The Clinic

You are setting up the IT infrastructure for a clinic.

Step 1: Log in as Administrator to the server and create and populate the following database

```
use master
go
create database TouroClinic
go
use TouroClinic
go


create table EMPLOYEETYPE (
   EmpTypeID int not null,
   EmpTypeDescription varchar(20) not null,
   constraint [PK_EmployeeType] primary key (EmpTypeID),
   constraint [UIX_EmplTypeDesc]unique (EmpTypeDescription)

)

insert into EMPLOYEETYPE
    values (1,'DOCTOR'),
           (2,'RECEPTIONIST'),
           (3,'BOOKKEEPER'),
           (4,'ACCOUNTANT'),
           (5,'LAB TECHNICIAN'),
           (6, 'NURSE'),
           (7, 'GUARD'),
            (8, 'ITAdmin'),
           ( 9, 'DBA')


create table PAYROLLTYPE(
    PayrollTypeID int not null,
    PayrollTypeDesc varchar(10) not null,
    constraint [PK_PayrollType] primary key (PayrollTypeID),
    constraint [UIX_PayrollTypeDesc] unique(PayrollTypeDesc)

);

insert into PAYROLLTYPE
values (1, 'MONTHLY'),
       (2, 'WEEKLY'),
       (3, 'HOURLY')



create table EMPLOYEE(
   EmployeeID int not null,
   FirstName varchar(15) not null,
   LastName varchar(35) not null,
   Birthdate date not null,
```

```
   SocialSecNum  char (9) not null,
   CellPhone char(10)not null,
   HireDate date not null,
   EmployeeType int not null,
   PayrollType int not null,
   CurrentPayAmount decimal(7,2),
   TotalPayrollReceipts decimal(7,2),
   constraint [PK_Employee] primary key (EmployeeID),
   constraint [UIX_EmpSSNum]unique (SocialSecNum),
   constraint [CHK_HireDate] check (dateDiff(year,birthdate,hiredate)>=18),
   constraint [FK_EMP_EMPTYPE] foreign key (EmployeeType)
      references EMPLOYEETYPE(EmpTypeID),
   constraint [FK_EMP_PAYROLLTYPE] foreign key (PayrollType)
     references PAYROLLTYPE(PayrollTypeID)  ,
    constraint [CHK_PAY] check (  CurrentPayAmount > 0 and
        CurrentPayAmount <=30000)

 );



create table SPECIALTYCODE(
   SpecialtyID int not null,
   SpecialtyCodeDesc varchar(20) not null,
   constraint [PK_SpecialtyCODE] primary key (SpecialtyID),
   constraint [UIX_SpecialtyCode] unique(SpecialtyCodeDesc)
)

insert into SPECIALTYCODE
  values (1, 'PEDIATRICS'),
          (2, 'CARDIOLOGY'),
          (3, 'PULMONOLOGY'),
          (4,'RADIOLOGY'),
          (5,'HEMOTOLOGY')



CREATE TABLE DOCTOR(
      DoctorID int NOT NULL,
      EmergencyPhoneNumber char(10) NOT NULL,
      SpecialtyID int NOT NULL,
 CONSTRAINT [PK_DOCTOR] PRIMARY KEY (DoctorID) ,
 constraint [FK_DOCTOR_EMPLOYEE] foreign key (DoctorID)
   references Employee(EmployeeID),
  constraint [FK_DOCTOR_SPECIALTY] foreign key (SpecialtyID)
   references SpecialtyCode ( SpecialtyID)
   );

create table PAYROLLTRANSACTIONS(
   TransactionDate date not null,
   EmpID int not null,
   GrossPay decimal(5,2) not null,
   TaxWithHeld decimal(5,2) not null default (0),
   AddAmtWithHeld decimal (5,2) not null default (0),
   NetPay decimal(5,2) not null,
   constraint [PK_PayrollTrans] primary key (TransactionDate,EmpID),
   constraint [FK_PayTrans_Emp] foreign key (EmpID)
```

```
    references Employee(EmployeeID),
   constraint [CHK_TAXAMT] check ( TaxWithHeld < GrossPay),
   constraint [CHK_NetPay] check (NetPay <= grosspay)
);
```

Step 2: Insert a number of records in the Employee table and related records in the Doctor table for those Employees who are doctors. Insert a few payroll transactions for at least one employee.

