

Policy Name	Policy for Sensitive Data as applied to Departmental/Local Databases
Policy Driven by	ITAG
Policy Effective Date	Dec 1, 2007
Policy Owner (responsible for changes or updates)	Wilson D'Souza
Version	1.0

Background (rationale for this policy)

FileMaker, Microsoft Access, MS Excel etc are useful for building small-scale departmental systems easily, but there are concerns about their security, integration, reliability and scalability. We want to reduce the points of exposure and thereby limit the risk of sensitive data leakage.

We strongly recommend that departments that have a need to store sensitive data consult with IS&T's DCAD group and explore all options including the utilization of IS&T's hosted FileMaker service. This will allow greater security and access control.

We have outlined some typical areas of concern below: (reference below is for FileMaker but equally applicable to other applications like MS Access, Excel, any local equivalent)

Security – As with any software manufacturer, FileMaker Inc makes no guarantees about the security of their product. The following outlines the risks, which apply not only to FileMaker but to any local database development environment.*

Inexperienced database designer

- High risk of unintentional threats caused by employees having inappropriate file and database feature access.
- Employees may introduce unintentional threats by sharing files without taking proper security measures.
- Data is exposed if FileMaker Pro accounts and privileges are not configured correctly to protect files adequately.

Inexperienced system administrator

- High risk of unintentional threats caused by inadequate operating system security, poor backup techniques.
- Poor network security increases the risk of intentional threats, particularly if files are shared over the web or on a wireless network.
- Risks are also introduced if shared files are accessed from file servers instead of using the built-in network sharing in FileMaker Pro and FileMaker Server. Employees can make inappropriate copies of the files and can introduce record locking and potential corruption issues when files are shared with inappropriate methods.

Databases store sensitive or valuable data

Increased risk of intentional threats of data theft, particularly if data is shared over the web or if access to data isn't adequately monitored and protected.

*Source-http://www.filemaker.com/downloads/documentation/fm8_security.pdf

Policy Statement

ITAG recognizes the need for developing applications with an easy-to-learn-and-use tool such as FileMaker. To gain the benefits of common knowledge and experience, we recommend that FileMaker be used for applications that meet the following criteria:

- It's a local application used within a single department (DLC).
- There will be fewer than 50 users of the system at any time.
- It's not used to develop applications that are expected to evolve into a complex database. Measures of complexity to consider are:
 - There are more than 20 well modeled tables or files
 - The application costs more than \$30k to develop.
 - Tables have a field count exceeding 100.
- There is no sensitive data being stored that will be distributed by the application via the Web or other means.
- Storing sensitive information: Please refer to the draft definitions on Sensitive Data @ <https://wikis.mit.edu/confluence/display/ITAG/ItagSensitiveData>
 - Some examples of data that should never be stored in FileMaker are: personal information, medical, SSN, and credit card information.
- The current recommended FileMaker version and server/client configuration are used. <http://itinfo.mit.edu/product.php?name=filemaker>
- The application will have little need to integrate with other applications, except accessing information from the Warehouse.
- The data collected will not need to be accessed by other non-FileMaker systems, such as the Data Warehouse.
- It isn't a System of Record for MIT Enterprise Administrative data.

Note: If you need help interpreting these guidelines, please contact DCAD.

The data you manage may fall under federally protected law such as FERPA or HIPAA. It is your responsibility to determine whether such laws are applicable to the data you own and manage.

Governance

It is the responsibility of the Client Support Services (CSS), Departmental Computing and Application Development (DCAD), Technology Review Board (TRB) and Information Technology Architecture Group (ITAG) organizations to educate and communicate this policy to all technical staff, clients, and end-users and developers who this might apply to.

Implementation Notes

If your application does not meet these guidelines, then we recommend another supported database and development stack be used. Please contact DCAD for more information.

Best Practices for FileMaker (comparable guidelines apply to MS Access and similar personal databases).

- All recommended measures are being followed. Examples:
 - 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
 - See additional guidelines at <http://web.mit.edu/ist/help/filemaker/fmug/Top10.pdf>
 - See more detailed information at <http://web.mit.edu/ist/db/fm/>

Review History

Date	Version	Author	Change	Reviewers
8/1/2006	0.1	S. Thorne	Document Creation	Wilson D'Souza,
8/16/2006	0.3	S. Thorne	Added feedback from ITAG meeting	ITAG
9/12/2006	0.4	S. Thorne	Feedback from DCAD	ITAG
9/21/2006	0.5	S. Thorne	Feedback from ITAG, DCAD	
9/22/2006	0.6	C. Marra	Additional edits	
9/25/2006	0.7	C. Marra	Edits from DCAD team mtg	
10/04/2006	0.8	S. Thorne	Edits from ITAG meeting	
11/07/2006	0.9	W. D'Souza	Feedback from DCAD, CSS and ITAG	CSS, ISDA