**Step 8: Row Level Security**

Name: Vaishnavi Pravin Apsingkar

NN: 142

**Setup:**

CREATE VIEW vTruckInfo142 AS

SELECT DISTINCT d.DriverID, d.Name, d.Salary, tr.TruckID, tr.Description

FROM Driver d

JOIN Trip t ON d.DriverID = t.DriverID

JOIN Truck tr ON t.TruckID = tr.TruckID;

**Result:**

Commands completed successfully.

**Part A: Access**

**Grant SELECT access to the view vTruckInfo142 to three employees KOT\_Alice, KOT\_Jack and KOT\_Joe:**

GRANT SELECT ON vTruckInfo142 TO KOT\_Alice;

GRANT SELECT ON vTruckInfo142 TO KOT\_Jack;

GRANT SELECT ON vTruckInfo142 TO KOT\_Joe;

**Result:**

Commands completed successfully.

**Part B: Row level security**

CREATE FUNCTION dbo.fnSecurityPredicateTruck142(@DriverID char(4), @Status char(10))

RETURNS TABLE

WITH SCHEMABINDING

AS

RETURN SELECT 1 AS fnSecurityPredicate\_result

WHERE (

(@Status = 'Full' AND USER\_NAME() = 'KOT\_Jack')

OR

(@Status = 'Part' AND USER\_NAME() = 'KOT\_Alice') );

**Result:**

Commands completed successfully.

**Creating policy:**

CREATE SECURITY POLICY dbo.securityPolicy\_Driver142

ADD FILTER PREDICATE dbo.fnSecurityPredicateTruck142 (DriverID, Status)

ON dbo.Driver

WITH (STATE = ON);

**Result:**

Commands completed successfully.

**Grant permission to Jak and Alice to view data on Driver table:**

GRANT SELECT ON dbo.Driver TO KOT\_Jack;

GRANT SELECT ON dbo.Driver TO KOT\_Alice;

**Part C: Test the row level security**

**For KOT\_Jack:**

EXECUTE AS USER = 'KOT\_Jack';

SELECT \* FROM Driver;

REVERT;

**Result:**

DriverID Name Salary StartDate Status

-------- -------------------- --------------------- ---------- ----------

D101 xxxx 0.00 2021-11-12 Full

D102 xxxx 0.00 2021-10-30 Full

D107 xxxx 0.00 2022-01-12 Full

D225 xxxx 0.00 2021-05-15 Full

D280 xxxx 0.00 2022-01-12 Full

(5 rows affected)

**For KOT\_Alice:**

EXECUTE AS USER = 'KOT\_Alice';

SELECT \* FROM Driver;

REVERT;

**Result:**

DriverID Name Salary StartDate Status

-------- -------------------- --------------------- ---------- ----------

D110 xxxx 0.00 2021-06-22 Part

D142 xxxx 0.00 2023-01-06 Part

D301 xxxx 0.00 2022-03-05 Part

D302 xxxx 0.00 2022-03-06 Part

(4 rows affected)

**CORRECTION 1:**

REVOKE SELECT ON dbo.Driver FROM KOT\_Jack;

REVOKE SELECT ON dbo.Driver FROM KOT\_Alice;

**Checking:**

EXECUTE AS USER = 'KOT\_Jack';

SELECT \* FROM dbo.vTruckInfo142;

REVERT;

DriverID Name Salary TruckID Description

-------- -------------------- --------------------- ------- -----------

D280 xxxx 0.00 B-001 Chev Box

D101 xxxx 0.00 B-017 Ford Box

D107 xxxx 0.00 B-018 Ford Box

D102 xxxx 0.00 S-001 Volvo Semi

D225 xxxx 0.00 S-017 Kenworth

(5 rows affected)

EXECUTE AS USER = 'KOT\_Alice';

SELECT \* FROM dbo.vTruckInfo142;

REVERT;

DriverID Name Salary TruckID Description

-------- -------------------- --------------------- ------- -----------

D301 xxxx 0.00 B-001 Chev Box

D301 xxxx 0.00 B-017 Ford Box

D302 xxxx 0.00 B-018 Ford Box

D142 xxxx 0.00 B-019 Ford Box

D110 xxxx 0.00 S-002 Peterbuilt

(5 rows affected)

**Correction 2:**

**Drop security policy:**

IF EXISTS (SELECT \* FROM sys.security\_policies WHERE name = 'securityPolicy\_Driver142')

DROP SECURITY POLICY securityPolicy\_Driver142;

GO

**Drop predicate function:**

IF OBJECT\_ID('dbo.fnSecurityPredicateTruck142', 'IF') IS NOT NULL

DROP FUNCTION dbo.fnSecurityPredicateTruck142;

GO

**Recreate predicate function:**

CREATE FUNCTION dbo.fnSecurityPredicateTruck142(@Status char(10))

RETURNS TABLE

WITH SCHEMABINDING

AS

RETURN (

SELECT 1 AS fnSecurityPredicate\_result

WHERE (

(@Status = 'Full' AND USER\_NAME() = 'KOT\_Jack')

OR

(@Status = 'Part' AND USER\_NAME() = 'KOT\_Alice')

));

GO

**Recreate security policy:**

CREATE SECURITY POLICY dbo.securityPolicy\_Driver142

ADD FILTER PREDICATE dbo.fnSecurityPredicateTruck142(Status)

ON dbo.Driver

WITH (STATE = ON);

GO

**Testing:**

EXECUTE AS USER = 'KOT\_Jack';

SELECT \* FROM dbo.vTruckInfo142;

REVERT;

**Result:**

DriverID Name Salary TruckID Description

-------- -------------------- --------------------- ------- -----------

D280 xxxx 0.00 B-001 Chev Box

D101 xxxx 0.00 B-017 Ford Box

D107 xxxx 0.00 B-018 Ford Box

D102 xxxx 0.00 S-001 Volvo Semi

D225 xxxx 0.00 S-017 Kenworth

(5 rows affected)

EXECUTE AS USER = 'KOT\_Alice';

SELECT \* FROM dbo.vTruckInfo142;

REVERT;

**Result:**

DriverID Name Salary TruckID Description

-------- -------------------- --------------------- ------- -----------

D301 xxxx 0.00 B-001 Chev Box

D301 xxxx 0.00 B-017 Ford Box

D302 xxxx 0.00 B-018 Ford Box

D142 xxxx 0.00 B-019 Ford Box

D110 xxxx 0.00 S-002 Peterbuilt

(5 rows affected)

**Negative testing:**

EXECUTE AS USER = 'KOT\_Jack';

SELECT \* FROM Driver;

REVERT;

**Result:**

Msg 229, Level 14, State 5, Line 2

The SELECT permission was denied on the object 'Driver', database 'KOT142', schema 'dbo'.