THE NATIONAL COUNCIL FOR TECHNICAL AND VOCATIONAL EDUCATION AND TRAINING

OCCUPATIONAL STANDARDS

OCCUPATION: CYBER SECURITY TECHNICIAN

LEVEL: NTA LEVEL 5

FEBRUARY 2024

TABLE OF CONTENTS

ABBREVIATIONS

CBET	Competency Based Education and Training
NACTVET	National Council for Technical and Vocational Education and Training
NOS	National Occupational Standards
OS	Occupational Standards
SQL	Structured Query Language
TET	Technical Education and Training
TVET	Technical and Vocational Education and Training
VPN	Virtual Private Network
Web	World Wide Web

GLOSSARY OF TERMS

Circumstantial Knowledge:	Detailed knowledge, which allows the decision-making in regard to different circumstances and cross cutting issues.
Competence:	The ability to use knowledge, understanding, practical, and thinking skills to perform effectively to the workplace standards required in employment.
Competency:	A description of the ability one possesses when able to perform a given occupational task effectively and efficiently.
Competency-based Education:	An instructional programme that derives its content from validated tasks and bases assessment on the learner's performance.
Curriculum:	A description or composite of statements about "what is to be learned" by the trainee/student in a particular instructional programme; a product that states the "intended learning outcomes".
Educational/Training Programme:	The complete curriculum and instruction (what and how) that is designed to prepare a person for employment in a job or other particular performance situation.
Occupation:	A specific position requiring the performance of specific tasks – essentially the same tasks are performed by all employees having the same title.
Occupational Area:	This is a broad grouping of related jobs. (Example: food service)
Occupational Competence:	The application of knowledge and skills that consistently meet the standards required by the work context.
Occupational Standards:	Specific requirements of competences people are expected to demonstrate in a particular occupational area, including knowledge and relevant attitudes. They also act as a performance tool of assessment of the prescribed outcomes.
Occupational/Job Analysis:	A process used to identify the tasks that are important to employees in any given occupation**.**
Performance Criteria:	Indicate expected end results or outcomes in the form of evaluative statements.
Skills:	The ability to perform occupational tasks with a high degree of proficiency within a given occupation. Skill is conceived of as a composite of three completely interdependent components: cognitive, affective, and psychomotor.
Standards:	A set of statements, which if proved true under working conditions, means that an individual is meeting an expected level and type of performance.

Task Analysis:	The process of analysing each task to determine the steps, circumstantial knowledge, attitudes, performance standards, tools and materials needed, as well as safety concerns required for the employees performing it.
Task:	A work activity that has a definite beginning and ending, is observable or measurable, and consists of two or more definite steps that leads to a product, service, or decision.
Underpinning Knowledge:	Crucial knowledge that an individual must acquire in order to demonstrate competences that are associated in performing a given task.
Verification Process:	The process of having experts review and confirm the importance of the task (competency) statements identified through occupational analysis. Other questions, such as the degree of task learning difficulty are also frequently asked. This process is also sometimes referred to as validation.

1.0. INTRODUCTION

Technical Education and Training (TET) is one of the most important education sub-sectors in Tanzania, responsible for developing a skilled workforce to support the country's industrialization economic agenda. Tanzania's *Development Vision 2025* intends to raise the country's economy to a middle-income status, with a high level of human development. This requires a skilled workforce that is aligned with the needs of the public and private sectors of the economy. The National Council for Technical and Vocational Education and Training (NACTVET) has begun the job of drafting Occupational Standards (OS) that will eventually be adopted as National Occupational Standards (NOS) for use in the delivery of TET that meets the needs of the labour market and the country's economic agenda.

Occupational Standards (OS) are performance criteria that are matched with labour market demands. Each of them describes the functions, performance standards, and understanding or knowledge underpinning a given occupation. They combine skills, knowledge, and attitudes to describe best practice. They are useful tools for establishing job roles, personnel recruitment, supervision, and appraisal, as well as TET Standards. They are also helpful for benchmarking and harmonizing job qualifications on a national and international level. Standards, in general, provide a solid framework for high-quality TET that is labour market-relevant, current, and consistent in application across all public and private institutions.

