SECTION A:	QUALIFICATION DETAILS			
QUALIFICATION DEVELOPER(S)	Institute of Development Management			
TITLE	Diploma in Cyber Security		**NCQF LEVEL**	6
STRANDS (where applicable)	N/A			
FIELD	Information and Communication Technology	**SUB-FIELD** Information Technology	**CREDIT VALUE**	249

New Qualification		✓	Legacy Qualification	

SUB-FRAMEWORK	General Education		TVET		✓	Higher Education	

QUALIFICATION TYPE	Certificate	I		II	III	IV	V	Diploma	✓	Bachelor	
	Bachelor Honours			Post Graduate Certificate				Post Graduate Diploma			
	Masters							Doctorate/ PhD			

RATIONALE AND PURPOSE OF THE QUALIFICATION

RATIONALE:

HRDC through its market research have identified cyber security and Information Security Analyst as a future job demand and occupational demand as an area of specialization. With the ever-increasing demand and growth of the IT industry in Botswana, it is becoming more and more a realization for the need of good and skilled IT workers. The Government of Botswana has long realized the critical role

of Information and Communication Technology (ICT) in economic development. This was consolidated and articulated in the National Information Technology Policy of 2007, commonly referred to as Maitlamo which presents ICT as a key driver of social, economic, cultural and political transformation.

The Thuto Net strategy under the Ministry of Education and Skills Development aims to use ICT as an enabler to enhance the teaching learning process through E-learning. The Education and Training Sector Strategic Plan (ETSSP 2015-2020) which sets out to improve the performance of the education sector views ICT as a driver of all the key initiatives and hence sets out to utilize and integrate ICT in the education sector. Similarly, all other sectors are repositioning themselves to optimize the use of ICT for enhance their performance and contribute to the envisaged transformed Botswana characterized by sustained economic growth.

Demand for cybersecurity employees is bound to increase as the threat landscape continues to grow in complexity and supply can't always keep up. Indeed, the inability to find qualified talent was cited most frequently as a challenge by organizations with cybersecurity staff shortages. Human Resources Development Council (HRDC) top occupational demand driven by industrial revolution aligned to global and African vision identified Cyber Security as a top priority skill for both current and future need. Cybersecurity has been identified as an area of specialization under HRDC skills need in the industrial automation.

Botswana Vision 2036 acknowledges Cyber Security as a key contributor to economic growth enabling private and public sector employment growth opportunities (World Economic Forum (2018).

PURPOSE: (itemise exit level outcomes)

The purpose of this qualification is to produce graduates with advanced knowledge, skills and competence to:

- Design and create a tight and secure IT infrastructure for business.
- Investigate cybersecurity legal compliance in companies and communities.
- Manage and assess risk to assets and evaluate current cybersecurity protection measures.
- Implement detection, protection and prevention systems and respond to breaches or incidences.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

NCQF Level IV certificate.

2. There will be admission with provisions through CAT and National RPL Policies.

SECTION B	QUALIFICATION SPECIFICATION
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**
LO 1. Demonstrate advanced knowledge and understanding of cyber security and computer networks.	1.1 Protect systems by defining access privileges, control structures, and resources. 1.2 Implement security audits across computer hardware, software programs. 1.3 Discover vulnerabilities and risks in networks and software systems. 1.4 Troubleshoot problems, implement ongoing network monitoring, and provide real-time security solutions to their team. 1.5 Monitoring network data and ensuring hardware and software applications are updated. 1.6 Design and develop a security architecture for an organization. 1.7 Implement different types of encryptions and or cryptographic algorithm. 1.8 Configure security protocols for protecting data on computer networks. 1.9 Develop an asset register.
LO 2. Design, develop, test and evaluate secure software for IT infrastructure.	2.1. Upgrades system by implementing and maintaining security controls.

	2.2. Prepare performance reports; communicate system status to keep users informed.
	2.3. Maintain quality service by adhering to organization standards.
	2.4. Maintain technical knowledge by attending educational workshops, reviewing publications.
	2.5. Create a LAN (Local Area Network) security plan.
	2.6. Apply the security principles and create a LAN and WAN.
	2.7. Create a data classification scheme and use this for managing risks with cloud solutions.
LO 3. Develop policies and procedures to manage IT enterprise computer and network security risks.	3.1 Execute risk management processes, risk treatment methods, and key risk and performance indicators.
	3.2 Prioritize business critical operations for business continuity.
	3.3 Design operational and strategic cyber security strategies and policies.
LO 4. Evaluate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training.	1.1 Perform vulnerability assessments and the weakness of using passwords for authentication.
	1.2 Perform simple vulnerability assessments and password audits.
	1.3 Identify physical points of vulnerability in simple networks.
	1.4 Determine and analyse software vulnerabilities and security solutions to reduce the risk of exploitation

