BQA NCQF QUALIFICATION TEMPLATE

SECTION A:	QUALIFICATION DETAILS																				
QUALIFICATION DEVELOPER (S)	**Cyber Intelligence College (CIC) Botswana**																				
TITLE	Bachelor of Science in Cybersecurity and Blockchain Technology													**NCQF LEVEL**						7	
STRANDS (where applicable)	N/A																				
FIELD	Information and Communications Technology													**CREDIT VALUE**						480	
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 Botswana's critical need for expertise in blockchain and cybersecurity amid digital transformation, with global cyber threats escalating at 921 password attacks per second and a projected 32% job growth for security analysts through 2032 (BLS 2023, median salary $120,360). It aligns with Botswana's Vision 2036 (Pillars 1 and 2) for sustainable development, NDP 11's knowledge-based economy, the Botswana Cybersecurity Act (2024) for national security, the National Cybersecurity Strategy for threat mitigation, and the EU Digital Services Act for compliance in digital service development. Informed by CIC's 2025 Blockchain and Cybersecurity Needs Assessment Survey and HRDC Priority Skills 2023/2024 (cybersecurity, data analytics, digital services), it fills skills gaps in secure blockchain applications and data protection. Benchmarking University of Maryland's cybersecurity specialization (US), Carnegie Mellon's blockchain security (US), Stanford's cloud innovation (US), Georgia Tech's blockchain focus (US), ETH Zurich's blockchain research (Switzerland), University of Warwick's NCSC-certified Cyber Security (UK), University of Oxford's cybersecurity pathway (UK), University College London's cybersecurity specialization (UK), Manchester Metropolitan University's DevSecOps focus (UK), University of Cape Town's cybersecurity specialization (Africa), University of Pretoria's information systems security (Africa), and BIUST's Cyber Security (Africa), the program embeds certifications (e.g., CEH, CBSP, GDPR) and real-world projects to produce graduates who innovate secure digital ecosystems and compete globally.

PURPOSE: (itemise exit level outcomes)

The purpose of the qualification is to produce graduates with specialized knowledge, skills, and competence to:

1. Apply core cybersecurity, networking, and cryptographic principles to analyse and evaluate the security architecture of various blockchain platforms (e.g., public, private, hybrid) and decentralized systems.
2. Design, develop, and rigorously test secure smart contracts and decentralized applications (DApps) by integrating secure coding practices and identifying potential vulnerabilities prior to deployment.
3. Conduct vulnerability assessments, ethical hacking, and digital forensics to detect, mitigate, and respond to cyber incidents and exploits.

4. Assess cyber risks associated with blockchain-based assets and infrastructure, then design and implement robust security policies, compliance frameworks, and governance models appropriate for decentralized technologies.
5. Apply theoretical knowledge to solve complex, real-world problems by designing and implementing secure, innovative blockchain solutions tailored for various industries, such as finance, supply chain management, and healthcare.
6. Adhere to professional and ethical standards demonstrating a comprehensive understanding of the legal, ethical, and professional responsibilities inherent in cybersecurity and blockchain.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

1. Applicants must have a minimum of Certificate IV, NCQF Level 4 (TVET/GE) or equivalent
2. Recognition of Prior Learning (RPL) and Credit Accumulation Transfer shall be administered according to the National RPL and CAT Policy for admission.

SECTION B	**QUALIFICATION SPECIFICATION**
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**
1. Design secure blockchain systems for enterprise applications to conceive and architect blockchain solutions	1.1 Analyse enterprise requirements for blockchain solutions, identifying key security, scalability, and integration needs. 1.2 Select appropriate blockchain platforms and consensus mechanisms based on enterprise application requirements. 1.3 Develop a robust blockchain architecture that addresses confidentiality, integrity, and availability requirements.

