BQA NCQF QUALIFICATION TEMPLATE

SECTION A:	QUALIFICATION DETAILS																
QUALIFICATION DEVELOPER (S)	Ed-Tech Africa																
TITLE	Diploma in Cyber Security												**NCQF LEVEL**	6			
STRANDS (where applicable)	N/A																
FIELD	Information and Communication Technology												**CREDIT VALUE**	360			
SUB FIELD	Information Technology																
New Qualification	√	Legacy Qualification										Renewal Qualification					
												Registration Code					
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

This qualification addresses a national shortage of mid-level cybersecurity practitioners who can support security operations, incident response, compliance, and digital infrastructure protection in both public and private sectors. In Botswana, increased government digitalisation has heightened cyber threat exposure, creating strong demand for skilled cybersecurity professionals. Current labour-market data indicate that supply does not meet this demand.

The Human Resource Development Council (HRDC) Priority Skills List (2023–2024) explicitly identifies Cybersecurity, Data Analytics, Data Science, Network Security and Information Security Management as priority and scarce skills within Botswana's economy (HRDC, 2024). These skills are needed in government, banking, telecommunications, logistics, and education, reflecting a skills gap that calls for focused tertiary education.

The HRDC Priority Skills Report (2025) further reinforces the growing demand for professionals with competencies in cybersecurity operations, data protection, analytics and secure digital systems, noting that technological transformation is outpacing current workforce capability (HRDC, 2025).

International evidence reflects a similar trend. The ISC2 Cybersecurity Workforce Study (2023) reports a global shortage of more than 4 million cybersecurity professionals, with the most critical gaps occurring in threat analysis, incident response, forensics, and governance competencies addressed by the developed diploma (ISC2, 2023).

The World Economic Forum Global Cybersecurity Outlook similarly identifies cybersecurity and data-driven security skills as among the fastest-growing global workforce needs, particularly in developing economies where institutional cyber resilience remains limited (WEF, 2023).

To address skills shortages, the developed Diploma in Cyber Security (NCQF Level 6) focuses on practical competencies in cyber defence, secure networks, data protection, digital forensics, penetration testing, and governance. Work-integrated learning and a capstone project ensure alignment with BQA's focus on occupational relevance and employability.

The developed qualification meets national priority skills, aligns with workforce trends, and equips Botswana with a skilled cyber security workforce for the protection information assets and drive sustainable digital growth.

PURPOSE:

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

- Analyse cybersecurity threats and vulnerabilities to determine their impact on organisational ICT infrastructure.
- Synthesise legal, ethical, and governance principles to formulate comprehensive cybersecurity strategies.
- Design secure network architectures, access controls, and intrusion detection systems to protect ICT assets.
- Conduct vulnerability assessments, penetration tests, and digital forensic investigations using industry-standard tools.
- Manage cybersecurity operations and teams, demonstrating autonomy and responsibility for

project outcomes.

- Apply innovative problem-solving techniques to address complex cybersecurity challenges and communicate recommendations to diverse stakeholders.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

(i) At least 5 "O" Level / BGCSE subjects with passes in Maths, English and Computer-related subjects with at least 30 Points.

(ii) Certificate IV (NCQF Level 4) or equivalent qualification in Information Technology or a related discipline.

(iii) Recognition of Prior Learning (RPL) shall be applied in accordance with the institution's approved RPL Policy and NCQF guidelines.

(iv) Credit Transfer shall be granted for equivalent modules completed at BQA-recognised institutions.

(v) All Recognition of Prior Learning (RPL) and decisions shall be implemented in accordance with the institution's approved RPL Policy and aligned to national RPL guidelines and Botswana Qualifications Authority requirements.