LO 5. Design a secure Virtual Private Network and implement wireless security.	5.1 Design Virtual Private Network security. 5.2 Deploy wireless security. 5.3 Configure encryption, protocols and policies. 5.4 Secure wireless local area networks. 5.5 Configure IPsec to secure network traffic.
LO 6. Identify, assess threats and come up with preventive measures and decide how to avoid, reduce or transfer risks.	6.1 Conduct regular risk assessments either through a team of risk management experts or personally on site. 6.2 Manage and prepare all documentation related to risk assessments and reviews of standard operating procedures. 6.3 Evaluate the gravity of each risk by considering its consequences. 6.4 Develop risk management controls and systems. 6.5 Design processes to eliminate or mitigate potential risks. 6.6 Create contingency plans to manage crises. 6.7 Evaluate existing policies and procedures to find weaknesses
LO 7. Use documents application to accomplish everyday tasks associated with creating, formatting, and finishing to produce accurate work outputs using devices and online skills.	7.1 Create documents and save them in different file formats. 7.2 Demonstrate skills in computer operations. 7.3 Demonstrate skills for online essentials application and use. 7.4 Choose built-in options, such as the Help function, to enhance productivity. 7.5 Create mathematical and logical formulas using standard spreadsheet functions. 7.6 Create and edit small-sized word and excel processing documents that will be ready to share and distribute. 7.7 Apply different formats to documents to enhance them before distribution; recognize good practice in choosing the appropriate formatting options. 7.8 Create tables, images, and draw objects into documents. 7.9 Prepare documents for mail merger operations. 7.7 Adjust document page settings

SECTION C	QUALIFICATION STRUCTURE			
	TITLE	**Credits Per Relevant NCQF Level**		**Total Credits**
COMPONENT		**Level [5]**	**Level [6]**	**Level [7]**	
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Communications and Academic Writing Skills	12			12
	ICDL Computer Essentials	5			5
	ICDL Word Processing	5			5
	ICDL Spreadsheets	5			5
	ICDL Online Essentials	5			5
	Professional Communication		12		12
	Introduction to Entrepreneurship and Innovation		10		10
CORE COMPONENT Subjects/Courses/ Modules/Units	Introduction to Information Systems		10		10
	Computer Network Fundamentals		10		10
	Cybersecurity Principles		10		10
	Cloud Security		10		10
	Database Theory and Practice		10		10

	Information System Security		10		10
	Information Security Management & Governance		10		10
	Network Security and Cryptography		10		10
	Linux Administration		10		10
	Information Technology Service Management		10		10
	Network Security		15		15
	Cybersecurity Data Analysis		15		15
	Secure Web Programming		15		15
	Ethical Hacking and Testing		15		15
	Ethics in IT		15		15
	Computing Project		20		20

STRANDS/ SPECIALIZATION	Subjects/ Courses/ Modules/Units	Credits Per Relevant NCQF Level			Total Credits
		Level [5]	Level [6]	Level [7]	
1.	Communications and Academic Writing Skills	12			12
	ICDL Computer Essentials	5			5
	ICDL Word Processing	5			5
	ICDL Spreadsheets	5			5

	ICDL Online Essentials	**5**			**5**
	Professional Communication		**12**		**12**
	Introduction to Entrepreneurship and Innovation		**10**		**10**
2.	Introduction to Information Systems		**10**		**10**
	Computer Network Fundamentals		**10**		**10**
	Cybersecurity Principles		**10**		**10**
	Cloud Security		**10**		**10**
	Database Theory and Practice		**10**		**10**
	Information System Security		**10**		**10**
	Information Security Management & Governance		**10**		**10**
	Network Security and Cryptography		**10**		**10**
	Linux Administration		**10**		**10**
	Information Technology Service Management		**10**		**10**
	Network Security		**15**		**15**
	Cybersecurity Data Analysis		**15**		**15**

	Secure Web Programming		**15**		**15**
	Ethical Hacking and Testing		**15**		**15**
	Ethics in IT		**15**		**15**
	Computing Project		**20**		**20**

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
5	3 2
6	2 1
TOTAL CREDITS	**249**

Rules of Combination:

(Please Indicate combinations for the different constituent components of the qualification)

- This qualification will have at least **249** credits and take at least two years to complete.

- The credit combination for this qualification is from **54** fundamental components, **195** core components.

The qualifications structure is premised on these rules of combination.

