVERY)

*Note : These are only available to Webrecs VP Cloud subscriptions.

Disaster recovery

Because we use virtualisation using industry standard technologies it is very easy and quick to move a subscription or virtual machine between physical servers or even hosting providers. And given that we have a backup of every virtual machine every day which is stored offsite, in the event of complete destruction of the data centre, it is a relatively simple case to retrieve the backups and move the virtual machines onto another server, host or even provider.

In theory this process could occur the same day, in practice it is sensible to assume at least 2 or 3 days downtime because of the potential disruptive nature of the disaster eg. travel and access to the remote site could be problematic, data cables could be down etc.

We can also provide the capability to have mirrored “dual live” sites in different locations, effectively allowing minimal downtime in the event of disaster at one site.

Redundancy

Our hosting provider provides a large measure of hardware redundancy which means that day-to-day hardware faults (drive failures, power-supply failures, input feed failures etc.) are picked up and rectified without any downtime. Webrecs always maintains spare capacity on servers to ensure that virtual machines can be moved to an unaffected server should an unrectified fault occur on any particular server.

System availability

100% availability is impossible in the hosting business. Most hosting providers (including ours) use a sliding scale from 90 to 99.99% which is from 72 hours to 4 minutes per year and provide refunds calculated on this basis. Our guarantee is somewhat different for 2 reasons :

1. We are Australia local, servicing local businesses. Because the customer timezone and hence working hours are known we can and do shutdown the application during non-working hours for the time it takes to do a backup (typically sub-minute depending on the data size) – the time is chosen to minimise disruption – typically 1-3am. We do this because it is the safest way to 100% guarantee data consistency between diverse applications (databases and filesystem documents) without extremely costly and complex synchronisation technologies. We can of course implement this if required in custom cases, but it comes at a cost which is really not necessary for 99% of our customers.
2. We work closely with our customers to customise, upgrade and support their (often custom) solutions, which occasionally requires a restart of their application(s). While we do notify affected customers, we do require the ability to react quickly and occasionally restart even during office hours. This typically requires a couple of minutes to perform.

So our guarantee goes as follows :

We guarantee that during standard business hours, if there is downtime for more than one hour per month attributable to Webrecs you get that month free. If that is unpalatable, we can implement mitigation measures at your request at a cost, and provide up to 99.99% availability

Privacy and access control

Webrecs does not use your details for any purposes other than to

- Provide the services to you
- Facilitate the billing process including the local storage of credit card data which is kept in a secure database. This can be avoided if you prefer by setting up direct debit or Paypal.

We do not provide contact or subscription information to anyone else, and only senior managers and members of the finance team are able to access billing information. We will not spam you with special offers, promotions and advertising, but will inform you regularly (usually bi-yearly) of information which you should be aware of relating to your system.

All access to your system is password controlled. Access to individual documents is governed by you, and can be extremely fine-grained, for example some groups may be able to see certain documents in a folder but not modify them, where others be granted special permission to see a particular document in a particular folder without having access to the other documents – but this is up to you. The standard subscriptions implement a fairly tight document security hierarchy which can be modified as required.

System Security

Physical security

Access to the physical hosting premises is strictly controlled and within the premises the Webrecs data is stored in locked cages accessible only to security-cleared Web24 personnel

Application security

At the core of the Webrecs application is the Alfresco Document Management Engine which is the most popular open-source document management system around. The number and scale of the deployments of this application means that security holes are very quickly fixed - and while it is impossible to say that ANY software is 100% secure from hacking , it is widely recognised that open-source software tends to be more secure than proprietory software because of the number of independant “eyes” on the source code. Webrecs builds onto the Alfresco engine using industry standard security techniques including OpenVPN for mounted drives, 256 bit SSL encryption and strict access authentication for all custom web-scripts.

Webrecs Cloud subscriptions are multi-tenant which means that the subscriptions are logically partitioned from one another but still running in the same virtual machine. It is not possible to access a subscription other than through a password-controlled login for that subscription.

Webrecs VP Cloud subscriptions add another level of security by running each subscription in its own virtual machine, which effectively physically isolates subscriptions from one another (no shared

application , database or storage locations) . One of the features of a Webrecs VP Cloud subscription is the ability to run other applications in the same container (eg. CRM, Web content management , Jira). Webrecs applies the same security rigour to these implementations, and for custom solutions (for example a custom database application) we will assist in making the solution secure.

Webrecs can also run subscriptions on a completely separate server if required - although this is typically only for large customers and is more expensive.

Anti-hacking measures

Hacking is a major concern to any online site and we adopt recommended measures to minimise our risk.

- Monitoring to reduce DDoS attacks.
- No unsecured ftp
- Regular changing of system passwords
- Usage of non-standard words in passwords
- Strong passwords on all databases
- Regular application of security patches
- Regular penetration testing