However, it must be noted that Occupational Standards are different from Training /Education Standards. Occupational standards are defined in terms of activities performed by a person in a selected occupation (e.g., an electrical engineer designs electrical circuits, performs troubleshooting in electrical circuits, etc.), and are usually defined by Employers following procedures as agreed upon by all the stakeholders. On the other hand, Training and Education Standards are developed from the activities defined in the occupational standards, and they specify learning objectives to ensure that the necessary skills and knowledge are developed by a person to enable him/her to function at an agreed level in an occupation. Training and Education Standards are used to define curricula in training institutions. It is critical, however, to establish a direct link between the occupational standards and the training standards for both of them to respond collaboratively to the demands of the labour market.

For the purpose of TET delivery, Tanzania has adopted the Competence Based Education and Training (CBET) approach. The CBET approach focuses on providing learners with the skills and knowledge required to meet the occupational standards. Occupational standards are thus the starting point for developing competency-based training (CBET) programmes. Therefore, it is quite pertinent for TET institutions to use the relevant occupational standards as a benchmark for formulating their curricula.

Occupational Standards are developed based on a given occupation's current and future demands. As a result, they serve as a means of bridging the gap between the worlds of employment and technical education and training.

The document explains how the occupational standards were developed, as well as the scope, the occupational profile in the form of DACUM charts, and the Occupational Standards.

2.0. OCCUPATIONAL STANDARD DEVELOPMENT PROCESS

The process of developing these Occupational Standards involved both local and international expertise. The process began with an examination of major documents that guide Tanzanian skills development including the *10-year National Skills Development Strategy (2016-2026).* NACTVET labour market reports were also used in the literature review to determine the skills demand in the Tanzanian labour market as a whole.

After the literature review, a team of experts in consultation with practitioners developed draft occupational standards. The draft document was used to develop an occupational profile for each occupation (DACUM Chart), which is attached as an **Appendix** to every Occupational Standard.

The occupational standards were validated during the stakeholders' forum held on 22nd and 23rd February 2024 at Morogoro. The information from the stakeholders' forum provides insight from the workplace, professional bodies, regulatory bodies and sector ministries regarding trends and changes in the profession, including how well graduates are prepared for working in the occupation.

3.0. THE SCOPE AND OVERVIEW OF THE OCCUPATION STANDARDS FOR CYBER SECURITY TECHNICIANS

The standards cover a broad range of duties and tasks that can be performed by a Cyber Security Technician. However, the occupational standards are not meant to replace individual job descriptions. Instead, they are to be used for guidance in defining skill levels and knowledge for the technician in specific settings or positions. The Cyber Security Technician may perform tasks in a number of key areas of the occupational standards, but not necessarily in all areas. For example, in large operations, other individuals may be employed or designated to perform specific tasks.

The Cyber Security Technicians shall install operating systems and applications on computers, use office applications, install and deploy network devices and assist in network security operation and maintenance under the supervision of engineers. Generally, the Cyber Security Technician performs the following responsibilities:

a) Installation and configuration of cyber security device

b) System safety operation

c) Data storage and backup operation

d) Database operation

e) Network safety consciousness

The Occupational Standards have been clustered into NTA qualification levels, i.e. NTA 4, 5 and 6.

4.0. VALIDITY PERIOD

Due to the rapid development of technology, the validity period of occupational standards is 3-5 years. The review will proceed in the same manner as the one before it, with new occupational standards being developed based on current trends of the labour market.

5.0. OCCUPATIONAL STANDARDS

5.1 OCCUPATIONAL STANDARDS FOR CYBER SECURITY TECHNICIAN – NTA LEVEL 5

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	PERFORM INSTALLATION AND CONFIGURATION OF CYBER SECURITY DEVICE	**DUTY NO.**	501
TASK TITLE	PERFORM CONFIGURATION OF CYBER SECURITY DEVICES	**TASK NO.**	5011
PERFORMANCE CRITERIA	The person performing this task must be able to configure cyber security devices as required.		
RANGE STATEMENT	The task can be performed on indoor and outdoor office computers under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Network cable; 3. Terminal software; 4. Safety gear.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Use basic tools such as computers and terminal software; 2. Connect the cable of cyber security devices; 3. Use terminal software to log in to cyber security devices; 4. Configure cyber security devices using graphical interfaces; 4. Configure cyber security devices using command line interfaces; 5. Back up and recover the device configuration files; 6. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Connect the cable of cyber security devices; 1.2 Log in to cyber security devices; 1.3 Configure the cyber security devices; 1.4 Back up and recover the configuration files of cyber security devices. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principles of configuring cyber security devices; 2.2 Working principles of cyber security devices; 2.3 Working principles of configuration files of cyber security devices. **3.0 Theories** The person performing this task must be able to

