PennState
College of Arts and Architecture

Filemaker Database Hosting Procedure
College of Arts and Architecture

This procedure outlines the requirements for hosting a database on the A&A college Filemaker server. These requirements must be followed for a database to be hosted, and all hosted databases will be checked for compliance. AAIT will work with database creators to ensure compliance with these requirements before a database is permitted to be hosted. In the event a hosted database is found to have fallen out of compliance, AAIT will work with the database creator to bring it back into compliance in a timely manner. If this cannot be achieved in a timely fashion the database will be temporarily removed from the server until such time as the issue can be resolved. This procedure is designed to ensure the security of all data in hosted databases and the hosting server in general.

1. All databases must have the fmdbadmins group defined in the Accounts and Privileges to have full access. This allows AAIT systems administrators to verify database compliance with these requirements. AAIT will ensure proper membership of this group.
2. Guest access must be disabled in all databases.
3. No internal accounts are permitted beyond the built in admin account except as specifically noted below. All access should be conducted through external accounts, which are maintained in Active Directory by AAIT systems administrators. Contact AAIT if groups are needed or complete the Request for Network Services form.

Database creators are responsible for the following:

1. Understanding the impact and options in the Accounts and Privileges section of their databases. See the document on Filemaker Security for further details.
2. Ensuring groups (external accounts) have only been granted the access they need following the principles of least privileged access. This prevents a data entry user from accidentally modifying a layout or a read only user from modifying data.
3. Ensuring the proper users are members of the assigned groups by communicating with AAIT, and updating AAIT as soon as the membership of a group needs to be modified. While AAIT removes users when notified of termination of service, this notice is not always sent, and does not account for change of access needs while still a member of the college.
4. Ensuring the password on any internal account (specifically the admin account) complies with PSU password policy on strength and complexity.
5. Ensuring some method of secure password storage with internal failover, such that a backup person can access the database in the absence of the creator. External accounts do not allow permission modification so AAIT will not be able to assist even with the fmdbadmins account compliance.
6. Ensuring all data in a database is compliant with PSU data policies such as GURU AD23, AD71, AD19, and AD35.

AAIT is responsible for the following:

1. Keeping track of who requested a Filemaker group and ensuring only that requestor or persons delegated by them can make requests to change the group membership.
2. Updating group membership in a timely fashion to meet the needs of the database creators.
3. Checking and verifying the rules in this procedure statement are followed on hosted databases.

For the sole purpose of external collaboration (individuals who do not have active PSU Access Accounts), user accounts can be created in a Filemaker database that are given to external individuals. These accounts replace the built in guest access as they are more secure. They can be given to multiple individuals and are therefore considered shared or group accounts. Said accounts will only have access to a given database, and the creation of such accounts will be a last resort after Friends of Penn State, STAA, and other options have been exhausted. These accounts can only be created after a Group Account Request form is completed and authorized.