IA 643 Database Security & Auditing
Group Project #4 User Administration

Total Points: 180 Due date: October 25, 2023
Turn-in items
(1) Upload an e-copy of a Word document for Part 1. (2) Upload an e-copy of fully executable script file **(plain text file)** for Part 2. The script code shall create the user profile, the user accounts, and the password complexity verification function.

Part 1: OS User Administration (30 points)

Your virtual machine's OS is "Microsoft Windows Server 2022 Base". Explore the OS's security features, and then complete the following tasks:

(1) Create an administrator user account with user name *jchen* and a password of your choice (case sensitive). **List the steps** (path or mouse clicks) you took to create the account. (10 points).

(2) **List the steps** you took to log into jchen account. (5 points)

(3) Is there an OS's password minimum complexity requirement? **If yes, list the steps** you took to find the requirements. (5 points).

(4) The file access control in Windows Server 2022 resembles which of the two access control implementations: the ACL or Capability or both, why? Use OS examples. (10 points).

Part 2: Database User Administration (150 points)

You (DBA643) work for Digi_Domain, as a project manager. You lead a team of developers on the company's main accounting application. You have created all the tables for the application in GP#3. Now you are ready to create users accounts and profile. Table 1 shows the database users.

Table 1 Database Users

Users	Job Title	Oracle Acct ID/ Default Password
Joe Smith	Developer	JSmith/ JSmith
Sam Houston	Developer	SHouston/ SHouston
Stephanie Clark	Developer	SClark/ SClark
Bob Johnson	Account Manager	BJohnson/ BJohnson

Account Policies for All Users

A. Create a tablespace called ***MyIA643_TBS*** with a size of 500K, extendable in 300K increment up to maximum of 100M. Use ***'MyIA643_dat'*** as datafile name

B. Make ***MyIA643_TBS*** Default Tablespace and TEMP temporary tablespace (TEMP is a tablespace created by Oracle installation)

C. Account should be unlocked after it was created.

D. Allow 5 failed attempts to login (account should be locked after the 5th failed login attempt)

E. Passwords should become expired after 3 months

F. An old password can be reused. However, the user must wait for 35 days and the password has been changed for four times before the old password can be reused.

G. Allow 3 days grace period for expired password.

Password Complexity Requirement
For all the user accounts, you want to enforce the following password complexity policy:

> A password must be at least 8 characters long, must contain at least one upper case letter, at least one lower case letter, and at least one digit, and does not contain three or more consecutive characters of the user name. **Create an Oracle verify function called *gd_pwd_fun* to enforce this password complexity**.

Resource Limits
For the three developers and one account manager you want create a profile called ***Develop_prof*** with the following resources limits:

A. Unlimited concurrent sessions
B. Unlimited amount of CPU time in a single session
C. Limit to 30 seconds of CPU time per call
D. Allow a single session to last up to 3 hours
E. Memory allocated to a single session should be no more than 15 kilobytes in SGA

Check List:

(1) Test the password verify function in your DBA643 account first. When the function is ready, it must be created in SYS account in IA643 pluggable database for it to take effect. SYS account password is the one you made up when you installed the Oracle 19c. **Never** create any tables or users or profile in SYS account. Use SYS account to create password verify function **ONLY**.

(2) If your scrip file is not in plain text file, **you will lose 10 points**.

(3) By running your script, the database user setup should be done automatically including the password verification function in SYS account. (**18** points off if your script file generates errors and not set up the accounts properly).