	1.4 Propose strategies for integrating blockchain solutions with existing enterprise systems and infrastructure.
2. Implement cybersecurity defences against emerging threats to protect against the latest cyber threats, including those targeting blockchain technology.	2.1 Identify and assess emerging cyber threats targeting blockchain and other digital systems. 2.2 Apply cryptographic techniques to secure data in transit and at rest within blockchain and cyber environments. 2.3 Implement network security controls to protect against unauthorized access and malicious activities. 2.4 Design and deploy secure smart contracts, considering potential vulnerabilities and best practices.
3. Analyse and protect data in blockchain and cyber environments to assess security risks in both blockchain and traditional cyber systems.	3.1 Evaluate security risks associated with data handling in both blockchain and traditional cyber systems. 3.2 Implement data protection strategies that ensure privacy and regulatory compliance. 3.3 Analyse data on blockchain ledgers for security vulnerabilities and potential misuse. 3.4 Develop and apply data integrity mechanisms for blockchain-based systems.

4. Align digital services with regulatory compliance to ensure that digital services and blockchain are compliant	4.1 Identify relevant regulations and legal frameworks impacting digital services and blockchain technology. 4.2 Develop strategies for ensuring compliance with data privacy regulations in blockchain implementations. 4.3 Evaluate the impact of regulatory compliance on the design and operation of digital services and blockchain solutions. 4.4 Implement governance models for blockchain and digital services that support regulatory adherence.
5. Lead interdisciplinary teams in blockchain-cybersecurity projects to guide and manage teams composed of individuals with diverse expertise in blockchain and cybersecurity	5.1 Facilitate effective communication and collaboration among team members with diverse expertise. 5.2 Assign roles and responsibilities within a project team, considering individual strengths and skillsets. 5.3 Oversee project progress and identify areas needing additional support or adjustment. 5.4 Mentor team members in both blockchain and cybersecurity concepts to enhance overall project performance.
6. Communicate strategic solutions for digital transformation to simplify complex technical and strategic information related to blockchain and cybersecurity.	6.1 Articulate complex technical concepts related to blockchain and cybersecurity in a clear and concise manner.

	6.2 Tailor communication styles and content to different audiences, including technical and non-technical stakeholders. 6.3 Develop strategic communication plans for promoting digital transformation initiatives. 6.4 Present blockchain and cybersecurity solutions and their strategic implications to leadership and key stakeholders.
7. Conduct security audits and vulnerability assessments for blockchain systems.	7.1 Utilize security audit methodologies to assess the robustness of blockchain implementations. 7.2 Identify and analyse vulnerabilities in blockchain applications, including smart contracts and network infrastructure. 7.3 Recommend appropriate countermeasures to mitigate identified security risks. 7.4 Generate comprehensive security audit reports detailing findings and recommendations for improvement.
8. Develop and implement incident response plans for blockchain-related cyber threats.	8.1 Formulate a detailed incident response plan for addressing cybersecurity incidents affecting blockchain systems. 8.2 Apply forensic techniques to investigate security breaches within blockchain environments. 8.3 Coordinate response efforts during a cybersecurity incident, involving relevant stakeholders.

	8.4 Analyse incident data to identify root causes and implement preventative measures.
9. Evaluate the societal and ethical implications of blockchain and cybersecurity technologies.	9.1 Assess the ethical challenges posed by the development and deployment of blockchain and cybersecurity technologies. 9.2 Analyse the societal impact of blockchain and cybersecurity on privacy, trust, and decentralization. 9.3 Advocate for the responsible use of blockchain and cybersecurity to promote digital equity and mitigate harm. 9.4 Engage in discussions on the policy and regulatory landscape surrounding blockchain and cybersecurity technologies.

SECTION C	QUALIFICATION STRUCTURE		
	TITLE	**Credits Per Relevant NCQF Level**	**Total Credits**

COMPONENT					
		Level [6]	Level [7]	Level [8]	
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Fundamentals of Cybersecurity	**20**			**20**
	Introduction to Blockchain	**20**			**20**
	Programming for Secure Systems (Python/Solidity)	**20**			**20**
	Discrete Mathematics & Cryptography Basics	**20**			**20**
	Operating Systems & Networks	**20**			**20**
	Professional Ethics & Digital Compliance	**20**			**20**
CORE COMPONENT Subjects/Courses/ Modules/Units	Secure Software Development		**20**		**20**
	Applied Blockchain (Smart Contracts)		**20**		**20**

