NATIONAL COUNCIL FOR TECHNICAL AND VOCATIONAL EDUCATION AND TRAINING

JANUARY 2023

PROPOSED OCCUPATIONAL STANDARDS

OCCUPATION: CYBER SECURITY ENGINEER

LEVEL: NTA 7

TABLE OF CONTENT

CONTENTS

ABBREVIATIONS ii

GLOSSARY OF TERMS iii

1.0. INTRODUCTION 1

2.0. OCCUPATIONAL STANDARD DEVELOPMENT PROCESS 2

3.0. THE SCOPE AND OVERVIEW OF THE OCCUPATION STANDARDS FOR CYBER SECURITY ENGINEERS 2

4.0. VALIDITY PERIOD 4

5.0. OCCUPATIONAL STANDARDS 4

5.1 OCCUPATIONAL STANDARDS FOR CYBER SECURITY ENGINEER – NTA 7 5

TABLE 1: DACUM CHARTS FOR CYBER SECURITY ENGINEER - NTA 7 33

ABBREVIATIONS

CBET	Competency Based Education and Training
DTP	Data Transformation Protocol
GPA	Gatekeeper for Physical Access
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
NACTVET	National Council for Technical and Vocational Education and Training
NOS	National Occupational Standards
OS	Occupational Standards
TET	Technical Education and Training
TVET	Technical and Vocational Education and Training

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. (Example: baker)

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. 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 Education has begun the job of drafting Occupational Standards that will eventually be adopted as National Occupational Standards for TET in order to ensure that it meets the needs of the labour market and the country's economic agenda.

National Occupational Standards (NOS) are performance criteria that are matched with labour market demands. Each National Occupation Standard describes functions, performance standards, and knowledge/understanding for one important function or task. They combine skills, knowledge, and attitudes to describe best practice. They are useful tools for establishing job roles, personnel recruiting, supervision, and appraisal, as well as TET standards. They're also helpful for benchmarking and harmonizing 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 delivery across all public and private institutions.

However, it must be noted that, Occupational Standards and Training standards/qualifications standards are different. 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 they are usually defined by employers following procedures agreed upon by all stakeholders. Education and training standards are developed from the activities defined in occupational standards, and they include learning objectives to ensure that the necessary skills and knowledge are developed by a person to enable him or her to function at an agreed level in an occupation. Education and Training standards are used to define curricula in training institutions. It is however critical that there must be a direct link between the occupational standards and the training standards to respond to the demands of the labour market.

In TET delivery, Tanzania 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. TET institutions will be required to benchmark their curricula with relevant occupational standards.

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 (TET).

The Cyber Security Engineer Occupation has its own set of occupational standards. 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 Occupational standard development process began with an examination of major documents that guide Tanzanian skill development. The *10-year National Skills Development Strategy (2016-2026)* was one of the documents reviewed, and it outlined six (6) economic sectors that should be prioritized when developing skills development programmes.

These sectors include: Transport and Logistics, Tourism and Hospitality, Agribusiness, Construction, Energy and ICT. NACTE 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 workshop comprised of expert workers and educators with substantial knowledge and experience in the occupation conducted an occupational analysis utilizing the DACUM approach to produce the occupational profile. The analysis resulted in DACUM Charts, which are attached as **Appendix 1** to this document.

The occupational standards were then developed. Experts in Occupational Analysis and the Development of Occupational Standards facilitated the workshop. Interviews, online surveys, and a stakeholder forum were used to validate the Occupational Standards. Engineers, supervisory technicians on the job, and experienced Cyber Security Engineers were key informants in the survey to discover occupational trends. This information was used to gain insight from the workplaces regarding trends and changes in the profession, including how well graduates are prepared for working in the occupation. A total of ... online surveys were completed by experts from the labour market across the country. Apart from the surveys aiding in defining the scope for the occupational analysis, they also served to engage a wide cross-section of experts in the occupation. Apart from this, the stakeholders' forum was attended by ... participants from different parts of the country representing various companies.