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

SECTION B	**QUALIFICATION SPECIFICATION**
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**
1: Analyse cybersecurity threats and vulnerabilities to determine their impact on organisational ICT infrastructure.	1.1 Identify and categorise different types of cybersecurity threats and vulnerabilities. 1.2 Analyse the potential exploitability of identified vulnerabilities. 1.3 Evaluate the potential impact of threats on the confidentiality, integrity, and availability of organisational data and systems. 1.4 Examine threats and vulnerabilities based on their risk level to the organisation.
2: Synthesise legal, ethical, and governance principles to formulate comprehensive cybersecurity strategies.	2.1 Identify relevant national and international laws, regulations, and standards applicable to cybersecurity.

	2.2 Apply ethical principles and professional codes of conduct to cybersecurity planning and decision-making. 2.3 Integrate governance frameworks and risk management principles into a coherent security strategy. 2.4 Formulate a comprehensive cybersecurity strategy that aligns with legal, ethical, and organisational requirements.
3: Design secure network architectures, access controls, and intrusion detection systems to protect ICT assets.	3.1 Develop secure network designs incorporating principles of defence in depth and least privilege. 3.2 Select and specify appropriate access control and identity management mechanisms. 3.3 Design an intrusion detection and prevention system (IDPS) strategy to monitor and protect network perimeters and endpoints. 3.4 Justify design decisions based on technical specifications, security principles, and organisational needs.
4: Conduct vulnerability assessments, penetration tests, and digital forensic investigations using industry-standard tools.	4.1 Plan and scope a vulnerability assessment or penetration test within defined rules of engagement. 4.2 Execute scanning and testing procedures using industry-standard tools in a controlled environment. 4.3 Document and report on identified vulnerabilities and exploitation paths with clear recommendations. 4.4 Apply forensic methodologies to acquire, preserve, and analyse digital evidence while maintaining chain of custody.
5: Manage cybersecurity operations and teams, demonstrating autonomy and	5.1 Plan and organise cybersecurity tasks, projects, and resources to achieve defined

responsibility for project outcomes.	objectives. 5.2 Allocate roles and responsibilities to team members based on their skills and expertise. 5.3 Supervise team performance and provide constructive feedback to support professional development. 5.4 Evaluate project outcomes against initial goals and quality standards, taking ownership of results.
6: Apply innovative problem-solving techniques to address complex cybersecurity challenges and communicate recommendations to diverse stakeholders.	6.1 Identify and analyse complex, non-routine cybersecurity problems in an organisational context. 6.2 Propose and justify innovative and creative solutions to address identified challenges. 6.3 Produce clear, structured, and professional reports and documentation tailored to technical audiences. 6.4 Present complex technical information and strategic recommendations effectively to non-technical stakeholders.

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

SECTION C	**QUALIFICATION STRUCTURE**				
COMPONENT	**TITLE**	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [5]	**Level [6]**	**Level [7]**	
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Digital Literacy and Productivity Tools	**16**			**16**
	Communication and Academic Writing	**12**			**12**

	Mathematics for Cybersecurity	**12**			**12**
	ICT Ethics & Legal Compliance		**12**		**12**
	Professional Practice and Workplace Skills	**20**			**20**
CORE COMPONENT Subjects'/Courses/ Modules/Units	Cybersecurity Foundations	**12**			**12**
	Network Fundamentals & Protocols	**16**			**16**
	Cryptography Essentials		**12**		**12**
	Python for Security Scripting		**12**		**12**
	Secure Database Management		**12**		**12**
	Operating Systems Fundamentals & Security		**12**		**12**
	Advanced Network Security		**16**		**16**
	Threat Intelligence Analysis		**12**		**12**
	Penetration Testing & Ethical Hacking		**16**		**16**
	Access Control and Identity Management		**12**		**12**
	Web Application		**16**		**16**

	Security				
	Applied Cybersecurity Capstone Project		**26**		**26**
	Web and Cloud Data Technologies		**16**		**16**
	Risk Management & Compliance		**12**		**12**
	Intrusion Detection and Prevention Systems		**16**		**16**
	Industry Attachment (Work-Integrated Learning)		**30**		**30**
	Security Policies and Governance		**12**		**12**
	Cyber Forensics and Incident Response		**16**		**16**
STRANDS/ SPECIALIZATION	Subjects/ Courses/ Modules/Units	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [5]	**Level [6]**	**Level [7]**	
Electives	Advanced Malware Analysis			**12**	**12**
	Cloud Security Architecture			**12**	**12**
	Mobile and			**12**	**12**