	Network Security & SIEM		**20**		**20**
	Identity Management in Blockchain		**20**		**20**
	Risk Management & Governance (NIST/ISO)		**20**		**20**
	Digital Forensics & Incident Response		**20**		**20**
	Enterprise Blockchain Architecture		**20**		**20**
	Cloud & Infrastructure Security		**20**		**20**
	Cyber Threat Intelligence		**20**		**20**
	DevSecOps for Blockchain		**20**		**20**
	Mini Capstone (Secure Digital Service Design)		**10**		**10**
	Advanced Blockchain Integration		**20**		**20**

	Ethical Hacking & Penetration Testing		**20**		**20**
	Strategy, Leadership & Audit		**20**		**20**
	Final Year Project – Blockchain-Cyber Capstone		**30**		**30**
STRANDS/ SPECIALIZATION	Subjects/ Courses/ Modules/Units	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [6]	**Level [7]**	**Level [8]**	
1.					
2.					
Electives	Mobile & IoT Blockchain Security	**30**			**30**
	Supply Chain Blockchain	**30**			**30**
	Mobile & IoT Blockchain Security	**30**			**30**

	OT & ICS Cybersecurity		**30**		**30**
	Zero Trust in Blockchain		**30**		**30**
	Secure AI & Blockchain		**30**		**30**
	Data Protection in Digital Services		**30**		**30**

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
Level 6	**120**
Level 7	**360**
TOTAL CREDITS	**480**

Rules of Combination:

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

The qualification requires:

- Fundamental: All 120 credits mandatory (Level 6).
- Core: All 360 credits mandatory
- Electives: Choose one 30-credit elective in (Level 6) and one in level 7 (totalling 60 credits.
- Progression: 50% pass per module; 120 credits at Level 8 required.
- Total: 480 credits, RPL up to 120.

ASSESSMENT ARRANGEMENTS
Assessment will consist of both formative and summative assessments and should be aligned with learning outcomes and sub-outcomes. Assessment will be conducted by registered and accredited assessors by a recognized regulatory body. Formative Assessment Formative (50%) Summative Assessment Summative (50%):
MODERATION ARRANGEMENTS
There will be provision for internal and external moderation in accordance with the university policies and regulations, internal and external moderations shall be conducted by qualified moderators or by a recognized regulatory body.
RECOGNITION OF PRIOR LEARNING
There is a provision for award of this qualification through RPL in line with institutional and national policies.
CREDIT ACCUMULATION AND TRANSFER
There is a provision for award of this qualification through credit accumulation in line with institutional and national CAT policies.
PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)
Horizontal Articulation: ● BSc Computer Science (UB, BIUST) ● BSc Cybersecurity (UCT).

Vertical Articulation:

Graduates of this qualification will have the following options for postgraduate education:

- MSc Blockchain/Cybersecurity (Maryland, Warwick), PhD Cybersecurity (Stanford, Carnegie Mellon).

Employment Pathways:

Graduates of this qualification will be able to take up the following jobs

- Blockchain Security Analyst
- Cyber Architect
- Digital Compliance Officer
- Enterprise Security Architect
- SOC Lead
- Cloud Consultant
- Risk Officer

QUALIFICATION AWARD AND CERTIFICATION

1. Minimum standards of achievement for the award of the qualification

   To be eligible for the award of the Bachelor of Science in Cybersecurity and Blockchain Technology, candidates should have obtained a minimum of 480 credits.

2. Certification

   A certificate will be issued to learners who are awarded the qualification.