Step 3. Logged in as Administrator , access AD (Active Directory)

- Create a new OU (Organizational Unit) TouroClinic
- Within the TouroClinic create an OU called Groups and an OU called Users
- Within the TouroClinic OU, Groups, Create an AD security group for each **EmployeeType that you anticipate will have to access the system for a valid reason. For example, guards will most likely NOT have to access the system at this point.**
- Within the TouroClinic OU, Users, Create user for each of the Employees you set up in the Employee table **that will have to access the system**. Assign each user to his/her appropriate AD group
  - Record the user name and the user password in a safe place so that you can easily reference this information

Step 4: As Administrator, log in to the SQL Server on the server machine. Create a log in for each Windows security group that you set up for the TouroClinic company, **if and only if there is reason to believe they will have to access the database system**.

Assign the DBA group login to the sysadmin server role
GRANT the ITAdmin the server permission CREATE ANY DATABASE
All the remaining logins should simply inherit the public server role.

Step 5: As Administrator , create a TouroClinic **database role** for each of the Employee Types (besides for GUARD and any other employee type that you decided need not access the database system at this point in time).

Step 6: create a view that extracts only some of the data stored about each employee

```
create view EmployeeData (EmpID, FName,LName,CellPhone,EmpType)
  as (select EmployeeID, FirstName ,   LastName ,
   CellPhone ,  EmployeeType from employee )
```

Step 7: Create the following two schemas in the TouroClinic database: ACCOUNTING, HR .

- Transfer the tables, EmployeeType, Employee, SpecialtyCode, Doctor from dbo to HR schema
- Transfer the tables, PayrollType, PayrollTransactions to the Accounting schema

Step 8: Assign the following permissions to the TouroClinic database roles

- ACCOUNTANT_ROLE full control over the Accounting schema (read, write , update, delete)
- BOOKKEEPER _ROLE execute rights to usp_payrollTransaction (see step 18)
- RECEPTIONIST _ROLE read rights to DOCTOR table and to the *View* EmployeeData
- DOCTOR _ROLE read rights to the DOCTOR and SPECIALTYCODE table

Step 9: As Administrator set up **one database user** in the TouroClinic database for each **sql server login** that you set up in step 4

Step 10: Assign each TouroClinic database user the appropriate database role

Step 12: As Administrator log in to the client machine

- Set up a folder on the C Drive TOUROCLINIC
- Within the folder set up two folders DOCTORFOLDER, ACCOUNTANTFOLDER

Step 13: Prevent all TouroClinic security groups from accessing any folders on the local machine, besides for the Doctor and Accounting security groups. Allow the DOCTOR security group full rights the the DOCTORFOLDER and the Accounting security group full rights to the ACCOUNTANTFOLDER.

Step 14: log out as Administrator and log in as a user to the client machine. Verify the security features implemented in the previous step

Step 15: check the windows and application logs to follow up on any security related issues that occurred.

Step 16: write queries to access SQL Server tables to view the server roles, server level permissions, database roles, database level permissions that were assigned while completing this lab exercise.

Step 17: write queries to retrieve the data you inserted into each of the tables

Step 18: create a procedure usp_payrollTransaction which accepts EmpID, GrossPay, TaxWithHeld and AddAmtWithHeld.

The procedure should calculate the NetPay = GrossPay minus (TaxWithHeld + AddAmtWithHeld)
It should insert the record into the PAYROLLTRANSACTIONS table
It should update the Employee record of this EmpID , modify the TotalPayrollReceipts field to include the GrossPay amount of this PayrollTransaction
If there is any error it should rollback the transaction. If all goes well, it should commit the transaction.

Step 19: execute the procedure with correct data

Step 20: execute the procedure with incorrect data