	UNIT ID: 2325
Domain	**COMPUTER SYSTEM SUPPORT**
Title:	**Apply security and disaster recovery procedures**
Level: 3	**Credits: 7**

Purpose

This unit standard is intended for those who apply security and disaster recovery procedures .People credited with this unit standard are able to perform security assessments, demonstrate understanding of value of security measures, identify security threats, disasters and risks, demonstrate an understanding of risk management and perform data backup and restore.

This unit standard is intended for those who work as computer system supporters.

Special Notes

1. Entry information:

   Prerequisites:

   - None

2. This unit standard is to be delivered and assessed in the context of information and communication technology.

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

4. Glossary of terms
   - *'Security features'* is a specific implementable function in a system which supports some part of the system's security policy.
   - *'Contingency procedures'* an alternative to the normal procedure; triggered if an unusual but anticipated situation arises
   - *'Backup procedures*' a backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required. Though backups popularly represent a simple form of disaster recovery, and should be part of a disaster recovery plan, by themselves, backups should not alone be considered disaster recovery.
   - *'Restore procedures*' is a process that involves copying backup files from secondary storage (tape, zip disk or other backup media) to hard disk.
   - *'Internet Security' i*s a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it

applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet.

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

6. Regulations and legislation relevant to this unit standard include the following:
   - Labour Act 2007(Act No 11, 2007).
   - Regulations relating to the health & 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: Perform security assessments

Performance Criteria

1.1 Security assessments on Operating System (OS) level are performed.

1.2 Security assessments on Network level are performed.

1.3 Security assessments on Application level are performed.

Element 2: Demonstrate understanding of value of security measures

Performance Criteria

2.1 Values of security measures on hardware are identified.

2.2 Values of security measures on software are identified.

2.3 Values of security measures on data are identified.

Element 3: Identify security threats, disasters and risks

Performance Criteria

3.1 Security threats are identified.

3.2 Security disasters are explained.

3.3 Security risks are outlined.

3.4 Security vulnerabilities are outlined.

Element 4: Demonstrate an understanding of risk management

Performance Criteria

4.1 Cost of risks vs cost of mitigation is explained.

4.2 Return on investments on risks is outlined.

4.3 Form of risk insurance is explained.

Element 5: Perform data backup and restore

Range

Back-up features may include but are not limited to Magnetic tape, Hard disk, Optical Storage, Solid state storage, Remote back-up service and Floppy disks.

Performance Criteria

5.1 Types of backups are explained.

5.2 Backups are performed.

5.3 Data restoration is performed.

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