

## AQS User Security Guidelines

The AQS User Security Guidelines have been prepared to outline the security measures for AQS, 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 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

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 to 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 database (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

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

## Rules of Behavior

- a. I understand that my AQS user-id and password are intended for my individual use only, and agree to not share them with others.
- b. I will protect my AQS password from accidental exposure; e.g. I will not write it down and leave it exposed in an unsecured location.
- c. If I suspect that my AQS account has been used by someone else, I will notify the EPA Call Center immediately (email: [epacallcenter@epa.gov](mailto:epacallcenter@epa.gov), phone: 866-411-4372).
- d. I will not attempt to access or modify any AQS data which I am not authorized to access or change.
- e. I will not degrade the availability of AQS for other users by submitting more than five concurrent batch load jobs or five concurrent report jobs.
- f. If my duties change and I am no longer required to interact with AQS by the organization that authorized my access, I will notify the EPA Call Center immediately.
- g. If I am no longer employed by the by the organization that authorized my access, I will notify the EPA Call Center immediately.
- h. I agree to abide by all published AQS security guidelines (e.g. changing my password as per the published schedule).
- i. If at any time, I am no longer able to comply with AQS guidelines, I will notify the EPA Call Center immediately.

## Password Protection

- a. Guard your user ID and password. Do not disclose your password to others.
- b. Control access to your PC. Log off whenever you leave your machine.
- c. Use a screen saver that requires the use of a password to reactivate the system.
- d. For passwords, do not use family names, birthdays, sports teams' names, or words that can be found in the dictionary.
- e. For passwords, do not use consecutive keys on a keyboard or all the same character.
- f. Use new passwords. Do not use increments of old passwords.
- g. If you believe your password has been compromised, change it immediately.
- h. Memorize your password rather than writing it down somewhere.

## Whom To Notify

AQS User Support is provided through the EPA Enterprise IT Service Desk (EISD), which is operated under contract to the EPA. The toll free number is 1-866-411-4EPA - (4372), select option 9. TDD: 1-866-489-4900, International callers: 1-703-679-1070. Their hours of operation are 6:00am - 9:00pm E.T. (Monday - Friday, excluding Federal holidays). You may also contact the Call Center via email (EISD@epa.gov) or fax (703-674-1008).

## Summary

This information was prepared to advise you of the security measures for the 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.

## **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