

MIT Libraries Policy on the Use of FileMaker for Applications

December, 2006

This document outlines the MIT Libraries' policy on the use of FileMaker for building local computer applications. It is intended for developers who are considering FileMaker as a platform for a new application, or a significant upgrade to an existing application.

Computer applications like FileMaker, Microsoft Access, Microsoft Excel, etc. are useful for building database systems easily, but there are particular issues with their security, interoperability, and reliability that should be considered carefully before decided to use them. This document provides guidelines for when it is appropriate to use FileMaker for a computer application and when another technology platform is called for¹. The main issues for FileMaker (equally applicable to Access or Excel) are listed below.

1. Security

FileMaker applications typically run on the Mac OS/X or Windows platform, which are harder to secure against network intruders. Extra precautions must be taken when developing applications in FileMaker (or Access) to insure that they are reasonably secure, and that there is no "sensitive data" stored in the application that could be compromised by an intruder. See the links below for the current ITAG definition of sensitive data <http://istwiki.mit.edu/istwiki/ItagSensitiveData> and policy on handling sensitive data in local applications: <http://web.mit.edu/itag/policies/sensitive-data.pdf>

Additional risks are introduced if shared files are accessed from file servers instead of using the built-in network sharing in FileMaker Pro and FileMaker Server. Users can make inappropriate copies of the files and can introduce record locking and potential corruption issues when files are shared with inappropriate methods.

The native Web user interface to FileMaker has many well-known security problems. If Web access to the database application is required, the system should be run on Mac OS/X and Apache web server should be used to access the application via PHP, using FM's XML export capability. For more information about securing FM Web applications see <http://www.filemaker.com/downloads/pdf/websecurity122002.pdf>

¹ The Libraries' standard alternative to FileMaker or Access for database applications is the LAMP platform: Linux, Apache, MySQL, and PHP (or Perl). We also support PostgreSQL, and Oracle database applications.

There is more information on using FileMaker for secured application on the IS&T website <http://itinfo.mit.edu/article.php?id=6033>

2. Integration

FileMaker provides *limited* ODBC and JDBC integration to the application. Specifically, it is not fully SQL compliant, which can make it difficult to create automated access to FileMaker data from other systems. For more information see

http://www.filemaker.com/downloads/documentation/fm8_odbc_jdbc_developer.pdf

3. Reliability

In the event of a server failure such as an unexpected loss of power, hard drive failure, or software failure, it will be necessary to restore the entire FileMaker application from backup files. Any system failure causing FileMaker Server to shut down inappropriately can result in corrupted files if cached data was not written to disk and the files were not closed properly (i.e. is not fully ACID compliant ²). Even if the files re-open and go through a consistency check or recovery, corruption might be buried in the file. File recovery cannot guarantee that problems have been fixed. For more about this information see

http://filemaker.com/downloads/pdf/fms_best_practices.pdf

FileMaker Use Policy Statement

The Libraries policy is that FileMaker may be used for applications that meet the following criteria:

- The application is a prototype that can be re-implemented later if necessary, OR the application will be used within a single department, unit, or functional area of the Libraries and will not evolve into a complex, Libraries-wide system.
- There is no sensitive data being stored that will be distributed by the application via the Web or email etc. (for a definition of sensitive data, see <http://istwiki.mit.edu/istwiki/ItagSensitiveData>).
- The current recommended FileMaker version and server/client configuration are used.

<http://itinfo.mit.edu/product.php?name=filemaker>

² See <http://databases.about.com/od/specificproducts/a/acid.htm> for details on ACID compliance

- The application does not require integration with other applications (e.g. SFX/Metalib, Barton, or the MIT Data Warehouse) using standard network protocols³.
- The application will not be a System of Record for any Libraries enterprise data.

If these conditions are met then using FileMaker for the application may be appropriate. Otherwise a review should take place the Associate Director of Technology and the Head of the Systems and Technology Services department to ensure that due diligence has been performed before proceeding with the FileMaker development.

Best Practices for Use of FileMaker

Recommended security measures for FileMaker include:

- Use FileMaker Server and not a peer-to-peer configuration
- Use strong passwords
- Hide filenames from network scanning on port 5003
- Turn on SSL
- Implement a robust backup and recovery procedure
- Physically secure your server and backup media
- Store backup media in alternative locations
- If feasible, use a Server OS firewall
- Use the Apache web server and PHP, not the Web Companion plug-in, to provide Web access to the database

Additionally, if the application will be used by more than one person (i.e. is not a personal desktop application) then consider using STS's hosted FileMaker server so that the application is regularly backed up and secured.

See additional guidelines on using FileMaker at <http://web.mit.edu/ist/help/filemaker/fmug/Top10.pdf>

See also more detailed information at <http://web.mit.edu/ist/db/fm/>

³ Data can be exported from a FileMaker application for batch import into other systems when analysis and programming resources are available to do the necessary data format mapping and conversion programming to the target data format.