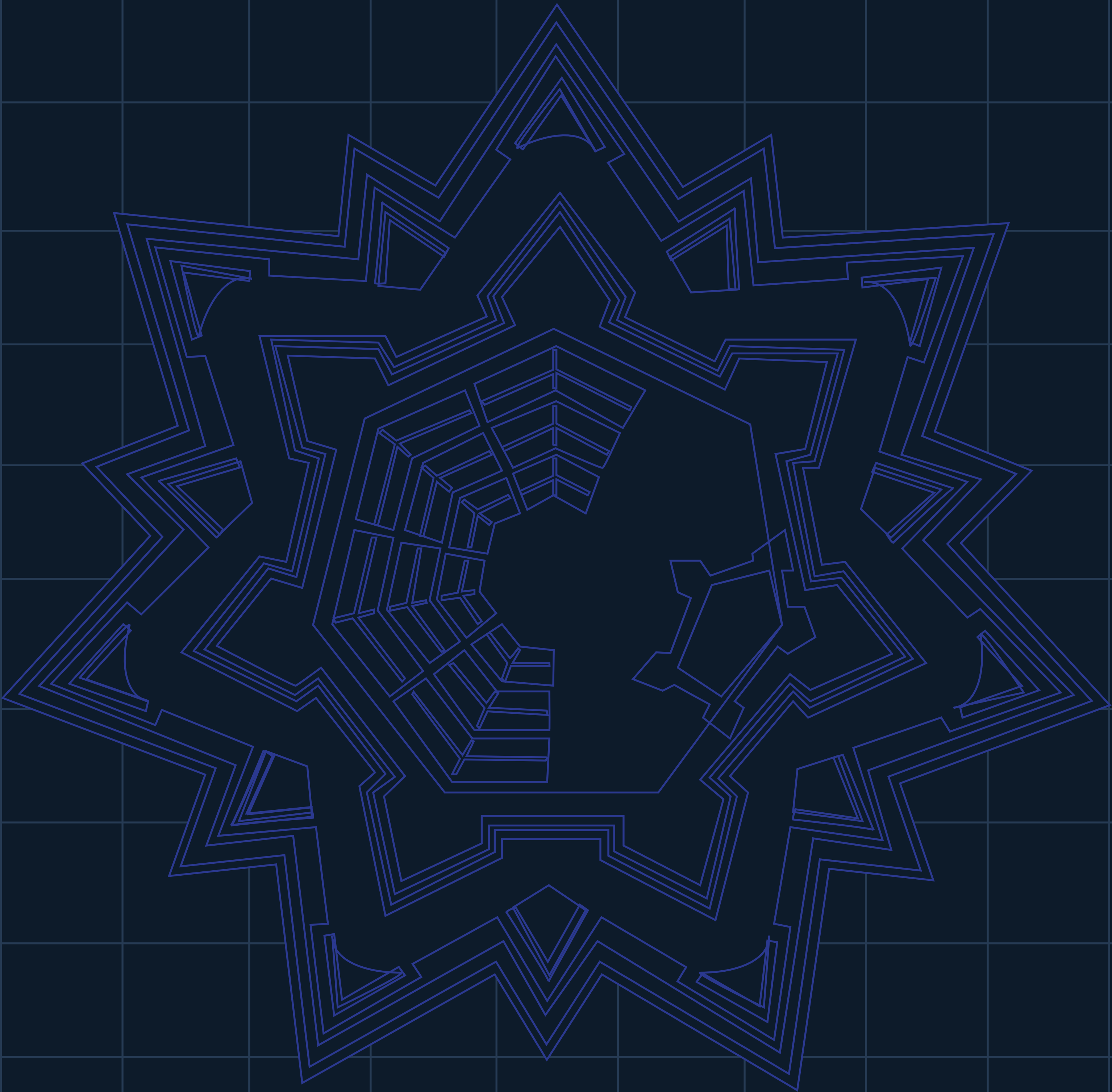
Security of OpenCRM Systems



opencrm

OpenCRM Security:
Covering all avenues

Our reputation depends on providing watertight security. We would like to assure you that your data is rigorously guarded. From the very beginning we decided that security was going to be the 'magic bullet' to win the confidence of our prospective clients, which is why we take this so seriously.