Fundamentals Level 5 = 32 Credits

Fundamentals Level 6 = 22 Credits

Core Level 6 = 195 Credits

There are no elective modules for the qualification

Total = 249 Credits

ASSESSMENT ARRANGEMENTS

This qualification is assessed as follows:

Integrated Assessment:

Both formative and summative assessment processes are monitored during the qualification and to determine competence at the end of the qualification. This is because assessment practices must be open, transparent, fair, valid, reliable, and ensure that no learner is disadvantaged in any way whatsoever, an integrated assessment approach is incorporated into the qualification.

Summative assessment

Summative assessment based on learning out comes leading to the award of the qualification will be done by means of a written examination (of at least 3 hours) at the end of every module (per module) contributing 60% of the overall mark.

Formative assessment- informs teaching and learning

Learners are continuously assessed to evaluates learner learning, knowledge, proficiency which constitutes 40% of the overall module mark:

MODERATION ARRANGEMENTS

The moderation process of assessments focuses on ensuring the assessment is aligned to the module learning objectives and the learning outcomes.

Professional registration and accreditation

Assessors and moderators must have valid registration and accreditation with all or some of the relevant bodies such as:

- Botswana Qualifications Authority (BQA)
- Fortinet Network Security Expert
- Computer Information System Company- CISCO

RECOGNITION OF PRIOR LEARNING

RPL for award of this qualification will be supported by institutional policies in line with national policies on RPL.

CREDIT ACCUMULATION AND TRANSFER

CAT for award of this qualification will be supported by institutional policies in line with national policies on CAT.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Horizontal articulation(related qualifications of similar level that graduates may consider)

Diploma in Network Security

Diploma in Information Systems

Diploma in Computer Networks

Diploma in Computing

Vertical Articulation- Pathways which the holders may progress to;

Bachelor of Science in Network Security

Bachelor of Science in Information Systems

Bachelor of Science in Computer Networks

Bachelor of Science in Computing

Employment Pathways

Cyber-security analyst

Security penetration tester

Security Engineer

Information Assurance Analyst

Cybersecurity Assessor/ Auditor

Cybersecurity related support roles

Application analyst

QUALIFICATION AWARD AND CERTIFICATION

To be awarded the **Diploma in Cyber Security**, a candidate must complete 54 Credits of the Fundamental Component, 195 Credits of the Core component. Those who meet that requirement will be issued a Certificate

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

The comparison was done internationally with the Level 5 Diploma in Cyber Security from NCC Education and University of Potomac (United Kingdom). At the time of comparison, no Diploma in Cyber Security (NQF Level 6) was found regionally, except for NQF Level 4 qualifications in South Africa, which was not used, hence comparison. The main variables were compared and the summary of comparison is presented as follows.

Similarities:

- The qualifications compared have similar titles with this Diploma in Cybersecurity.
- The main exit level outcomes, modules and employment pathways have also been found to be similar.
- The formative and summative assessment weigh 60 – 40%.

- All the international qualifications are worth 120 credits with this qualification has 249 credits in line with the minimum requirements for NCQF Level 6 qualifications.

Differences

- The qualifications are all regulated but the diploma in Cybersecurity in Botswana is not a regulated profession.
- The international qualifications are on the UK RQF Level 5 with is equivalent and similar in terms of level of complexity to this qualification at NCQF Level 6.

Based on comparison of the attributes above, this qualification compares favourably, or is similar to the qualifications compared with.
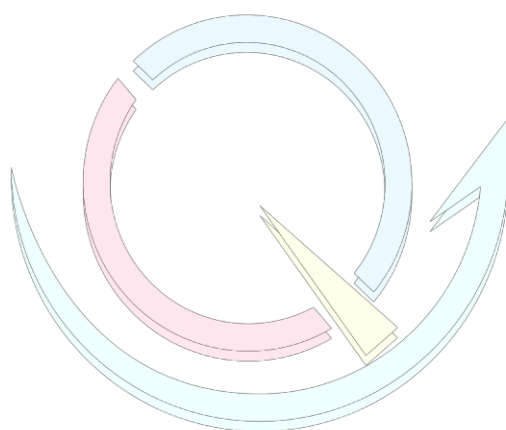
REVIEW PERIOD

Every 5 years. However, the IT landscape is forever changing and review of the qualification will provide a window for constant refining and updating where applicable, arising from legislative changes or stakeholder feedback

For Official Use Only:

CODE (ID)			
REGISTRATION STATUS	BQA DECISION NO.	REGISTRATION START DATE	REGISTRATION END DATE
LAST DATE FOR ENROLMENT		LAST DATE FOR ACHIEVEMENT	

Note: Please use Arial 11 font for completing the template)