MYSOLUTIONS SECURITY PRACTICES

At Purplebox Software, our #1 priority is Information Security. Since the nature of our work involves confidential information, we have processes in place to ensure we maintain a high level of security to make certain you and your data is safe.

- Purplebox Software

1 SQL INJECTION

The MySolutions database is protected from SQLi through firewall, data sanitization, validations and database privileges.

2 XSS (CROSS-SITE SCRIPTING)

Permission levels are set for authorised users to access the database and files. Azure Firewall is also set up to prevent XSS,

3 SERVER/CLIENT-SIDE VALIDATION

Standard validation through Microsoft Azure and user's policy management is set up to prevent privilege escalation and directory traversal.

4 PASSWORD ENCRYPTION

User passwords are encrypted and never stored in plain text - furthermore the passwords are kept in a database held in Microsoft Azure, adding another layer of protection.

5 INFRASTRUCTURE SECURITY OF MICROSOFT AZURE

The MySolutions database and file security is handled by Microsoft's cloud computing platform, Azure, and is one of the top performers in cloud computing.

6 SESSION HIJACKING/COOKIE POISONING

To avoid session hijacking, MySolutions does not use cookies to handle sessions. No cookies means no cookie tampering.

7 SECURE DATA TIER

The MySolutions web application files and database reside in different locations for an added layer of physical security.

8 HTTPS CONNECTION

Data sent between your computer's internet browser and the website is secure, as all the communication between the two are encrypted via SSL.