At OpenCRM, security is more than just a technical consideration, it is embedded into our day to day operations, from the development team right across the company.

Security is very important to us, it is not just what we do today, but the continual reviews on what we need to do for the future.

Below are some of the security precautions we take and some of the features in OpenCRM that will allow you to control the access to your system. There are many more that we don't publish because, as you might expect, that wouldn't be a good security policy!

Watching Out for Your Data

Where is my data?

We use the Amazon Web Services (AWS) London region to host all our OpenCRM systems. This means your data, both back-ups and your primary system, is always located within the UK.

Your data is stored within an Amazon RDS database, a type of fantastically fast, super secure, and ridiculously reliable database, meaning that it scales across multiple AWS datacentres, is encrypted at rest, and inaccessible outside these networks.

Any files you upload are encrypted at rest and stored within Amazon S3, AWS' dedicated storage system. It provides a secure and durable way to store files making sure they are accessible when you need them.

Actually, while held in AWS, your whole OpenCRM journey is encrypted. Any time you login, or upload a file, your data will be transmitted securely and be encrypted at rest.

Accessing your data

Our new web servers run on Amazon EC2, which maintains a base uptime of 99.99% (although our projected uptime is actually higher).

Your files are held in Amazon S3, which has "eleven nines [99.999999999%] durability"--basically meaning that by storing and constantly maintaining multiple, encrypted copies of your uploads, you can rest easy knowing that your files are in safe hands.

So both your database and your files will be available when you need them

But is AWS Secure?

Amazon Web Services are used by some of the biggest names in the most demanding industries, from Netflix, the Financial Industry Regulatory Authority, and NASA.

AWS divide the security of their data centres into four layers: Perimeter, Infrastructure, Data, and Environment.

There are a number of controls in place to ensure these centres are secure both in terms of the buildings themselves and the way they are accessed.

Perimeter Layer

Ensuring the security of the perimeter layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

Access is only given to authorised people, entry is highly controlled and monitored (including the data centre workers), and the whole operation is overseen on a truly global level.

Infrastructure Layer

This layer is the data centre building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer. These devices and systems help protect servers and ultimately your data.

As with the perimeter layer, access to infrastructure is highly monitored. The only people who are there are there to run diagnostics and generally maintain the equipment to make sure it is available when you need it.

And this includes all the emergency backup equipment.

Data Layer

The Data Layer is the most critical point of protection because it is the only area that holds customer data. Protection begins by restricting both physical and technological access and maintaining a separation of privilege for each layer. The installation and servicing of data storage devices, as well as their eventual destruction, is all held to an incredibly high standard.

In addition, AWS deploy threat detection devices, video surveillance and system protocols, further safeguarding this layer.

And finally, the whole process is thoroughly audited, by external parties, throughout the year.

