# AeroCRS System specifications (Technical Requirements Protocol)

- Web based system
  - Supported browsers:
    - Internet explorer 9+
    - Firefox 3x+
    - Chrome (latest build – this web browser is automatically updated)
    - Safari 4+
  - All operating systems which run one of the above web browsers are supported

- Code:
  - PHP
  - ASP

- Database
  - MS-SQL
  - 3 different databases
    - Data
    - Website data
    - Management
  - All databases are permission-based and sockets are opened according to needs of applications

- Accessibility features
  - The company does not provide accessible IBE / System and it is not under the AA/AAA standard.
  - Customers are responsible to embed accessibility tool-bars and are responsible of maintaining standard in their published articles and information in the IBE.

- Infrastructure:
  - EU Ireland - Amazon Web Services
    - 15 Servers
    - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers, more info: https://aws.amazon.com/ec2
    - Elastic Load balancing - Servers are connected via load balancers, Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It can handle the varying load of the application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant, read more: https://aws.amazon.com/elasticloadbalancing

  - Disaster recovery Plan
    - AeroCRS Infrastructure is rolled out in 2 different availability zones, allowing a sophisticated DRP.
    - Data is backed up to the DRP on a 5 minute basis.
    - Read more about availablity zones by AWS: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

- AWS compliance: AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Read more: https://aws.amazon.com/compliance/shared-responsibility-model/
- External SMTP servers to insure email delivery quality for your customers using MailChimp - https://mailchimp.com/

- Security
  - Using 256 bit encryption with premium SSL protects sensitive information during transition between airline and AeroCRS servers

  - Firewall and Elastic Load balancers
    - Only authorized personnel and only from specific locations can access services other than http port
    - Internal servers not connected to the internet and accessible only via VPN to specific authorised personnel.

  - Web application firewall
    - All the information passed to and from our servers is protected using a very secure layer of security called “Web Application Firewall”
    - In this type of security, all packets of information are inspected on a different firewall before reaching AeroCRS servers
    - This helps us (and the customer’s websites) protect from the following attacks:
      - DDoS (distributed denial of service) attacks
      - Bad bots
      - Remote file inclusions
      - SQL injection
      - Cross site scripting
      - Illegal resource access
      - Backdoor attacks
    - We use a service called incapsula which is a web-based WAF. This means that once someone tries to attack another website, you are also protected, as the learning curve of the service is much better than a standalone protection which needs to be updated and patched on a daily basis.
    - Incapsula’s Web Application Firewall protects against the most critical web application security risks, such as SQL injection, cross-site scripting, illegal resource access, remote file inclusion, and other OWASP Top 10 threats. Security experts behind Incapsula’s service ensure optimum protection against newly discovered vulnerabilities to prevent disruption to your application and improve website performance.

  - Trendmicro deep security
    AeroCRS is using Trend micro deep security product on all servers, which provides with:
    - Defend against network and application threats, leveraging proven host-based network security controls like intrusion detection and protection (IDS/IPS)
    - Protect against vulnerabilities, instantly shielding vulnerable applications and servers with a ‘virtual patch’ until a workload can be replaced
    - Lock down servers so that only authorized processes can run with application control for Windows and Linux
    - Keep malware like ransomware off workloads, ensuring that servers and applications are protected
    - Identify suspicious changes on servers, including registry settings, system folders, and application files that shouldn’t change
      Read more:

https://www.trendmicro.com/en_us/business/products/hybrid-cloud.html

- AeroCRS developers follow OWASP guidelines and are certified by an external company, the training is done yearly.
- AeroCRS conducts security checks yearly to the system to check vulnerabilities.
- AeroCRS updates servers on a regular basis to make sure they are updated with the latest patches.

- CDN
  - The storage is kept on 20 server locations worldwide, so if a customer in the UK is requesting information, the server which will be serving the static information (like images etc.) will be stored at a location next to him, so the system and website would work faster.

- Backup Procedure
  - Main Databases
    - 5 min interval MS-SQL mirroring between several servers in different availability zones.
    - Daily backup procedure to storage (S3 (AWS) Bucket backup)
    - 14 days retention period
  - Logs
    - Different log retention according to needs.

- Monitoring
  Besides 24/7 monitoring of AWS Cloud facilities, we use 4 additional monitoring services:
  - Datadog - AeroCRS uses datadog to actively monitor servers performance such as CPU, Memory usage, Network usage etc.
  - AeroCRS Uses “Raygun” for code and system performance monitoring, to allow us to get real time monitoring of customer’s errors, the error rate for 2017, was 0.0001% errors per transactions performed in the system.
  - Host Monitor application installed on a server – monitoring SQL services, http and Intrusion detection – System alerts in SMS and E-mail to our technicians 24/7.
  - “Statuscake” external monitoring service - monitoring all websites and services for uptime from a different location. (independent monitoring service) – Alerts managed by our NOC, E-mail, weekly report sent to AeroCRS management.
    See the status of our system at http://status.aerocrs.com