	explain the following: 3.1 Basic introduction to network and information security; 3.2 Cyber security best practices; 3.3 Cyber security control; 3.4 Basic syntax of command lines of cyber security devices; 3.5 Operation safety knowledge of power supply of cyber security devices. **4.0 Essential Skills** 4.1 Computer skills; 4.2 Communication skills; 4.3 Writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The cyber security devices are configured as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Knowledge of intellectual property and laws and regulations.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	PERFORM INSTALLATION AND CONFIGURATION OF CYBER SECURITY DEVICE	**DUTY NO.**	501
TASK TITLE	CONDUCT ANALYSIS OF NETWORK PROTOCOL	**TASK NO.**	5012
PERFORMANCE CRITERIA	The person performing this task must be able to complete the analysis of network protocol as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Network protocol analysis software; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Use computers, network protocol analysis software, etc.; 2. Download and install network protocol analysis software such as Wireshark; 3. Capture data packets using network analysis protocol; 4. Use protocol analysis software to analyse data traffic; 5. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Use web browser to download network protocol analysis software; 1.2 Install network protocol analysis software in the operating system; 1.3 Analyse the captured packets. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of network protocol analysis; 2.2 Compilation specifications of protocol analysis summary report; 2.3 Working principles of network protocol analysis software; 2.4 Working principles of common network protocols. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Composition and structure of common packet headers.

	4.0 Essential Skills 4.1 Communication skills. 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The network protocol is analysed as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Security protection and confidentiality awareness of private data.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT SAFETY OPERATION OF OPERATING SYSTEM	**DUTY NO.**	502
TASK TITLE	PERFORM SECURITY CONFIGURATION OF WINDOWS/LINUX OPERATING SYSTEM	**TASK NO.**	5021
PERFORMANCE CRITERIA	The person performing this task must be able to complete the security configuration of Windows/Linux operating system as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Windows/Linux operating system; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. View the basic information of the operating system; 2. Download the operating system patches through the operating system website; 3. Modify the operating system account name and add login password; 4. Configure the operating system firewall; 5. Set access rights of key files; 6. Install antivirus software for the operating system; 7. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Install patches of the operating system; 1.2 Set the operating system account number and password; 1.3 Turn on and off the operating system firewall; 1.4 Modify the access rights of specific files; 1.5 Install antivirus software in the operating system. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of security configuration of the operating system. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Usage of operating system patches; 3.2 Operating system account number and password; 3.3 Circumstantial knowledge of operating system firewall;

	3.4 File access rights; 3.5 Circumstantial knowledge of computer virus; 3.6 Use instructions of antivirus software. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The security configuration of Windows/Linux operating system is completed as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Knowledge of intellectual property and laws and regulations.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT SAFETY OPERATION OF OPERATING SYSTEM AND APPLICATION	**DUTY NO.**	502
TASK TITLE	PERFORM SECURITY CONFIGURATION OF WEB APPLICATION SERVICES	**TASK NO.**	5022
PERFORMANCE CRITERIA	The person performing this task must be able to complete the security configuration of Web application services as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Web application servers; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Check the basic information of Web application server; 2. Check the basic information of client Web application; 3. Use account number and password for identity authentication; 4. Encrypt the data accessing the web server by using the Secure Socket Layer service functions; 5. Perform security monitoring and log recording; 6. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Conduct identity authentication and access control; 1.2 Conduct data encryption and secure transmission; 1.3 Export and view the operation log of the Web server. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic working principles of Web application server; 2.2 Principles of authentication and access control; 2.3 Principles of data encryption and secure transmission; 2.4 Principles of security monitoring and log recording. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Web application server workflow. 3.2 Web application fundamentals.