Environmental Layer

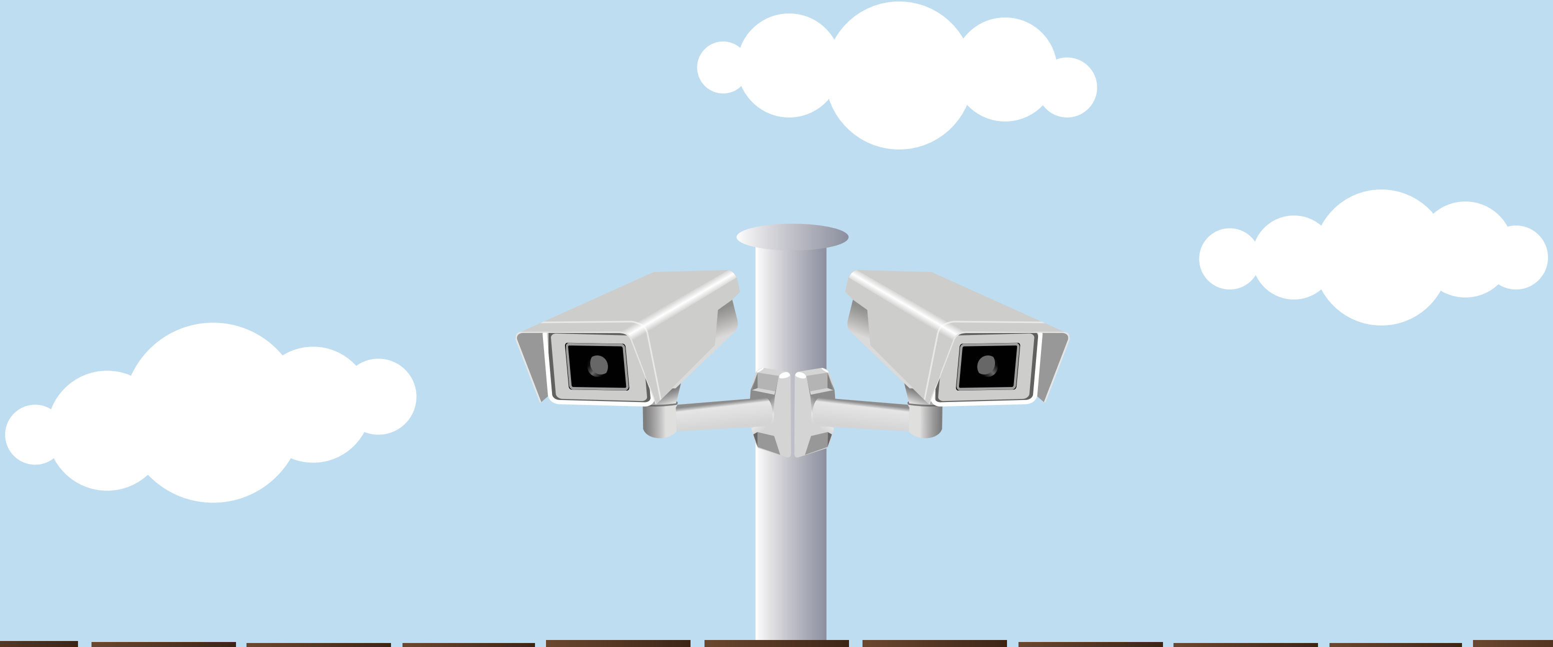
This layer refers to the way the actual data centre sites are selected, constructed, and maintained. All are dedicated mitigating risk and disruption from environmental factors, such as extreme weather or natural disasters.

AWS has sensors to detect and equipment to respond to flooding, fires, power outages, and other threats. Practice drills are regularly conducted to ensure all staff members are ready in case of an environmental emergency.

Each AWS region is a sperate geographic area and has multiple Availability Zones which are isolated locations with data centres within them, providing you with the most reliable access to your OpenCRM system.

Controls

All of the controls surrounding the various layers of the AWS infrastructure are subjected to regular review and monitoring. Plans and contingency measures are in place to make sure all OpenCRM users will be able to keep doing business no matter what happens at their end.



Keeping Security in Our Sights

OpenCRM Security Policies

In addition to the security measures put in place regarding our data centres and the access to your system, we have a number of policies and measures in place to protect your system and the data within it. These policies and measures have been modelled on those taken by banks.

- We keep a full ticket history of work carried out on your OpenCRM system including comprehensive versioning of core application code and any bespoke development work.

- There are telephone communication protocols implemented with each customer to ensure only authorised contacts can request amendments to your system, including user access changes and configuration/development enhancements.

- We run a clean desk policy for all employees.

- We have a robust policy on printed data and its authorised destruction.

