



FEMA

Microsoft Access REQUEST FORM

Request Date:	
----------------------	--

Sponsor Information:

Name:		Office:	
FEMA Login ID:		Phone Number:	
Email Address:			

Supervisor Information:

Name:		Office:	
Email Address:		Phone Number:	

Database Information:

Request Type:	<input type="checkbox"/> New MS Access	<input type="checkbox"/> Existing MS Access	<input type="checkbox"/> Remove MS Access
Database Requested:			
Contains PII:			
Database Location:			
Database Version:			
MS Access Version:			
Brief statement of the operational requirements:			

Certification:

As the requestor of the account, I certify that I have read and signed the *Rules of Behavior for MS Access* and agree to terms within, using Microsoft Access per operational necessity of the aforementioned database(s).

Sponsor's Print Name: _____ **Signature:** _____ **Date:** _____

As the supervisor of the above named requestor, I certify that I have read the above statement on the operation requirement, read and signed the *Rules of Behavior for MS Access*, and approve this request for a MS Access Use based on its operational necessity.

Supervisor's Print Name: _____ **Signature:** _____ **Date:** _____

Retain a copy for your records

Database Name:	
-----------------------	--

Sponsor's Name		
	Last Name	First Name

Upon completion, please return FAX pages 1 and 2 via any of the following methods:

EMAIL: FEMA-Enterprise-Service-Desk@fema.dhs.gov
FAX: (540) 686-4468

SDI USE ONLY

<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved	Date:		By:	
	SDI Notes:			
	Reason for Disapproval (if required):			
	Date Last Validated:			

IT SECURITY USE ONLY

<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved	Date:		By:	
	ITSB Notes:			
	Reason for Disapproval (if required):			
	Date Last Validated:			

Retain a copy for your records



Rules of Behavior for Microsoft Access

Policy for USE of Computer Resources.

As an employee, contractor, or visitor of the Federal Emergency Management Agency (FEMA), you are required to be aware of, and comply with the FEMA's policy on all usage and security of computer resources.

You are responsible for all actions performed with Microsoft Access with your Network ID.

- Microsoft Access will be used for the performance of official business on the requested databases(s) only.
- You must take necessary steps to prevent any unauthorized person from gaining knowledge of the password.

Policy, standards, and procedures must be followed.

- Use of all computer resources, including personal computers, laptops, all parts of the FEMA network, communication lines, and computing facilities are restricted to FEMA official business activities.
- Be aware that all computer resources assigned, controlled, accessed, and maintained by FEMA employee, tenet, and contractor personnel are subject to periodic test, review, and audit.

Access to information must be controlled.

- The account privileges and permissions must be assigned "least" privileges required to perform functions.
- Full auditing of account and workstation activity must be enabled.
- Microsoft Access need shall be reviewed annually for renewal.
- All FEMA user account and password policies must be followed as defined in the DHS Sensitive Systems Handbook 4300
- When handling Personally Identifiable Information, all employee, tenet, or contractor personnel with access to the database must follow the guidelines stated within the *DHS Handbook for Safeguarding Personally Identifiable Information*.
- Only access information for which you are authorized, and have a "need-to-know/access."
- Do not leave computers logged-on and unattended.
- If you know that a person, other than an individual granted knowledge, has used or is using this userID, you must report the incident immediately to your supervisor, the Information System Security Officer, and the Office of Cyber Security.
- Take steps necessary to maintain security of computer files and reports containing FEMA information.

You are responsible for the proper use of your computer resources.

- Only use FEMA approved software, and complies with vendor software license agreements.
- Back-up your programs and data on a regular basis, and do not store sensitive or mission critical data on your PC's hard-drive.
- All FEMA computer resources, including hardware, software, programs, files, paper reports, and data are the sole property of the FEMA.

Retain a copy for your records