	4.0 Essential Skills 4.1 Computer skills; 4.2 Communication skills; 4.3 Writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The security configuration of Web application services is completed according to the requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Security protection and confidentiality awareness of private data.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT SAFETY OPERATION OF OPERATING SYSTEM AND APPLICATION	**DUTY NO.**	502
TASK TITLE	PERFORM SECURITY CONFIGURATION OF VPN SERVICES	**TASK NO.**	5023
PERFORMANCE CRITERIA	The person performing this task must be able to complete the security configuration of VPN services as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. VPN servers; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. View the basic information of VPN services; 2. Configure common VPN services; 3. Ensure the security of VPN user accounts; 4. Ensure the security of VPN transmission data; 5. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Configure the SSL VPN services; 1.2 Configure the IPSec VPN services; 1.3 Use VPN client software to connect to VPN services. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic working principles of VPN services; 2.2 Basic working principles of SSL VPN; 2.3 Basic working principles of IPSec VPN; 2.4 Basic principles of VPN technologies. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Tunnel technologies of VPN; 3.2 Common tunnel protocols of VPN; 3.3 Application scenarios of VPN technologies; **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT /	The security configuration of VPN services is

SERVICE	completed as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Knowledge of intellectual property and laws and regulations.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT SAFETY OPERATION OF OPERATING SYSTEM AND APPLICATION	**DUTY NO.**	502
TASK TITLE	PERFORM SECURITY EVENT RESPONSE	**TASK NO.**	5024
PERFORMANCE CRITERIA	The person performing this task must be able to complete the security event response as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Safety gear.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Make a network security event response plan; 2. Evaluate network security risks; 3. Take pre-and post-event response measures to security events; 4. Conduct disaster recovery of data; 5. Detect and eliminate computer viruses; 6. Protect data; 7. Collect electronic evidence; 8. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Analyse the causes of network security events; 1.2 Prepare a summary report on network security events; 1.3 Detect and prevent viruses; 1.4 Back up and recover data. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of security event response; 2.2 Basic principles of common network attacks. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Basic concepts of security event response; 3.2 Common ways of network attack; 3.3 Basic methods of security event response. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The network security risk assessment and security event response plan are prepared as

	required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Knowledge of intellectual property and laws and regulations; 2. Data security protection and confidentiality awareness; 3. Safety operation specifications of equipment.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT DATA STORAGE AND BACKUP OPERATION	**DUTY NO.**	503
TASK TITLE	PERFORM BACKUP AND RECOVERY OF WINDOWS/LINUX OPERATING SYSTEM DATA	**TASK NO.**	5031
PERFORMANCE CRITERIA	The person performing this task must be able to back up and recover the Windows/Linux operating system data as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Data backup and recovery software; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Use data backup software to back up data of the operating system; 2. Use data recovery software to recover data of the operating system; 3. Use the operating system backup and recovery functions to back up and recover data; 4. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1. Back up the operating system data; 2. Recover the operating system data. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of data storage; 2.2 Basic principles of data recovery; 2.3 Working principles of computer hardware; 2.4 Principles of storing operating system data. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Using instructions of data backup software; 3.2 Using instructions of data recovery software; **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The data of Windows/Linux operating system is backed up and recovered as required.

CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Data security protection and confidentiality awareness.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT DATA STORAGE AND BACKUP OPERATION	**DUTY NO.**	503
TASK TITLE	PERFORM BACKUP AND RECOVERY OF APPLICATION SYSTEM DATA	**TASK NO.**	5032
PERFORMANCE CRITERIA	The person performing this task must be able to complete the backup and recovery of application system data as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Data backup and recovery software; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Identify common data of application system; 2. Back up the data of the application system; 3. Recover the data of the application system from the backups; 4. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Use tool software to back up application system data; 1.2 Use tool software to recover application system data; **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of backup and recovery of application system data; 2.2 Working principles of common application systems. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Methods of backup and recovery. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The application system data is backed up and recovered as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT DATA STORAGE AND BACKUP OPERATION	**DUTY NO.**	503
TASK TITLE	PERFORM INFORMATION SECURITY AUDIT	**TASK NO.**	5033
PERFORMANCE CRITERIA	The person performing this task must be able to complete the information security audit as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Operating system applications; 3. Specialized forensic tools; 4. Safety gear		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Conduct security audit on data content; 2. Report harmful information; 3. Implement log audit measures; 4. Prepare information security audit report; 5. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Obtain system operation logs; 1.2 Use text detection tools to identify sensitive information; 1.3 Block and report sensitive information. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Working principles of text recognition. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Basic methods of information security audit; 3.2 Workflow of information security audit. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The information security audit report is prepared and submitted as required.

CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Sensitive data protection and confidentiality awareness.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CARRY OUT DATA STORAGE AND BACKUP OPERATION	**DUTY NO.**	503
TASK TITLE	PERFORM SECURITY PROTECTION OF SENSITIVE DATA	**TASK NO.**	5034
PERFORMANCE CRITERIA	The person performing this task must complete sensitive data security protection as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Data security protection software; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Identify sensitive data; 2. Encrypt and decrypt sensitive data by AES cryptography algorithm; 3. Encrypt and decrypt sensitive data by AES cryptography algorithm; 4. Verify the integrity of sensitive data by MD5 algorithm; 5. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Encrypt sensitive data; 1.2 Decrypt sensitive data. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of data encryption and decryption; 2.2 Working principles of common encryption algorithms. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Common sensitive data. **4.0 Essential Skills** 4.1 Computer skills; 4.2 Communication skills; 4.3 Writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The sensitive data security protection is completed as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of computers.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CONDUCT DATABASE OPERATION	**DUTY NO.**	504
TASK TITLE	CARRY OUT DATABASE INSTALLATION	**TASK NO.**	5041
PERFORMANCE CRITERIA	The person performing this task must be able to install the database as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Installation packages of database software; 3. Safety gear.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Download the installation package of database software from the database software website through the web browser; 2. Install common mainstream databases; 3. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Download installation packages of database software; 1.2 Install common databases in the operating system. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of database. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Common mainstream databases; 3.2 Applications of database software. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The database is installed as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Knowledge of intellectual property and laws and regulations.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CONDUCT DATABASE OPERATION	**DUTY NO.**	504
TASK TITLE	PERFORM BASIC USE OF DATABASE	**TASK NO.**	5042
PERFORMANCE CRITERIA	The person performing this task must be able to use the database as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Installation package of database management software; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Download installation packages of database management software; 2. Install the database management software; 3. Use database management software to connect to the database; 4. Add, delete, query and update the data in the database; 5. Back up and recover the data in the database 6. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Download and install the installation package of the database management software through the browser; 1.2 Write SQL statements to add, delete, query and update the data in the database. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of SQL statements. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Basic syntax of SQL statements; 3.2 Mainstream maintenance methods for database. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The database is used as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Security protection and confidentiality awareness of data.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CONDUCT NETWORK SAFETY CONSCIOUSNESS	**DUTY NO.**	505
TASK TITLE	CARRY OUT IDENTIFICATION OF CYBERCRIME	**TASK NO.**	5051
PERFORMANCE CRITERIA	The person performing this task must be able to identify cybercrime as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Network; 3. Specialized cyber forensic tools; 4. Storage devices; 5. Safety gear.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Identify the situation of cybercrime; 2. Use operating system application to collect and preserve cybercrime evidence; 3. Use specialized forensic tools to collect and preserve cybercrime evidence; 4. Analyse cybercrime evidence; 5. Compile cybercrime case analysis report and presentation to institution management; 6. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Use the provisions on cybercrime in cyber security laws and regulations; 1.2 Record the situation of cybercrime; 1.3 Collect and preserve cybercrime evidence; 1.4 Prepare cybercrime analysis report and presentation. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Common network security laws and regulations; 2.2 General principles for electronic evidence. . **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Types of cybercrimes; 3.2 Composition of cybercrime; 3.3 Understanding electronic evidence; **4.0 Essential Skills** 4.1 Communication skills;

	4.2 Writing skills; 4.3 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The cybercrimes are identified and case analysis reports are written as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Safety operation specifications of equipment; 2. Knowledge of laws and regulations.

OCCUPATION	CYBER SECURITY TECHNICIAN	**OCCUPATION CODE**	
DUTY TITLE	CONDUCT NETWORK SAFETY CONSCIOUSNESS	**DUTY NO.**	505
TASK TITLE	CARRY OUT CYBERCRIME AWARENESS	**TASK NO.**	5052
PERFORMANCE CRITERIA	The person performing this task must be able to conduct cybercrime awareness as required.		
RANGE STATEMENT	The task can be performed in indoor and outdoor offices under the supervision of senior cyber security technicians. The tools and equipment to be used include: 1. Computers; 2. Network; 3. Safety gear.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Carry out publicity lectures and make posters in communities, schools, enterprises and other occasions to cybercrimes awareness; 2. Conduct cybercrime awareness through television, radio, internet, social media, etc. 3. Observe health, occupational and environmental safety rules and regulations.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Publicize network security awareness; 1.2 Publicize anti-telecommunication fraud for citizens. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Basic principles of anti-telecommunication fraud. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Common modus operandi of telecommunication fraud, such as pretending to be a public security organ officer, pretending to be an acquaintance, refunding online shopping, and reissuing mobile phone cards. **4.0 Essential Skills** 4.1 Computer skills; 4.2 Communication skills; 4.3 Writing skills; 4.4 Teamwork skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	The anti-telecommunication fraud publicity is completed as required.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Knowledge of laws and regulations.

