Airline Management System – Database Security Policy

Following database security policy is suggested to keep database secure and protected:

- **Lower system and database privileges; increase database security with Role Based Access Control**
  The access privileges will be awarded absolutely on a need basis with strict role based access control coming into play. The DBA will be master control and it will branch down accordingly.

- **Separating the Database and Web Servers**
  The database server will be kept separate from the web server. A database should reside on a separate database server located behind a firewall, not in the same one as the web server. While this makes for a more complicated setup, the security benefits are well worth the effort.

- **Encrypting stored files and backups**
  The stored files will be encrypted. If stored in plain text, it provides the keys an attacker needs to access our sensitive data. The backups will also be encrypted.

- **Using a Firewall**
  A http://www.applicure.com/solutions/web-application-firewall can be installed. In addition to protecting the site against cross-site scripting vulnerabilities and web site vandalism, our firewall can thwart SQL injection attacks as well. By preventing the injection of SQL queries by an attacker, it can help keep sensitive information stored in the database away from prying eyes.

- **Keeping the Patches Current**
  With the airline web sites being rich with third-party applications, widgets, and components and various other plugins and add-ons, one can easily find themselves a target to an exploit that should have been patched. By keeping the patches updated, this can be prevented.

- **Minimizing the Use of 3rd Party Apps**
  The plan will be to keep third-party applications to the bare minimum. We want our web site to be filled with interactive widgets and sidebars filled with interesting content, but any app that pulls from the database is a potential threat. Many of these applications are created by hobbyists or programmers who discontinue support for them. Unless they are absolutely necessary, plan is to not install them.

- **Not Using a Shared Server**
  Our database holds sensitive information and it is most important for us to not share a server. While it may be easier and cheaper to host our site with a hosting provider, we are essentially placing the security of our information in the hands of someone else.

- **Secure Your Data with an Effective Disaster Recovery Plan and Test It Regularly**
  The database will be backed up per the security policy and a recovery plan will be in place to fall back to. This setup will be tested regularly to be better equipped to handle such contingencies.