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

The standards cover a broad range of duties and tasks that can be performed by a Cyber Security Engineer. 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 Engineer 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 Engineer shall assist enterprise in designing cyber security plan, cyber security protection management, and system penetration test. Due to the increasing severity of network attacks, the Cyber Security Engineer needs to discover traces of attack intrusions, provide emergency response to attacks, block attacks, and further analyse and track traces of intrusions. Generally, the Cyber Security Engineer performs the following responsibilities:

a) Protection strategy planning

b) Protection strategy implementation and management

c) Operation manual development

d) Cyber security vulnerability detection and analysis

e) System penetration test and verification

f) System security risk analysis

g) Cyber security emergency tracking and monitoring

h) Cyber security emergency assessment and analysis

i) Cyber security emergency response

j) Cyber security emergency electronic evidence collection

k) Training implementation

l) Technical guidance

m) Interpretation of common cyber security laws and regulations

n) Interpretation of intellectual property laws and regulations

o) Cyber security protection management

p) Cyber security test

q) Cyber security emergency handling

r) Cyber security training and guidance

s) Interpretation of cyber security-related intellectual property

t) Cyber security research

u) Cyber security planning

v) Project management

w) Cyber security risk assessment

x) Case study on cyber security laws and regulations

The Occupational standards have been clustered into NTA qualification levels i.e. NTA level 7 and 8.

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 ENGINEER – NTA 7

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PROTECTION MANAGEMENT	**DUTY NO.**	701
TASK TITLE	PROTECTION STRATEGY PLANNING	**TASK NO.**	7011

PERFORMANCE CRITERIA	The person performing this task must be able to plan and develop the security protection strategies for the target system in accordance with its security needs.
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computers; 2. Vulnerability scanners; 3. System configuration testing tools; 4. Log analysis tools; 5. Operation manual of security protection products.

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Analyse the current state of security protection of the target system; 2. Define the security protection needs of the target system; 3. Develop security protection strategies for the target system; 4. Clean the facilities, equipment and workplaces; 5. Arrange and store the tools and equipment.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Design security protection strategies. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principles of information system security management; 2.2 Principles of security protection system design; **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Requirements for designing the contents of the security protection system; 3.2 Requirements for classification and grading of information assets; 3.3 Requirements for the design of security protection strategies. **4.0 Essential Skills** 4.1 Communication skills;

	4.2 Customer service skills;
	4.3 Teamwork skills;
	4.4 Report writing skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	The security protection strategies of the target system are developed in accordance with operation specifications and requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PROTECTION MANAGEMENT	**DUTY NO.**	701
TASK TITLE	PROTECTION STRATEGY IMPLEMENTATION AND MANAGEMENT	**TASK NO.**	7012

PERFORMANCE CRITERIA	The person performing this task must be able to securely configure and manage network equipment, security equipment, operating systems, and application systems, and properly implement the security protection strategies in accordance with the developed system security protection strategies.
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computers; 2. Vulnerability scanners; 3. System configuration testing tools; 4. Log analysis tools; 5. Operation manual of security protection products.

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Save and make a backup of the existing system configuration; 2. Configure security protection policies; 3. Test the effect of security protection strategies; 4. Clean the facilities, equipment and workplaces; 5. Arrange and store the tools and equipment.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Configure security protection policies; 1.2 Test the effect of security protection strategies. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principles of hierarchical and area-based protection **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Application requirements for authentication; 3.2 Application requirements for access and control; 3.3 Application requirements for data encryption; 3.4 Application requirements for intrusion prevention; 3.5 Application requirements for disaster recovery. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills;

	4.3 Teamwork skills; 4.4 Report writing skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The security protection strategies of the target system are configured in accordance with operation specifications and requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

