CITY OF MADISON INFORMATION TECHNOLOGY

Microsoft Access Policy

Overview

Effective: 06/01/2009

Amended: 07/06/2021

Objective: Establish a policy on Microsoft Access usage.

Background

Cyberattacks against government computer networks are unfortunately now common place and have to be prepared for. These attacks result in financial losses, lost productivity, system damage, and lost and/or compromised sensitive data. A single, poorly secured application on the City network can put the entire network at risk. There are many concerns surrounding Microsoft Access' poor security controls and its role as a substitute for enterprise applications. The software presents deficient internal controls as identified by external auditors. In today's regulatory environment (PHI, PCI, CJIS, HITECH, GASB-34, FTI), there is a need to hinder unsanctioned Access applications in the enterprise to improve security and mitigate inherent weaknesses within the software.

Some potential Access problems include, but are not limited to:

- **Few users are experts, and often make errors in calculations that end up skewing entire files.** Planning sessions consequently go awry when executives show up with their own data sets and cause confusion over whose information is right.
- **Financial and Resource Management statements are prepared using poorly designed Access tables.** The data's accuracy becomes compromised, and staff end up wasting many hours verifying the validity of the numbers rather than performing their jobs. Worse, this faulty information is used to make important business decisions that are not aligned with organizational goals and do not meet regulatory compliance or financial reporting requirements.
- **Information Technology (IT) has little or no responsibility for an Access file's existence or support.** The valuable data contained within the file may not be backed up, secured, or checked for quality.
- **Access files quickly become overly cumbersome and complex, ultimately breaking down since Access lacks sufficient scalability to grow as data requirements.** IT is brought in to sort it all out, only to discover that no documentation was written regarding the creation or purpose of the Access files, and the system was poorly constructed, often times with serious flaws. For more information about Access database file limits, please refer to this Microsoft support article.
- **Databases are often created to fill perceived shortcomings in corporate applications when a new query, report, or small modification would meet those needs.** This results in duplication of data across the organization and raises questions

about which data should be used with decision making, and leads to silos of information that cannot be easily shared.

- **Often users eventually decide their Access data needs to integrate with other data sources or extend to the Internet.** Access's lack of controls and the poor design of most systems makes this a difficult and labor-intensive process, if not impossible. Data from Access Databases will never be displayed on a City website.
- **The front-end application and database are combined in the same file.** This means application controls and database controls are one in the same, which is a security threat. Anyone that has permission to run the application has permission to do anything within the application.
- **Access lacks some controls altogether, which include:** Database controls, input controls, processing controls, output controls, and auditing controls.

Policy

The following outlines the IT policy on Microsoft Access:

1. **IT will limit Access support.** Beyond giving users network file permissions to existing Access applications, IT cannot commit to providing further support due to limited staff resources.
2. **Existing Access applications can remain.** IT will not be removing existing Access applications and will not be able to provide further support beyond network file permissions as stated above.
3. **Migrate to current platforms.** Agencies should consult with IT staff to evaluate data risks posed by Access and create a plan to migrate the data to a more stable and controlled platform or delete the data entirely. This may incur additional costs for the agency, but migrating the data may provide long-term benefits for sustainability. IT will migrate the data to an enterprise system for existing Access databases.

Enterprise Systems

There are other enterprise systems supported by IT that can replace Access databases. These systems can provide better technical support and reporting capabilities when compared to Access. It is highly recommended that agencies migrate their data to one of these systems to take advantage of these benefits.

Exceptions

Any exceptions to this policy will require written approval of the IT Director or their designated employee. Requests shall be in writing, will state the specific policy item that is being challenged, and the business reason for the exception. The decision of the IT Director shall be final.