- We run a strict data retention policy when working on 'client data' for uploads.

A CRM with Muscle

System Security

We also have a number of additional, technical security measures in place to protect all OpenCRM systems.

We use 256 bit AES SSL encryption, the same used for internet banking and many large financial services transactions.

We utilise Automated Distributed Denial of Service (DDoS) protection and all of our customer networks are segregated using a private VLAN.

We set rules to stop brute force username and password attacks, including policies for number of failed attempts.

If you are logged in and don't use OpenCRM for a while, you will be logged out automatically – this time period can be set by your admins to fit the way that you work.

There is an audit trail of the important functions that your users carry out, so you can see what your users have been doing.

We run a strict 'authorised administrator' policy which means that any account unlocking or changes to any aspect of your system security MUST be authorised by a known OpenCRM system administrator.

For further peace of mind, we monitor saturation on network links, with alerts being generated if critical links are acting unusually. This allows us to very quickly see any potential issues that may arise.

We utilise additional third party enterprise software monitoring tools that allow us to track a wide number of components.

We use Host Based Intrusion Detection software to carry out Log Monitoring, Policy enforcement and Alerting of any critical incidents over the regular 'noise' on any number of things you can do to keep your data safe.

Taking Matters into Your Own Hands

System Administrator Security Controls

We work very hard to keep OpenCRM secure. Here are some extra steps you can take, as an administrator, to protect your system and the data within it:

- IP Whitelist – you can specify a Global Whitelist for allowed IP addresses, you can also specify a User Whitelist of allowed IP addresses for specific user credentials.
- IP Blacklist – you can specify a Global Blacklist restricting access to your OpenCRM system and bouncing any attempts from a restricted IP to a predefined page/site.
- You can set up data access rules that determine what data can be accessed and by which users.
- No one has access to your OpenCRM systems, unless you invite them. You can remove any users whenever you want, either by marking their account as inactive or removing their details completely. Any changes are carried out in real time and take immediate effect.

- Users must choose a password to access OpenCRM. Administrators can specify the Password Policy that you wish to enforce, including being able to specify:
  - Non-dictionary words
  - Minimum length of password
  - Forcing mixed alphanumeric and mixed character case
- Enable Multi-Factor Authentication for all use accounts.
- Automatically log inactive users out after set time period.

Password Recommendations

- Create a password nobody can guess, no dictionary words or family names. Be cryptic or use multi-word pass phrases - easy to remember, hard to crack.

- Remember the old favourites – replace 'I' with 1, 'E' with 3, 'A' with 4 or 'O' with a zero.

- Prefix or suffix a random character into the mix.

- Don't share your password with anybody.

- Don't write your password on a sticky note and attach it to your computer.

- Don't save a copy of your password in an insecure file location on your computer. If you are concerned that you will forget your password, we strongly recommend using an enterprise password manager.

- Don't allow the browser to save your login; this eliminates access from a stolen or compromised computer. OpenCRM by default prevents you saving your login credentials – don't use third party applications to bypass this control.

Security in the Cloud

General Security Advice for Cloud-Based Systems

What else can you do?

- Create a Company wide Security Policy that outlines:
  - What your employees should have access to
  - What they are allowed to do with data and company assets
  - What they should do in the event of any loss or breach
  - How you will enforce this policy when any issues arise, with clear guidelines on responsibility

- Keep your computer operating system up to date by installing recommended software updates and system patches.
  - For Windows users, take a look here https://microsoft.com/security
  - For Mac OSX users https://support.apple.com/kb/HT1338
  - For Linux users search https://www.google.co.uk for your Linux distribution + keywords 'Security Update Patches'

- Keep your browser software up to date.

- Select a web browser that is known to be secure and offers regular security updates.

- Make sure you only login at https://yourcompanyname.opencrm.co.uk.

- We will never email you or ask you on the telephone for your password, so NEVER divulge these to anyone.

Making You Feel Safe

How can OpenCRM be safer than desktop software?