<table>
<tr><td><b>OCCUPATION</b></td><td colspan="2">CYBER SECURITY ENGINEER</td><td><b>OCCUPATION CODE</b></td><td></td></tr>
<tr><td><b>DUTY TITLE</b></td><td colspan="2">CYBER SECURITY TEST</td><td><b>DUTY NO.</b></td><td>702</td></tr>
<tr><td><b>TASK TITLE</b></td><td colspan="2">OPERATION MANUAL DEVELOPMENT</td><td><b>TASK NO.</b></td><td>7021</td></tr>
<tr><td><b>PERFORMANCE CRITERIA</b></td><td colspan="4">The person performing this task must be able to independently develop the operation manual required to accomplish the work in accordance with the working contents of cyber security testing, so that the other technicians of the team can operate in accordance with the manual.</td></tr>
<tr><td><b>RANGE STATEMENT</b></td><td colspan="4">The task can be performed at the information system site under the supervision of senior cyber security engineers.
The tools and equipment to be used include:
1. Computer;
2. Documentation software;
3. Office collaboration and management software.</td></tr>
<tr><td colspan="5"><b>EVIDENCE REQUIREMENT</b></td></tr>
<tr><td colspan="2"><b>PRACTICAL PERFORMANCE</b></td><td colspan="3"><b>UNDERPINNING KNOWLEDGE</b></td></tr>
<tr><td colspan="2">The person performing this task must be able to do the following:
1. Develop emergency response plans for unforeseen situations that will occur during test;
2. Develop effective programmes to address vulnerabilities;
3. Understand the technical architecture of the target asset and develop corresponding testing programmes;
4. Develop efficient group work distribution strategies;
5. Be familiar with various types of vulnerabilities, and examine the hazards of vulnerabilities.
6. Be aware of the latest security happenings and adjust the strategy accordingly;
7. Prepare penetration test report.</td><td colspan="3"><b>Detailed knowledge about:</b>
<b>1.0 Methods</b>
The person performing this task must be able to explain how to:
1.1 Carry out cyber security testing in strict accordance with the steps of information gathering, fingerprinting, vulnerability scanning, manual verification, obtaining permissions, and verifying vulnerabilities;
1.2 Control the risks during the test, and make it clear that it is prohibited to change the configuration of the customer system, delete and modify existing data, or affect the normal operation of the business system after obtaining the authority during the test;
1.3 Conduct the project kick-off meeting for discussion and efficient group work distribution, and define the roles of project manager, technical leader, engineers, etc.

<b>2.0 Principles</b>
The person performing this task must be able to explain the following principles:
2.1 Precautions during test;
2.2 Principles of vulnerability hazard assessment;
2.3 Principles of selecting test tools;
2.4 Principles of testing methods such as information collection, fingerprinting, vulnerability scanning, manual verification, and obtaining permissions;</td></tr>
</table>

	2.5 Specifications of penetration testing process. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Requirements of operating system reinforcement; 3.2 Requirements of middleware reinforcement; 3.3 Requirements of network equipment reinforcement; 3.4 Principles of common vulnerabilities and requirements of defense; 3.5 Requirements of cyber security emergency response. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Report writing skills; 4.3 Customer service skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	A standardized operation manual is prepared to guide engineers in charge of various parts in accordance with operation specifications and requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY TEST	**DUTY NO.**	702
TASK TITLE	CYBER SECURITY VULNERABILITY DETECTION AND ANALYSIS	**TASK NO.**	7022

PERFORMANCE CRITERIA	The person performing this task must be able to independently detect and analyse security vulnerabilities in target assets and prepare vulnerability detection and analysis reports.
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Documentation software; 3. Penetration test operating system; 4. Information collection tools; 5. Fingerprinting tools; 6. Vulnerability scanner; 7. Programming tools.

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Collect assets; 2. Perform fingerprint identification; 3. Control test risks; 4. Scan vulnerabilities; 5. Perform vulnerability replication; 6. Write scripts; 7. Develop effective programmes of security reinforcement.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Perform manual and automated asset collection using asset collection tools; 1.2 Determine the fingerprint status of the target assets based on fingerprinting tools and manual judgement; 1.3 Avoid risks occurred in test by the reasonable arrangement of peak and flat periods of the target industries and assets; 1.4 Use the vulnerability scanner to perform routine vulnerability scanning of the target system; 1.5 Perform manual test and verification of vulnerabilities; 1.6 Write scripts for vulnerabilities that match the current scenario for automated utilization; 1.7 Develop and improve security reinforcement programmes. **2.0 Principles** The person performing this task must be able to explain the following principles:

	2.1 Methods of testing work; 2.2 Principles of vulnerability hazard assessment; 2.3 Causes of vulnerabilities; 2.4 Principles of testing methods such as information collection, fingerprinting, vulnerability scanning, manual verification, obtaining permissions, and verifying vulnerabilities; 2.5 Principles of vulnerability reinforcement for weak passwords, middleware vulnerabilities, operating system vulnerabilities, etc. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Technical requirements of asset collection; 3.2 Technical requirements of fingerprint identification; 3.3 Technical requirements of vulnerability scanning; 3.4 Technical requirements of vulnerability exploitation; 3.5 Requirements of common security testing tools; 3.6 Requirements of vulnerability exploitation scripting; 3.7 Technical requirements of security reinforcement. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Report writing skills; 4.3 Customer service skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The schedule of cyber security vulnerability detection and analysis is developed to avoid risks, and the vulnerability detection and analysis report is prepared through asset collection, fingerprinting, vulnerability scanning, vulnerability exploitation, scripting, and security reinforcement programme development in accordance with customer needs, industry status, and the specific business system.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY TEST	**DUTY NO.**	702
TASK TITLE	SYSTEM PENETRATION TEST AND VERIFICATION	**TASK NO.**	7023
PERFORMANCE CRITERIA	The person performing this task must be able to perform vulnerability verification, replication, and exploitation in accordance with system penetration test reports, so as to validate the reasonability of the security reinforcement programme for the target system.		
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Documentation software; 3. Penetration test operating system; 4. Information collection tools; 5. Fingerprinting tools; 6. Vulnerability scanner; 7. Programming tools.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Control test risks; 2. Scan vulnerabilities; 3. Perform vulnerability replication; 4. Write exploitable scripts; 5. Develop effective programmes of security reinforcement.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Avoid risks occurred in test by the reasonable arrangement of peak and flat periods of the target industries and assets; 1.2 Use the vulnerability scanner to perform targeted and routine scans on reported problems to test the effect of the security reinforcement programme; 1.3 Analyse and replicate the vulnerabilities in reports and test whether the security reinforcement programme can be bypassed; 1.4 Write automated vulnerability exploitation scripts and test the effect of security reinforcement programme; 1.5 Develop the most concise and effective security reinforcement programme and give feedback to the client. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principles of verification; 2.2 Principles of vulnerability hazard assessment;

	2.3 Causes of vulnerabilities; 2.4 Principles of testing methods such as information collection, fingerprinting, vulnerability scanning, manual verification, obtaining permissions, and verifying vulnerabilities; 2.5 Principles of vulnerability reinforcement for weak passwords, middleware vulnerabilities, operating system vulnerabilities, etc. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Technical requirements of vulnerability scanning; 3.2 Technical requirements of vulnerability exploitation; 3.3 Requirements of common security testing tools; 3.4 Requirements of vulnerability exploitation scripting; 3.5 Technical requirements of security reinforcement. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Report writing skills; 4.3 Customer service skills; 4.4 Teamwork skills; 4.5 Computer application skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Vulnerabilities of the relevant system are replicated by vulnerability scanning, manual review, script verification, and other methods in accordance with the system penetration test report, so as to verify the effect of security reinforcement programme, or propose an effective security reinforcement programme if the vulnerabilities cannot be fixed.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY TEST	**DUTY NO.**	702
TASK TITLE	SYSTEM SECURITY RISK ANALYSIS	**TASK NO.**	7024
PERFORMANCE CRITERIA	The person performing this task must be able to perform the server security baseline verification, identify existing security risks, and propose reasonable modification plans in accordance with the status of target asset.		
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computers; 2. Documentation software; 3. Penetration test operating systems; 4. Baseline verification tools; 5. Vulnerability scanners; 6. Programming tools.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Verify the security configurations of the server operating system; 2. Verify the security configurations of server middleware; 3. Verify the security configurations of server database; 4. Verify the security configurations of terminal equipment; 5. Verify the security configurations of network equipment; 6. Develop reasonable security reinforcement programmes; 7. Write scripts for batch verification.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Conduct baseline security verification of operating system; 1.2 Conduct baseline security verification of middleware; 1.3 Conduct baseline security verification of database; 1.4 Conduct baseline security verification of network equipment; 1.5 Conduct baseline security verification of terminal equipment; 1.6 Conduct security reinforcement. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principles of system security risk analysis; 2.2 Principles of risk level assessment. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Technical requirements for server security baseline verification;

	3.2 Precautions for each security configuration of the operating system; 3.3 Precautions for each security configuration of the middleware; 3.4 Precautions for each security configuration of the database; 3.5 Precautions for each security configuration of network equipment; 3.6 Precautions for each security configuration of terminal equipment; 3.7 Requirements of writing batch verification scripts. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Report writing skills; 4.3 Customer service skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The baseline configuration verification is conducted in accordance with the actual situation of the customer's business system to detect the cyber security risks of security configurations in customer' business system, which includes servers, operating systems, databases, and middleware such as Web servers, collate the risks and prepare a baseline verification report, and give corresponding recommendations.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY EMERGENCY HANDLING	**DUTY NO.**	703
TASK TITLE	CYBER SECURITY EMERGENCY TRACKING AND MONITORING	**TASK NO.**	7031

PERFORMANCE CRITERIA	The person performing this task must be able to complete daily cyber security testing and tracking according to job requirements.
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Firewalls; 2. Intrusion detection system; 3. Log analysis system; 4. Internet behavior management system.

