	Unit ID: 2309
Domain	**NETWORKING**
Title:	**Manage network access security**
Level: 5	**Credits: 10**

Purpose

This unit standard is intended for those who manage network access security. People credited with this unit standard are able to describe the basic security principles for information systems, describe the importance of an organisation`s security policy, describe information security over a local area network using Transmission Control Protocol/Internet Protocol (TCP/IP) protocol architecture, demonstrate technical skills and describe network security aspects to secure network access, apply technical skills required to manage security of a computer system connected to a network, apply skills and techniques required for a network security specialist, identify internal and external security gaps/threats and apply security updates/fixes.

This unit standard is intended for those who work in the networking environment

Special Notes

1. Entry information:

   Prerequisite:

   - None

2. Assessment evidence may be collected from a real or a simulated workplace in which networking operations are carried out.

3. Tools and equipment may include but are not limited to computer, external devices, storage devices and other and basic computer applications.

4. Performance of all elements in this unit standard must comply with industry standards.

5. Regulations and legislation relevant to this unit standard include the following:
   - Labour Act 2007(Act No 11, 2007).
   - Regulations relating to the health and safety of employees at work under schedule 1 (2) of the Labour Act No.11 of 2007 and all subsequent amendments.

Quality Assurance Requirements

This unit standard and others within this sub-field may be awarded by institutions which meet the accreditation requirements set by the Namibia Qualifications Authority and the Namibia Training Authority and which comply with the national assessment and moderation requirements. Details of specific accreditation requirements and the national assessment arrangements are available

from the Namibia Qualifications Authority on www.namqa.org and the Namibia Training Authority on www.nta.com.na

Elements and Performance Criteria

Element 1: Describe the basic security principles for information systems

Performance Criteria

1.1 Information confidentiality is described according to system security.

1.2 Information availability is described according to system security.

1.3 Integrity is described according to system security.

1.4 Non-repudiation is described according to system security.

Element 2: Describe the importance of an organisation`s security policy

Performance Criteria

2.1 Organisation`s security policy is identified.

2.2 The organisation`s security policy is analysed.

2.3 Security issues being addressed by an organisation`s security policy are identified.

2.4 Organisation`s security policy purpose is understood and interpreted.

Element 3: Describe information security over a local area network using Transmission Control Protocol/Internet Protocol (TCP/IP) protocol architecture

Performance Criteria

3.1 Information security is described according to physical/network access layer of TCP/IP protocol architecture.

3.2 Information security is described according to network/internet layer of TCP/IP protocol architecture.

3.3 Information security is described according to application layer of TCP/IP protocol architecture.

Element 4: Demonstrate technical skills and describe network security aspects to secure network access

Performance Criteria

4.1 Security protocols are identified and described.

4.2 Authentication protocols are identified and described.

4.3 Purpose and benefits of using a firewall are identified and described.

4.4 Purpose and benefits of using a proxy are identified and described.

4.5 Impact on a network functionality of a security implementation is determined based on a given connectivity scenario.

Element 5: Apply technical skills required to manage security of a computer system connected to a network

Performance Criteria

5.1 Desktop computers are scanned for viruses.

5.2 Viruses found are recorded and removed according to industry's standards, procedures and to an organisation IT security policy.

5.3 Desktop computers are monitored for unauthorised and pirated software.

5.4 Incidences of unauthorised software are recorded.

5.5 Recording of viruses and unauthorised software are reported according to company`s standards and procedures.

Element 6: Apply skills and techniques required for a Network Security Specialist

Performance Criteria

5.1 Network security threats, exposures and violations are identified.

5.2 Network security measures and actions are taken according to an organisation IT policy (provided), procedures and requirements.

5.3 Back-ups of network software/IOS (Internet Operating System) is performed according instructions, procedures and specifications.

5.4 Access to the network is provided according to instructions, procedures and specifications.

Element 7: Identify internal and external security gaps/threats and apply security updates/fixes

Performance Criteria

7.1 Security exposures and violations are identified.

7.2 Security exposures and violations are resolved according to organisation requirements and security policy.

7.3 Security systems are monitored and tuned in line with IT security policy.

7.4 In-built and current security and access features of the systems are reviewed.

7.5 Security configuration changes are applied to the systems according to instructions.

7.6 User awareness program is created.

Registration Data

Subfield:	Information and Communication Technology
Date first registered:	30 July 2020
Date this version registered:	30 July 2020
Anticipated review:	2025
Body responsible for review:	Namibia Training Authority