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

The BSc in Cybersecurity and Blockchain Technology at CIC Botswana is a 4-year, 480-credit qualification (NCQF Level 7) designed to equip students with skills in securing blockchain systems and defending against cyber threats. It was favourably compared with the following qualifications:

1. EDUVOS Faculty of Information Technology South Africa Bachelor of Science in Information Technology (Security and Network Engineering) NQF Level 7, SAQA ID 120690 480 credits, 4 years
2. Amity University (Tashkent, Uzbekistan): Offers a Bachelor of Science in Cyber Security and Blockchain 3-year, full-time undergraduate degree
3. Helvetic Institute of Technology (Switzerland, with Tiffin University): Features a Bachelor in Blockchain 135 credit hours or 180 European Credit Transfer System (ECTS) credits.
4. National University (Oman): BSc in Blockchain Technology BSc in Blockchain Technology 4-year, full-time program worth 120 credit hours

The following is a summary of similarities and differences

Similarities

Qualification Type

All are undergraduate bachelor's degrees in information technology–related fields, with a focus on cybersecurity, blockchain, or network engineering.

Duration / Credit Load

Standard full-time study programs (3–4 years) with credit loads aligned to regional frameworks (NQF credits in SA, ECTS in Switzerland, and credit hours elsewhere). Emphasis on comprehensive learning and practice-oriented training to meet academic and industry standards.

Exit Outcomes

Graduates are expected to demonstrate: Technical competence in cybersecurity, blockchain, and IT systems. Problem-solving and innovation skills for secure digital solutions. Ethical and professional responsibility in IT and data handling. Ability to apply theoretical knowledge to real-world problems and transition into industry roles.

Domains / Modules Core domains include:

Cybersecurity principles and practices Blockchain technologies (design, implementation, applications) Networks and systems administration Software development / programming Mathematics, algorithms, and applied computing Most also embed professional skills, ethics, and project/research components.

Education & Employment Pathways

Graduates are prepared for roles such as Cybersecurity Analyst, Blockchain Developer, Network Engineer, Security Architect, IT Consultant, or Researcher.

All provide a pathway to postgraduate studies (Master's/PhD) in IT, Cybersecurity, or Blockchain.

Differences

●Title of Qualification

Eduvos: BSc in IT (Security & Network Engineering) → broader IT with specialisation.

Amity: BSc in Cyber Security and Blockchain → dual-focus program.

Helvetic/Tiffin: Bachelor in Blockchain → specialised in blockchain, less broad IT.

Oman: BSc in Blockchain Technology → explicitly blockchain-focused but positioned within IT.

● NQF Level & Credit Value

Eduvos: NQF Level 7, 480 SA credits (4 years) – highest workload.

Amity: 3 years, unspecified local credit framework.

Helvetic/Tiffin: 135 US credit hours / 180 ECTS credits – European/US credit alignment.

Oman: 120 credit hours, 4 years – typical Middle East/US credit system.

● Qualification Rules / Standards

Eduvos aligns with SAQA/NQF requirements (clear SA standards for exit level outcomes).

Amity aligns with Uzbekistan higher education standards, likely influenced by Amity's global model.

Helvetic/Tiffin integrates European Bologna Process standards (ECTS) and US degree norms.

Oman follows GCC/Middle Eastern higher education regulations, with emphasis on applied learning.

●Assessment Weightings

Eduvos: Clear balance of fundamental, core, and electives with research/project.

Amity: More practice-oriented, with focus on lab/project-based evaluation in cybersecurity and blockchain.

Helvetic/Tiffin: Likely research and case-study driven, aligned with international blockchain applications.

Oman: Structured around theory, labs, and final-year project, following US-style credit hour assessment weightings.

Focus Areas

Proposed qualification: Stronger in network engineering and security infrastructure.

Amity: Balanced between cybersecurity and blockchain integration.

Helvetic/Tiffin: Deep specialisation in blockchain design, development, and innovation.

Oman: Blockchain-specific, with regional application relevance (e.g., fintech, supply chain, e-government).

Conclusion

All four qualifications share the goal of producing industry-ready IT graduates with strong cybersecurity and blockchain expertise, assessed through a mix of coursework, projects, and applied learning. The main differences lie in their regional frameworks, credit values, and balance of general IT vs. blockchain specialisation. The proposed qualification is the most broad and comprehensive, Amity offers a dual-focused blend, Helvetic/Tiffin is the most specialised in blockchain, and Oman balances regional needs with international standards.

REVIEW PERIOD
The qualification will be reviewed every 5 years.

(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	