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Monitor and response to emergency; 2. Conduct daily monitoring and early warning; 3. Record daily emergency work logs.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Install and configure firewalls and intrusion detection systems for security detection; 1.2 Install and configure log subsystems to capture the logs of information system; 1.3 Analyse early warning messages from firewall intrusion detection systems; 1.4 Inspect and analyse the behavior of the Internet behavior management system; 1.5 Record daily inspection logs **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Precautions of developing cyber security daily patrol programme; 2.2 Requirements of routine inspection of cyber security equipment logs. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Working mechanism of the firewall; 3.2 Working mechanism of the intrusion detection system;

	3.3 Configuration requirements of firewall security strategies; 3.4 Configuration requirements of intrusion detection system security strategies; 3.5 Configuration requirements of the log analysis system; 3.6 Methods of Internet behavior management system; 3.7 Methods of log tracking. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Report writing skills; 4.3 Customer service skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Daily monitoring is conducted and monitoring reports are prepared in accordance with operation requirements and specifications.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY EMERGENCY HANDLING	**DUTY NO.**	703
TASK TITLE	CYBER SECURITY EMERGENCY ASSESSMENT AND ANALYSIS	**TASK NO.**	7032
PERFORMANCE CRITERIA	The person performing this task must be able to assess and analyse systems and network data to detect cyber security emergencies.		
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Traffic analysis tools; 2. Log analysis system; 3. Threat intelligence analysis system.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Analyse anomalies of operating system processes, services, loaded modules, startup items, and accounts; 2. Analyse the logs of IPS, IDS, WAF, security gateways, behavior management equipment, and network equipment to detect anomalies; 3. Analyse anomalies of network traffic; 4. Analyse security emergencies using threat intelligence systems.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Analyse and discover abnormal information in various equipment in the network; 1.2 Analyse and detect anomalies in network traffic. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Precautions of developing cyber security daily patrol programme; 2.2 Requirements of routine inspection of cyber security equipment logs. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 The structure of network traffic; 3.3 Features of various network events; 3.4 Methods of log assessment; 3.5 Methods of traffic assessment; 3.6 Methods of using threat intelligence system. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Report writing skills; 4.3 Customer service skills;

	4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Security analysis reports and cyber security emergency logs are prepared in accordance with operation requirements and specifications.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY EMERGENCY HANDLING	**DUTY NO.**	703
TASK TITLE	CYBER SECURITY EMERGENCY RESPONSE	**TASK NO.**	7033
PERFORMANCE CRITERIA	The person performing this task must be able to response to various cyber security emergencies in accordance with technical requirements.		
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Firewalls; 2. Anti-virus software; 3. Trojan virus killing tools; 4. Data recovery tools.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Dispose of harmful programmes; 2. Dispose of network attacks; 3. Dispose of information destruction; 4. Dispose of equipment failures.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Dispose of various cyber security emergencies. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Methods of cyber security emergency management; 2.2 Methods of cyber security emergency rating; 2.3 Methods of cyber security emergency classification. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Rating specifications of cyber security emergencies; 3.2 Classification requirements of cyber security emergencies; 3.3 Operation requirements of virus killing in harmful programmes; 3.4 Methods of disposing of network attacks; 3.5 Methods of data recovery. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Management skills;

	4.3 Report writing skills;
	4.4 Customer service skills;
	4.5 Teamwork skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	Disposal plans or reports are prepared in accordance with operation requirements and specifications.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY EMERGENCY HANDLING	**DUTY NO.**	703
TASK TITLE	CYBER SECURITY EMERGENCY ELECTRONIC EVIDENCE COLLECTION	**TASK NO.**	7034
PERFORMANCE CRITERIA	The person performing this task must be able to collect electronic evidence for various cyber security emergencies in accordance with technical requirements.		
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Tools of extracting and saving evidence; 2. Tools of analysing evidence; 3. Data recovery tools; 4. Decryption tools.		

