

Appendix D

The following is an example of Row Level Security.

Row Level Security Setup

The following creates a table of “accounts” where rows may be labeled with a security label to filter results based on role membership.

```
-- Create table with security labels
CREATE TABLE accounts(id SERIAL PRIMARY KEY, name TEXT NOT NULL,
    phone_number TEXT NOT NULL, security_label TEXT);

ALTER TABLE accounts ENABLE ROW LEVEL SECURITY;

-- Create groups that map to security-labels
CREATE ROLE unclassified;
CREATE ROLE classified;

-- Add roles to groups
CREATE ROLE bob LOGIN IN GROUP unclassified;
CREATE ROLE alice LOGIN IN GROUP classified;

-- Dummy data
INSERT INTO accounts(name, phone_number, security_label) VALUES ('bob', '123-456-7890', 'unclassified');
INSERT INTO accounts(name, phone_number, security_label) VALUES ('alice', '098-765-4321', 'classified');

-- Function to check if user is in group for security label filtering
CREATE OR REPLACE FUNCTION user_in_group(group_name TEXT, user_name TEXT)
RETURNS boolean
AS 'SELECT EXISTS(
    SELECT grosysid FROM pg_group WHERE groname = $1
    AND (SELECT usesysid FROM pg_user
        WHERE username = $2) = ANY(grolist));'
LANGUAGE SQL;

-- Row level security policy for information
CREATE POLICY classification_filter ON accounts
    USING ((SELECT user_in_group(accounts.security_label, current_user)));

-- Allow access to table
GRANT SELECT ON accounts TO classified;
GRANT SELECT ON accounts TO unclassified;
```

```

-- Change to role bob and query table
SET ROLE bob;
SELECT current_user;
SELECT * FROM accounts;

RESET ROLE;

-- Change to role alice and query table
SET ROLE alice;
SELECT current_user;
SELECT * FROM accounts;

RESET ROLE;

-- Cleanup
DROP TABLE IF EXISTS accounts CASCADE;
DROP ROLE IF EXISTS bob, alice, classified, unclassified;

```

Results

```

current_user
-----
bob
(1 row)

 id | name | phone_number | security_label
-----+-----+-----+-----
  1 | bob  | 123-456-7890 | unclassified
(1 row)

RESET
SET
current_user
-----
alice
(1 row)

 id | name | phone_number | security_label
-----+-----+-----+-----
  2 | alice | 098-765-4321 | classified
(1 row)

```