APPENDIX: DACUM CHARTS FOR CYBER SECURITY TECHNICIAN - NTA LEVEL 5

DUTIES	TASKS	ENABLERS
1.0 Perform installation and configuration of cyber security device	1.1 Perform configuration of cyber security devices. 1.2 Conduct analysis of network protocol.	**General skills and knowledge** · Cooperating with others using communication skills and reporting to the superiors · Using safety operation manual of computers · Using operating systems and applications · Skills for writing documents **Tools and equipment** · Computers · Internet · U disks · Cyber security devices · Tool software **Materials** · Operation manual of network device conforming to technical requirements **Requirements for employees** · Ability of autonomic learning · Teamwork spirit · Integrity · Time management · Emphasis on commitment · Network safety consciousness · Awareness of obeying laws and regulations
2.0 Carry out safety operation of operating system	2.1 Perform security configuration of windows/Linux operating system. 2.2 Perform security configuration of web application services. 2.3 Perform security configuration of VPN services.	**General skills and knowledge** · Cooperating with others using communication skills and reporting to the superiors · Using safety operation manual of computers · Basic knowledge of operating systems · Basic knowledge of Web application services

DUTIES	TASKS	ENABLERS
	2.4 Perform security event response.	· Basic knowledge of VPN services · Basic knowledge of security events · Skills for writing documents **Tools and equipment** · Computers · Common operating systems · VPN services **Materials** · Safety operation manual of operating system conforming to technical requirements **Requirements for employees** · Ability of autonomic learning · Teamwork spirit, integrity, time management and commitment · Network safety consciousness · Awareness of obeying laws and regulations
3.0 Carry out data storage and backup operation	3.1 Perform data backup and recovery of Windows/Linux operating system. 3.2 Perform backup and recovery of application system data. 3.3 Perform information security audit. 3.4 Perform security protection of sensitive data.	**General skills and knowledge** · Cooperating with others using communication skills and reporting to the superiors · Using safety operation manual of computers · Basic knowledge of computer hard disk · Basic knowledge of data storage · Basic knowledge of application system · Basic knowledge of information security audit · Basic knowledge of data security **Tools and equipment** · Data recovery, encryption and decryption software commonly used in computers **Materials**

DUTIES	TASKS	ENABLERS
		· Operational manual for data storage and backup conforming to technical requirements **Requirements for employees** · Ability of autonomic learning · Teamwork spirit, integrity, time management and commitment · Network safety consciousness · Awareness of obeying laws and regulations
4.0 Conduct database operation	4.1 Carry out database installation. 4.2 Perform basic use of database.	**General skills and knowledge** · Cooperating with others using communication skills and reporting to the superiors · Using safety operation manual of computers · Basic knowledge of database · Basic knowledge of data operation **Tools and equipment** · Computers, commonly-used database and database management software, etc. **Materials** · Operation manuals for database conforming to technical requirements **Requirements for employees** · Ability of autonomic learning · Teamwork spirit, integrity, time management and commitment · Network safety consciousness · Awareness of obeying laws and regulations
5.0 Conduct network safety consciousness	5.1 Carry out identification of cybercrime.	**General skills and knowledge**

DUTIES	TASKS	ENABLERS
	5.2 Carry out telecommunication fraud publicity.	· Good communication skills · Legal awareness · Ability to accurately reflect problems · Good ability to read and comprehend **Tools and equipment** · Computers, the Internet, etc **Materials** · Legal documents such as network security laws and regulations, and typical cases of cybercrimes **Requirements for employees** · Ability of autonomic learning · Teamwork spirit, integrity, time management and commitment · Network safety consciousness · Awareness of obeying laws and regulations