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Extract and save electronic data; 2. Decrypt data; 3. Recover electronic data; 4. Analyse electronic data.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Make clean boot disks; 1.2 Install various evidence collection tools; 1.3 Conduct site investigation; 1.4 Conduct site evidence collection; 1.5 Analyse the evidence; 1.6 Write analysis reports; 1.7 File the evidence. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Specifications of electronic evidence collection; 2.2 Operation requirements of evidence extracting and saving tools; 2.3 Operation requirements of evidence analysis tools; 2.4 Operation requirements of data recovery tools; 2.5 Operation requirements of decryption tools. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Requirements of encryption algorithms;

	3.2 Structure of disk and memory; 3.3 Structure of operating system; 3.4 Structure of various types of files and data. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Management skills; 4.3 Report writing skills; 4.4 Customer service skills; 4.5 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Evidence saving and analysis reports are prepared in accordance with operation requirements and specifications.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

<table>
<tr><td><b>OCCUPATION</b></td><td>CYBER SECURITY ENGINEER</td><td><b>OCCUPATION CODE</b></td><td></td></tr>
<tr><td><b>DUTY TITLE</b></td><td>CYBER SECURITY TRAINING AND GUIDANCE</td><td><b>DUTY NO.</b></td><td>704</td></tr>
<tr><td><b>TASK TITLE</b></td><td>TRAINING IMPLEMENTATION</td><td><b>TASK NO.</b></td><td>7041</td></tr>
<tr><td><b>PERFORMANCE CRITERIA</b></td><td colspan="3">The person performing this task must be able to conduct cyber security training and guidance in accordance with technical requirements.</td></tr>
<tr><td><b>RANGE STATEMENT</b></td><td colspan="3">The task can be performed in a cyber security practical training site or a cyber security computer room under the supervision of senior cyber security engineers.
The tools and equipment to be used include:
1. Network system and equipment;
2. Cyber security equipment;
3. Computers.</td></tr>
<tr><td colspan="4"><b>EVIDENCE REQUIREMENT</b></td></tr>
<tr><td colspan="2"><b>PRACTICAL PERFORMANCE</b></td><td colspan="2"><b>UNDERPINNING KNOWLEDGE</b></td></tr>
<tr><td colspan="2">The person performing this task must be able to do the following:
1. Conduct demand analysis and programme design of cyber security training and guidance;
2. Determine the objectives of cyber security training and guidance, and organise its implementation;
3. Organise training participants and training work distribution;
4. Develop training contents and training schedules;
5. Select training methods based on the actual situation;
6. Develop training assessment mechanisms and processes based on training objectives;
7. Develop overall training programmes and organise its implementation based on the programmes.</td><td colspan="2"><b>Detailed knowledge about:</b>
<b>1.0 Methods</b>
The person performing this task must be able to explain how to:
1.1 Analyse the demand of cyber security training and guidance;
1.2 Prepare training programmes;
1.3 Organise training teams and implement training programmes;
1.4 Organise training assessment teams to assess training effects.
<b>2.0 Principles</b>
The person performing this task must be able to explain the following principles:
2.1 Methods and processes of developing training programmes;
2.2 Analytical methods of training demands;
2.3 Organization requirements of training participants and training teams;
2.4 Requirements of developing training courses;
2.5 Requirements of coordinating training site, facilities, and equipment;
2.6 Methods of assessing training effects.
<b>3.0 Essential Skills</b>
3.1 Communication skills;
3.2 Customer service skills;
3.3 Teamwork skills;</td></tr>
</table>

	3.4 Report writing skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Cyber security training and guidance is conducted in accordance with technical requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY TRAINING AND GUIDANCE	**DUTY NO.**	704
TASK TITLE	TECHNICAL GUIDANCE	**TASK NO.**	7042

PERFORMANCE CRITERIA	The person performing this task must be able to conduct cyber security technical guidance in accordance with technical requirements.
RANGE STATEMENT	The task can be performed in a cyber security practical training site or a cyber security computer room under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Network system and equipment; 2. Cyber security equipment; 3. Computers.

