:

springfields offspring

Hosting, Security, and Licensing for Offspring – Android Grievance Application

Overview

The Android Grievance Application can be purchased through a mixed-delivery model using a ‘hosted’ third-party solution for the architecture and a **one-time perpetual license and installation fee** from Springfield’s to provide a complete ready-to-use solution for the customer. This enables the customer to take full responsibility for data security and access while maintaining the ongoing hosting fees directly with the hosting provider.

Hosting Architecture

Springfield’s recommends the deployment of the Android Grievance Application using Amazon Web Services (AWS). AWS has set high standards for the entire Infrastructure as a Service (IaaS) industry by building a solid foundation with comprehensive administrative, physical and logical controls — from strict policies for physical access to its data centers, to well thought-out configuration change management procedures.

Springfield’s is using AWS below deployment framework for Auto scaling of the server to manage any number of hits to the server.

• Amazon EC2 (Elastic Compute Cloud): It allows the scalable deployment of the application.
• Amazon S3 (Simple Storage Service): It is an online file storage web service which provides memory storage of more than 50 terabytes.
• Amazon RDS (Relational Database Service) simplifies the scaling of the relational database of the app.
Sample License Key Terms

However, a secure foundation is just the start and to build an end-to-end secure computing environment, users of our Application should take an active role in protecting systems, applications and data as part of the AWS shared security model.

Security

Customers pay only for the hosting services they use with AWS, meaning that you can have the security you need, but without the upfront expenses, and at a lower cost than in an on-premises environment.
In addition, **AWS offers 12-months free use for all new customers**.

Following the first 30 days after installation, once the customer is familiar and ready for live deployment, Springfield’s will transfer all access codes and login authorization for the customer to maintain. Springfield’s relinquishes all access to the server and future Customer data associated with the Application.

For further information, please read below for comprehensive security and data practices using AWS.

https://aws.amazon.com/compliance/data-privacy-faq/
https://aws.amazon.com/security/

Licensing

Springfield’s grants to the Customer a perpetual, non-exclusive, non-transferable and non-sublicensable license to use.

Key terms of the agreement

- **Installation of Upgrade and Update**

Springfield’s will be responsible for the installation of the Application on the AWS. This includes ensuring all the proper deployment, configuration and testing the functionality with the customer. Springfield’s will provide initial training and guidance on how to use the system with support during the first 30 days.

- **Maintenance and Support**

The customer can choose whether to purchase maintenance and support services from Springfield’s with respect to all software licensed. Maintenance services do not include the provision of any newly developed modules, released by Springfield’s after the effective date that include significantly different features and functionality, and which are packaged and marketed as separate software.

- **Coding**

No “back door,” “lockout,” “time bomb,” “drop dead device,” restraint, monitoring, logging or disabling code or similar devices that may be activated or used by Springfield’s are incorporated or present within the Licensed Software. Further, Springfield’s shall use commercially reasonable efforts to ensure that the Licensed Software, when delivered to the Customer is free of computer viruses, worms and other malicious code that may potentially interfere with Customer’s use of the Licensed Software or damage or compromise any computer systems or networks on which it is operated.

During the development phase of the Application, the following practices were conducted:

- Testing against SQL injection attacks
- Testing for XSS (Cross Site Scripting) and JavaScript Injection attacks
- Log Verification to check that sensitive data is not present in the log files

- **Confidential Information**

During the term of this License Agreement and thereafter, each party will use and reproduce the other party’s Confidential Information only for the purposes of this Agreement and will restrict disclosure of the other party’s Confidential Information to its employees, accountants, consultants, and advisors.

Technology Stack of the Application

Database Type: MySQL | MS SQL
Suggested Hosting infrastructure: Amazon AWS
Programming Languages:
Android App Development (JAVA)
Admin and Web Services Development (PHP | .Net)