

Db2 Mask

Mask Production Data Before Use in Test

- Test Safer
- Regulation Compliance
- Test Smarter

Business Challenges

Meeting audit and government (**HIPAA and Gramm-Leach-Bliley Act**) requirements or just properly safeguarding your client or employee information can be difficult. Sensitive information should be restricted from test environment(s) where it could be breached.

Test Db2 Applications Safely

TestBase **Db2 Mask** from Softbase allows you to mask sensitive data during the extract process, before it hits the test DASD. It is available to users who also have Testbase **Db2 Subset** which manages subsets of referentially intact data from multiple Db2 subsystems throughout the enterprise. Users define mandatory masking that must be applied to production or other sensitive sources of data. TestBase **Db2 Subset** then, ensures sensitive production data remains completely private during testing by applying the Db2 Masking rules at extract time.

Integrated with Other TestBase Components

TestBase Db2 Subset – Db2 Mask is executed as part of Db2 Subset. Mandatory masks are defined and applied to production data providing data privacy and regulatory compliance.

Masking Rules

Masking rules which can keep sensitive data safe include:

Table Input	Data from a table
File Input	Data from a file
Test View	Data from SQL results
Supplied Value	Tables of values supplied
Random	Random number generated
Jumble	Swap digit or char positions
Translate	Lookup in a translate table

Masking rules can only be set up and changed by authorized users.

Masking Audit Reports

The following reports are available on request by authorized personnel at any time:

Privacy Definitions	How data is supposed to be masked
Privacy Definition History	History of how data was supposed to be masked
Privatized Execs	Sample masked and unmasked data
Non-Privatized Execs	Executions by authorized personnel that is not masked and where the data is loaded

Audit reports are saved and authorized to audit personnel.