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Conduct the demand analysis of cyber security technology; 2. Determine the objectives, contents and schedules of cyber security technical training; 3. Develop training assessment mechanisms and processes; 4. Implement the training.	**1.0 Methods** The person performing this task must be able to explain how to: 1.1 Provide technical guidance on cyber security technology. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Requirements of planning cyber security protection strategies; 2.2 Requirements of implementing cyber security protection strategies; 2.3 Requirements of detecting and analysing cyber security vulnerabilities; 2.4 Requirements of system penetration test and verification; 2.5 Requirements of system security risk analysis; 2.6 Requirements of cyber security emergency tracking and monitoring; 2.7 Requirements of cyber security emergency assessment and analysis; 2.8 Requirements of cyber security emergency response; 2.9 Requirements of electronic evidence collection of cyber security emergency. **3.0 Theories** The person performing this task must be able to

	explain the following: 3.1 Fundamentals related to cyber security technology; 3.2 Methods of information collection; 3.3 Technical requirements of security protection equipment. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Teamwork skills; 4.4 Report writing skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Cyber security technical guidance is conducted in accordance with technical requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CASE STUDY ON CYBER SECURITY LAWS AND REGULATIONS	**DUTY NO.**	705
TASK TITLE	CASE STUDY OF THE VIOLATION OF CYBER SECURITY LAWS AND REGULATIONS	**TASK NO.**	7051
PERFORMANCE CRITERIA	The person performing this task must be able to analyse the cases of illegal events, interpret the laws and regulations of cyber security that have been violated, and write case study reports in accordance with international and national cyber security laws and regulations.		
RANGE STATEMENT	The task can be performed in the customer' office under the supervision of senior cyber security engineers. The equipment and tools to be used include: 1. International and national laws and regulations related to cyber security; 2. International and national standard documents related to cyber security; 3. Computer.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Detemine the laws and regulations applicable to the cyber security cases; 2. Analyse violations of cyber security laws and regulations; 3. Determine the evidence violating cyber security laws and regulations; 4. Understand the latest cyber security developments; 5. Determine the extent to which the case violates the law; 6. Prepare reports of cyber security case study.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Analyse cyber security cases; 1.2 Select laws and regulations applicable to cases; 1.3 Conduct an efficient work distribution. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 The quoted provisions comply with the applicable scope and validity period of cyber security laws and regulations; 2.2 The validity of the evidence provided based on cyber security laws and regulations; 2.3 The evidence provided comply with the application scope of cyber security laws and regulations. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Jurisprudential basis for the development of cyber security laws;

	3.2 Requirements of laws and regulations related to cyber security.
	4.0 Essential Skills
	4.1 Communication skills;
	4.2 Management skills;
	4.3 Report writing skills;
	4.4 Customer service skills;
	4.5 Teamwork skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	Violations of cyber security laws and regulations are analysed, legal provisions violated by the behavior are interpreted, evidence of violations of cyber security laws and regulations are collected, the extent of the violation of cyber security laws is determined, and reports of cyber security case studies are prepared in accordance with specifications and requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

<table>
<tr><td><b>OCCUPATION</b></td><td>CYBER SECURITY ENGINEER</td><td><b>OCCUPATION CODE</b></td><td></td></tr>
<tr><td><b>DUTY TITLE</b></td><td>INTERPRETATION OF CYBER SECURITY-RELATED INTELLECTUAL PROPERTY</td><td><b>DUTY NO.</b></td><td>706</td></tr>
<tr><td><b>TASK TITLE</b></td><td>INTERPRETATION OF CASES OF VIOLATION UPON CYBER SECURITY RELATED INTELLECTUAL PROPERTY</td><td><b>TASK NO.</b></td><td>7061</td></tr>
<tr><td><b>PERFORMANCE CRITERIA</b></td><td colspan="3">The person performing this task must be able to work independently on analysing and interpreting cases of cyber security related intellectual property.</td></tr>
<tr><td><b>RANGE STATEMENT</b></td><td colspan="3">The task can be performed in the customer' office under the supervision of senior cyber security engineers.
The equipment and tools to be used include:
1. Intellectual property legislation documents of cyber security;
2. International and national standard documents of cyber security;
3. Computer.</td></tr>
<tr><td colspan="4"><b>EVIDENCE REQUIREMENT</b></td></tr>
<tr><td colspan="2"><b>PRACTICAL PERFORMANCE</b></td><td colspan="2"><b>UNDERPINNING KNOWLEDGE</b></td></tr>
<tr><td colspan="2">The person performing this task must be able to do the following:
1. Determine the duration and scope of protection for intellectual property;
2. Analyse intellectual property infringement and its legal consequences;
3. Write case studies of intellectual property infringements.</td><td colspan="2"><b>Detailed knowledge about:</b>
<b>1.0 Methods</b>
The person performing this task must be able to explain how to:
1.1 Identify the features and scope of protection for various types of intellectual property;
1.2 Select the validity period for specific intellectual property cases.
<b>2.0 Principles</b>
The person performing this task must be able to explain the following principles:
2.1 Compliance of quoted IP clauses with national laws and regulations;
2.2 Validity of evidence provided.
<b>3.0 Theories</b>
The person performing this task must be able to explain the following:
3.1 Jurisprudential basis of patent and copyright protection;
3.2 Guidelines and agreements on intellectual property protection of different countries and regions.
<b>4.0 Essential Skills</b></td></tr>
</table>

