Hixson-Lied College of Fine and Performing Arts

FileMaker Database Hosting Policy

Purpose

This policy outlines the requirements for hosting a database on the College FileMaker server. These requirements must be followed for a database to be hosted. All hosted databases will be checked for compliance.

The CFPA ITS FileMaker Database Hosting service is intended to provide a reliable and secure hosting infrastructure for all College FileMaker databases. The requirements in this policy provide reasonable security for the data within each database. CFPA ITS will work with database developers to ensure compliance with these requirements before a database is hosted. In the event a hosted database is found to have fallen out of compliance, CFPA ITS will work with the developer 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 the issue can be resolved. This policy is designed to ensure the security of all data in hosted databases and the hosting server in general.

Security

1. Sensitive data is not permitted on the CFPA ITS FileMaker server. Sensitive data includes social security numbers, credit card or other bank account information, medical information, or any other information that might lead to identity theft.
2. Hosted FileMaker databases are only accessible on specific wired UNL networks. If a user must access a database from a UNL wireless network or from off campus, a Virtual Private Network connection is required.
3. Guest access must be disabled in all databases.
4. All database access will be managed through external UNL-AD groups. No internal accounts are permitted beyond the built in admin account, which will be owned by CFPA ITS to ensure the security of the database.
5. All databases names must use one of the following department prefixes: AAH, CFPA, JCS or SOM. Examples would be “SOM Band Marching Uniforms” or “AAH Faculty Mailing List”.

Database Developer Responsibilities

1. Plan database implementations in advance. CFPA ITS will do its best to upload databases in a timely manner, but cannot guarantee databases will be uploaded the same day they are submitted.
2. Developers will design, fix, and adapt databases for the web. Currently CFPA ITS is only staffed to maintain the FileMaker server and cannot provide any additional support.
3. Understand the impact and options in the Privilege Sets and Accounts settings of their databases.
4. Configure all necessary Privilege Sets before submitting a database for hosting and ensure UNL-AD groups have only been granted the access each group needs. This will ensure a data entry user does not accidentally modify a layout or other database settings. Once a database is hosted, Privilege Sets and Accounts can only be modified by CFPA ITS staff.
5. Inform CFPA ITS whenever user membership in UNL-AD groups needs to be changed. A user will not be added to or removed from a UNL-AD group until the developer or designated admin notifies CFPA ITS of the user change. If students have been granted access to a database, the developer or designated admin is responsible for notifying CFPA ITS when the student no longer needs access. Students may need to be removed at the end of a semester, at graduation, or at termination of employment.

CFPA ITS Responsibilities

1. Verify the integrity of hosted databases and maintain scheduled off-site backups.
2. Upload new databases and update database security settings in a timely fashion to meet the needs of the database developers and users.
3. Ensure that only the database developers or designated admins can make requests to change the security settings of databases or UNL-AD group membership. All changes will be logged.
4. Verify that all applicable policies are followed on hosted databases.