

Section 7. Legal and Security Considerations

This section focuses on legal and security considerations for all user types to ensure security and reliability of the user accounts and data submitted through the LT2 DCTS. By using web forms or the XML upload process to submit LT2 data, the DCTS reduces the burden on reporting facilities and responsible environmental agencies for collecting and reporting data, and for keeping records. The reduced burden is a result of eliminating labor, time, and other costs associated with submitting data on paper. It is important to note, however, that electronic reporting does not alleviate or alter a submitter's responsibilities or liabilities.

7.1 Application Location

The LT2 DCTS is hosted on USEPA's Research Triangle Park (RTP) database and Internet Web servers. All users access the LT2 DCTS directly through the USEPA servers via their Internet connection and Web browser. The LT2 DCTS is hosted within a secure environment and monitored by USEPA's National Technology Services Division (NTSD). The LT2 DCTS was designed and developed in accordance with all USEPA policies and procedures for public access databases intended for release into the central environment.

7.2 LT2 User Responsibilities

The USEPA relies on all LT2 users to ensure that the data are protected from loss, misuse, and unauthorized access or modification. Users are required to behave in an ethical and trustworthy manner. Users should not attempt to perform actions or processing for which they do not have authorization. Actions related to LT2 database administration are tracked using audit trails.

Update authority at the PWS and laboratory is controlled by the individual organizations. Enforcement of security for these facilities is not a USEPA responsibility. All LT2 users are responsible and accountable for the use of the data either through direct access or via applications the users develop.

7.3 Passwords

Each individual is responsible for maintaining the integrity of his/her own User Name and Password. Transactions made with your User Name and Password are considered approved and submitted by you. If you believe your User Name or Password has been compromised, email LT2 Technical Support, at stage2mdbp@epa.gov, or contact the LT2 Hotline, at 1-888-LT2-0020.

Users can help ensure the integrity of their passwords by taking the following precautions:

- Change your passwords every 30 days
- Use passwords containing at least eight characters, including letters and numbers
- Do not use family names, birthdays, words describing personal interests or facets of your life that could be guessed, or words found in a dictionary
- Use a different password than those used within the last eight versions of your password
- Control access to your PC workstation and logout whenever leaving your machine.

7.4 Record Keeping

USEPA recommends that you keep a copy of all transactions (including the time and date) sent to and received from USEPA or in accordance with your policies and procedures. These transactions may include submissions, receipt acknowledgments, error messages, resubmissions, and transmissions. The saved copies are your audit trail for submissions to USEPA.

The LT2 Rule will require laboratories to keep hardcopies of all quality control (QC) data for all data submitted. Laboratories may only submit data to the LT2 DCTS that has met all of the QC requirements. Common business practice is to back up and archive your electronic data in case the system fails. As technology progresses and you upgrade, you may want to consider backward compatibility for document retrieval. You also should consider keeping more than one copy as a backup in case the hardware or software fails, a virus attacks, or other technological anomalies occur.