061006T4ICT
ICT TECHNICIAN LEVEL 6
IT/OS/ICT/CR/03/6
Control ICT Security Threats
Nov/Dec 2024

TVET CURRICULUM DEVELOPMENT, ASSESSMENT AND CERTIFICATION COUNCIL (TVET CDACC)

PRACTICAL ASSESSMENT

Time: 3 HOURS

INSTRUCTIONS TO CANDIDATE:

1. You are required to perform the following tasks
   i. **TASK 1**: Perform User Account Security
   ii. **TASK 2**: Establish Security Control
   iii. **TASK 3**:Configure and Monitor Real-Time Protection

2. You have been provided with the following resources for the practical tasks:
   i. A Working computer installed with a genuine Windows 10 and Microsoft office 2010 and above.
   ii. Stable internet access.
3. Create a folder named **CDACCEXAM** on the desktop to store all the tasks done.

TASK 1: Perform User Account Security

a) Create a new user account named "CDACC" in your computer.
b) Set the password of the account "CDACC" to be "ICTL6@"

TASK 2: Establish Security Control

a) Create a folder named "Level 6" in the "CDACC" account created above in task1.
b) Open a presentation program and create a document named "Firewall".
c) Save the presentation document in "Level 6" folder.
d) Encrypt the presentation document with the password "ICT@24ND".
e) Save the changes.
f) Open the "firewall" presentation program.
g) Screen captures the prompt that appears.
h) Save the Screen capture in a word document named "SOCKET" in the "Level 6" folder.
i) Hide the word document "SOCKET" in the Level 6" folder.

TASK 3: Configure and Monitor Real-Time Protection

a) Setting Up Real-Time Protection

i. Open window setting
ii. Check the status of window defender.
iii. Enable real- time protection.
iv. Enable block apps and download.
v. Turn on cloud delivered protection.
vi. Turn on periodic scanning of the Microsoft defender.
vii. Install Mozilla Firefox from the internet.
viii. Block the inbound connection of the Mozilla Firefox software installed.
ix. Disable the rule of outbound connection of Mozilla Firefox software installed.

b) Monitoring and Interpreting Threat History

i. Display the protection history.

ii. Review the list of detected threats based on quarantined items.

iii. Perform custom scan on any of the hard disk.

iv. Screen capture the results and save in the “SOCKET” word document in “Level 6” folder created above.