	4.1 Communication skills;
	4.2 Report writing skills;
	4.3 Customer service skills;
	4.4 Teamwork skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	Analytical reports on violations of intellectual property, including piracy, counterfeiting, patent infringement, etc., are prepared in accordance with specifications and requirements. Reports contain the legal consequences resulting from violations of intellectual property, which may include compensation for damages, prohibition of infringement, and criminal penalties.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

TABLE 1: DACUM CHARTS FOR CYBER SECURITY ENGINEER - NTA 7

DUTIES	TASKS	ENABLERS
1.0 Cyber security protection management	1.1 Protection strategy planning.	**General skills and knowledge** · Cooperation with others using communication skills and submission of reports to the superiors · Using report writing skills to write documents · Occupational health and safety · Using computer application skills to complete computer related operations · Operation of various security products **Tools and equipment** · Vulnerability scanner · System configuration testing tools · Log analysis tools · Operation manual of security protection products **Materials** · Computer **Requirements for employees** · Teamwork spirit, integrity, time management and commitment
	1.2 Protection strategy implementation and management.	
2.0 Cyber security test	2.1 Operation manual development.	**General skills and knowledge** · Cooperation with others using communication skills and submission of reports to the superiors · Using report writing skills to write documents · Occupational health and safety · Using computer application skills to complete computer related operations **Tools and equipment** · Documentation software; · Office collaboration and management software
	2.2 Cyber security vulnerability detection and analysis.	
	2.3 System penetration test and verification.	
	2.4 System security risk analysis.	

DUTIES	TASKS	ENABLERS
		Materials - Computer **Requirements for employees** - Teamwork spirit, integrity, time management and commitment
3.0 Cyber security emergency handling	3.1 Cyber security emergency tracking and monitoring.	**General skills and knowledge** - Cooperation with others using communication skills and submission of reports to the superiors - Using report writing skills to write documents - Occupational health and safety - Using computer application skills to complete computer related operations **Tools and equipment** - Documentation software - Office collaboration and management software **Materials** - Computer **Requirements for employees** - Teamwork spirit, integrity, time management and commitment
	3.2 Cyber security emergency assessment and analysis.	
	3.3 Cyber security emergency response.	
	3.4 Cyber security emergency electronic evidence collection.	
4.0 Cyber security training and guidance	4.1 Training implementation.	**General skills and knowledge** - Cooperation with others using communication skills and submission of reports to the superiors - Using report writing skills to write documents - Occupational health and safety - Using computer application skills to complete computer related operations **Tools and equipment** - Documentation software - Office collaboration and management software
	4.2 Technical guidance.	

DUTIES	TASKS	ENABLERS
		Materials · Computer **Requirements for employees** · Teamwork spirit, integrity, time management and commitment
5.0 Law and regulation interpretation	5.1 Interpretation of common cyber security laws and regulations. 5.2 Interpretation of intellectual property laws and regulations.	**General skills and knowledge** · Cooperation with others using communication skills and submission of reports to the superiors · Using report writing skills to write documents · Occupational health and safety · Using computer application skills to complete computer related operations **Tools and equipment** · Documentation software · Office collaboration and management software **Materials** · Computer **Requirements for employees** · Teamwork spirit, integrity, time management and commitment