A lot of people worry about the security of cloud-based software, thinking that it can't possibly be safer than software they host in house or just have installed on their computer.

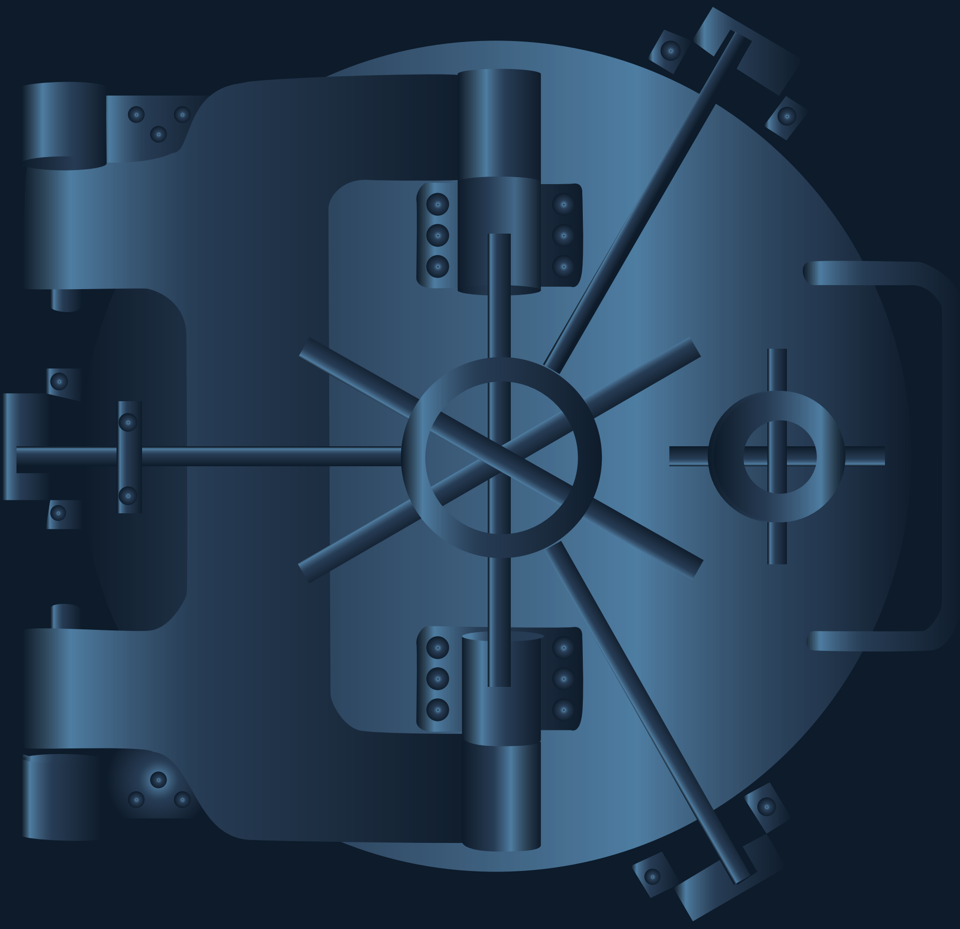
But it can...and is...here's why:

- Unlike desktop applications, your data isn't stored on your computer, so if your computer is lost or stolen no one can access your data without a login and meeting the rigorous policies applied.

- Online applications can be much more secure than emailing your data or giving out discs/USB memory sticks containing your data.

- We give you peace of mind with nightly, weekly, and monthly snapshots of your data.

With all the security procedures and measures put in place within OpenCRM and at the data centres, along with all of the options you have at your fingertips to control your own system security, you can be sure that your data is safe and secure.



Keep your data safe and
secure with the team at

opencrm

Email: sales@opencrm.co.uk
Website: https://opencrm.co.uk
Tel: +44 (01748) 473000

1 Bailey Court, Colburn Business Park, Richmond, North Yorkshire, DL9 4QL, UK