	Wireless Security				
	AI and Machine Learning for Security			**12**	**12**

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
NCQF Level 5 Modules	72
NCQF Level 6 Modules	276
NCQF Level 7 Modules	12
TOTAL CREDITS	360

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

To be awarded the Diploma in Cyber Security, a learner must successfully complete the prescribed combination of modules in accordance with the National Credit and Qualifications Framework (NCQF) requirements.

The rules of combination for this qualification are as follows:

1. **Fundamental Component**
   - All fundamental modules are compulsory.
   - The fundamental component contributes a total of 72 credits toward the qualification.
2. **Core Component**
   - All core modules are compulsory and must be successfully completed.
   - The core component contributes a total of 276 credits, including the Industry Attachment (Work-Integrated Learning) and the Applied Cybersecurity Capstone Project.
3. **Elective Component**
   - Learners must select one (1) elective module only from the approved elective list.
   - The elective component contributes 12 credits toward the qualification.

The qualification structure and learning pathway are premised on these rules of combination.

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

ASSESSMENT ARRANGEMENTS

Assessment for the Diploma in Cyber Security is conducted as follows:

1. **Formative Assessment (40%)**

2. **Summative Assessment (60%)**

MODERATION ARRANGEMENTS

(i) Moderation Arrangements

Moderation is an integral component of the quality assurance system for the Diploma in Cyber Security and is implemented to ensure the validity, reliability, fairness and consistency of assessment practices.

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

(ii) 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

Recognition of Prior Learning (RPL)

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

CREDIT ACCUMULATION AND TRANSFER

Credit Accumulation and Transfer (CAT) shall be implemented in accordance with the National Credit and Qualifications Framework (NCQF) and applicable Botswana Qualifications Authority (BQA) guidelines.

The transfer and accumulation of credits shall apply only to modules that are NCQF-aligned and recognised by BQA and shall be guided by the institution's approved Credit Accumulation and Transfer Policy.

Credits awarded through CAT must demonstrate equivalence in learning outcomes, level, credit value and assessment standards to ensure the integrity of the qualification.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

1. Learning Pathways

The Diploma in Cyber Security provides both horizontal and vertical articulation opportunities within the National Credit and Qualifications Framework (NCQF), enabling learner mobility and lifelong learning.

1.1 Horizontal Articulation

Graduates may articulate horizontally into related NCQF Level 6 diploma qualifications, subject to institutional entry requirements and Credit Accumulation and Transfer (CAT) arrangements.

Possible horizontal progression pathways include:

- Diploma in Information Technology
- Diploma in Computer Science
- Diploma in Information Systems
- Diploma in Network Engineering
- Diploma in Software Engineering
- Diploma in Business Information Technology
- Diploma in Data Analytics
- Diploma in Digital Forensics
- Diploma in Cloud Computing
- Diploma in Information Security

1.2 Vertical Articulation

Graduates may articulate vertically into NCQF Level 7-degree qualifications, subject to institutional admission requirements.

Possible vertical progression pathways include:

- Bachelor of Cyber Security
- Bachelor of Data Science (with security focus)
- Bachelor of Information Security and Assurance
- Bachelor of Applied Computing (Cyber Security or Network Security stream)
- Bachelor of Science in Artificial Intelligence with Cyber Security

- Bachelor of Science in Computer Science
- Bachelor of Science in Information Systems

2. Employment Pathways

Graduates of the Diploma in Cyber Security will be equipped with practical, occupationally relevant skills enabling entry-level and junior-level employment in the following occupational areas across public and private sector organisations:

- Cybersecurity Analysts and Information Security Specialists
- Incident Response and Cyber Threat Management Practitioners
- Network Security and Network Defence Practitioners
- Systems and Information Security Analysts
- Cybersecurity Technicians and Security Operations Centre (SOC) Analysts
- ICT Security Support Practitioners
- Digital Forensics and Digital Evidence Technicians
- Information Security Compliance and Governance Support Practitioners

These occupations are applicable across sectors including:

- Government ministries and parastatals
- Financial services and banking institutions
- Telecommunications and network service providers
- ICT and cybersecurity service firms
- Education and research institutions
- Law enforcement and cybercrime investigation units
- Private sector organisations requiring information security support

QUALIFICATION AWARD AND CERTIFICATION

The Diploma in Cyber Security shall be awarded to learners who have successfully met all the requirements of the qualification in accordance with the National Credit and Qualifications Framework (NCQF).

To qualify for the award, a learner must:

- Accumulate a minimum of 360 credits, comprising:
  - 72 compulsory credits from the Fundamental component.
  - 276 compulsory credits from the Core component; and

- 12 credits from one approved Elective module.

- Successfully complete the Industry Attachment (Work-Integrated Learning) component.
- Achieve a minimum pass mark of 50% in all registered and required modules.

Certification shall be issued in accordance with the institution's assessment, moderation and quality assurance policies and the requirements of the Botswana Qualifications Authority (BQA).

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

(a) Title of Qualification: The title of the developed qualification, Diploma in Cyber Security, is identical to the benchmark qualifications examined at Zetech University (Kenya), Zentrix Africa Technology Institute (Uganda), Victoria University (Australia), and OTHM (UK).

(b) NQF Level, Credit Value, and Duration: The developed qualification is registered at NCQF Level 6 with a total value of 360 credits delivered over 3 years
While benchmarks such as the Kenya and Australia diplomas are often shorter (1–2 years) and situated at Level 5 on their respective frameworks, they are considered comparable in complexity because the NCQF Level 6 descriptors for "Advanced Knowledge and Skills" align with the depth required for autonomous cybersecurity practice in those jurisdictions
The 3-year duration of the developed qualification is necessitated by the inclusion of extensive work-integrated learning and a high-credit capstone project to meet local industry needs.

(c) Main Exit Outcomes: Across all benchmarks and the developed qualification, there is a unified focus on producing graduates capable of protecting ICT infrastructure, conducting forensic investigations, and implementing defensive security controls
The learning outcomes are comparable as they all require graduates to synthesise technical security measures with legal and ethical governance frameworks

(d) Domains/Modules Covered: The developed qualification and the benchmarks are highly similar in their core technical domains, specifically covering Networking, Cryptography, Operating Systems Security, Ethical Hacking, and Digital Forensics
The developed qualification is further enhanced by offering specialised electives in AI and Cloud Security, providing the same opportunities for specialisation as seen in international standards

(e) Assessment Strategies and Weightings: The assessment strategy for the developed qualification

utilises a 40% Formative and 60% Summative weighting
This differs from the 100% assignment-based model of the OTHM (UK) benchmark but was selected to ensure a robust evaluation of both practical laboratory skills and theoretical mastery, which is consistent with the blended assessment models used at Victoria University and Zetech University

(f) Qualification Rules and Minimum Standards: To be awarded the qualification, learners must accumulate a minimum of 360 credits, including 72 fundamental, 276 core, and 12 elective credits
This structure is comparable to the benchmarked qualifications, which also require the successful completion of all core modules and a mandatory practical project

(g) Education and Employment Pathways: The developed qualification provides clear horizontal and vertical articulation into higher ICT degrees (NCQF Level 7) and entry-level professional roles such as Cybersecurity Analyst and SOC Technician, mirroring the career and academic progression pathways established in the Kenyan, Australian, and UK frameworks.
Conclusion: The developed qualification is globally comparable in title, core domains, and professional outcomes.
It offers greater depth and workplace readiness than some regional benchmarks due to its higher credit volume and mandatory industry attachment

REVIEW PERIOD

The qualification shall be formally reviewed every five (5) years, following the completion of a full delivery cycle.

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

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	