Print Form

**MEMORANDUM**

**SUBJECT**: AQS USER SECURITY GUIDELINES

**TO:** ALL AQS USERS

**FROM:** Michael W. Hamlin, AQS Security Officer

## PURPOSE

The AQS User Security Guidelines have been prepared to outline the security measures for the reengineered AQS system, to explain why these measures were developed, and to request the support of all users in complying with these measures. The security measures for AQS are intended to protect the air quality data that State and local agencies periodically submit to EPA. This protection is designed to prevent unauthorized modification or loss of data, while at the same time protecting the underlying computer system that EPA operates.

The reengineered AQS application, and the data it contains, supports EPA, as well as State, local and tribal agencies needing information to carry out air quality management programs. All users must ensure that the AQS application and its data are protected from loss, misuse, and unauthorized access or modification.

### EPA's Security Measures for AQS

The reengineered AQS is an Oracle database management system located on EPA's National Computer Center (NCC). As such, AQS is bound by and relies upon the security procedures set forth by the NCC. These measures primarily involve the use of user accounts, user IDs, passwords and Oracle security. Briefly, these procedures require that:

a. Any individual who needs access the AQS data base must be approved and be authorized to do so. Authorized individuals will be given an EPA account and a NCC user ID. The user ID and a secure password (determined by the user) must be used when accessing the NCC and AQS database. Certain AQS users (primarily State and local agency representatives) are given controlled authority to Aupdate@ the AQS data base (i.e., they may add or modify data for their particular agency).

b. A user ID is assigned only to an individual (rather than an agency) and only to an individual in the State, local or tribal agency who requests access to AQS in writing. Requests are approved by the appropriate EPA Regional Office AQS contact and Regional RACF Administrator.

Individuals granted user ID's are responsible to use their ID's in an appropriate manner at all times and ensure that the access they have been personally granted is not shared with others (either deliberately or inadvertently).

c. AQS data are backed-up on a nightly basis so that if the production database were compromised, the data base could be rebuilt from the back-up files. This security measure assures that the vast majority of the data would be protected from alteration with only data uploaded or changed after the last nightly back-up being potentially lost.

## AQS Application Guidelines for All Users

There are certain security practices and guidelines that must be followed to minimize the potential misuse or damage to the AQS database. These include:

### General

- Be familiar with the security policies and practices involving the AQS application
- Maintain security for the application by using established security mechanisms (use of unique user ID and password) and practices when accessing the AQS application.
- Do not attempt to view, change, or delete data unless you are authorized to do so.
- Be alert to potential threats to corrupt or destroy AQS application and database.

### Password Protection

- Guard your user ID and password. Do not disclose your password to others.
- Control access to your PC. Log off whenever you leave your machine.
- Change your application password every 90 days. Use at least 9 characters in your application password. Use a mix of alpha and numeric characters.
- Use a screen saver that requires the use of a password to reactivate the system.
- For passwords, do not use family names, birthdays, sports teams' names, or words that can be found in the dictionary.
- For passwords, do not use consecutive keys on a keyboard or all the same character.
- Use new passwords. Do not use increments of old passwords.
- If you believe your password has been compromised, change it immediately.
- Memorize your password rather than writing it down somewhere.

### Whom To Notify

- Notify the Security Officer for the reengineered AQS application immediately of security incidents (Mr. Michael Hamlin at 919-541- 5232).
- Notify the AQS application manager (Mr. Jake Summers at 919-541-5695) when staff have been terminated or changed positions to have their access to the application terminated.

### Summary

This information was prepared to advise you of the security measures for the reengineered AQS system. The goal is to assure that the contents and integrity of AQS data will be secure. In order to maintain security for the data provided in AQS, these guidelines must be followed. The security measures that have been established are designed to protect the data that State, local and tribal agencies submit, while at the same time protecting the computer systems that EPA operates.

Print Form

# AQS User Security Guidelines Signature Page

I have read the AQS User Security Guidelines and will comply with what has been outlined to insure the security of AQS is not violated.

Agency of AQS User

Printed Name of AQS User

Signature of AQS User ______________________________

Date