**Dynamic Data Masking –** provides a much more efficient solution to protecting sensitive data (SSN, Account#, CreditCard etc) .

* It masks data to non-privileged users.
* It can mask a predetermined amount of the sensitive data
* All masking is done at the database level without modify the data
* Masking is applied automatically to query results based on dynamic data masking rules.

For example, it can obfuscate/mask the first 5 characters of the SSN. There are four (4) functions you can use to when implementing DDM:

* + Default – Full masking according the data types of the designated fields.
    - Binary, varbinary, numeric, or image data types are masked with 0s.
    - Data and time data is masked with 01.01.1900:00:00:00:0000000
    - String data type are masked with Xs.
  + Email – Display the first character of the email and the suffix. Ie. [aXXXX@XX.com](mailto:aXXXX@XX.com)
  + Random – Masks the original value with a random value within a specified range.
  + Custom- Masking method that exposes the first and last letters and adds a custom padding string in the middle. prefix,[padding],suffix

/\*\*\*\* Implement Default Masking \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

ALTER TABLE SensitiveData

ALTER COLUMN CreditRating ADD MASKED

WITH (FUNCTION = 'default()')

CREATE USER NPUser WITHOUT LOGIN

GRANT SELECT ON SensitiveData TO NPUser

EXECUTE AS USER = ‘NPUser’

SELECT \* FROM SensitiveData;

REVERT;

/\*\*\*\*\* Implement partial Masking \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

ALTER TABLE SensitiveData

ALTER COLUMN SSN ADD MASKED

WITH (FUNCTION='partial(0, "XXX-XX-", 4)')

ALTER TABLE SensitiveData

ALTER COLUMN CreditCard ADD MASKED

WITH (FUNCTION='partial(0, "CCCC-CCCC-CCCC-c", 3)');

/\*\*\*\*\*\*\* Implement Email Masking \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

ALTER TABLE SensitiveData

ALTER COLUMN Email ADD MASKED

WITH (FUNCTION='email()');