BQA NCQF QUALIFICATION TEMPLATE

SECTION A:	QUALIFICATION DETAILS																
QUALIFICATION DEVELOPER (S)	**Cyber Intelligence College (CIC) Botswana**																
TITLE	Bachelor of Science in Cybersecurity and Artificial Intelligence												**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 has been developed as a response to HRDC's PRIORITY SKILLS 2023/2024 CONSOLIDATED LIST OF PRIORITY OCCUPATIONS AND SKILLS report that clearly state the need of Industrial Automation Engineers with technical skills in Cybersecurity & Artificial intelligence. Botswana's accelerated digital transformation has increased exposure to sophisticated cyber threats across key sectors such as finance, healthcare, government, education, and telecommunications. As highlighted in the National Cybersecurity Strategy, there is a critical shortage of cybersecurity expertise in the country, limiting Botswana's capacity to proactively detect, prevent, and respond to complex cyber incidents.

The Bachelor of Science in Cybersecurity and Artificial Intelligence directly addresses this national challenge by developing a new generation of cybersecurity professionals with technical depth, strategic insight, and hands-on capabilities. The four-year degree offers a comprehensive curriculum covering network and system security, digital forensics, cloud and mobile security, blockchain and AI security, cyber law, secure APIs, and threat intelligence. It balances theoretical foundations with practical skills, research, and industry-aligned projects, ensuring that graduates are ready for real-world cybersecurity environments.

Human Resource Development Council (HRDC) 2023/24 priority skills list ranks Cybersecurity, Programming, AI, Cloud Security, and Software Development among Botswana's top ICT skill gaps. The qualification also incorporates globally recognized industry certifications such as Security+, CEH, CCNA Security, AWS Security, and Microsoft Security Fundamentals, enhancing employability and relevance.

Globally, the (ISC)² Cybersecurity Workforce Study (2023) estimates a shortage of over 4 million cybersecurity professionals, signalling intense global demand for qualified practitioners. The Bachelor of Science in Cybersecurity and Artificial Intelligence aligns with this need, offering a future-ready qualification that is not only responsive to national development priorities but also globally competitive.

The qualification further supports national innovation by bridging academia and industry, fostering partnerships, and preparing students to contribute to Botswana's cybersecurity resilience and digital economy.

PURPOSE: (itemise exit level outcomes)

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

1. Apply AI/ML (Artificial Intelligence and Machine Learning) methods to analyse cyber threats, detect vulnerabilities, and formulate proactive defence strategies.
2. Design and implement secure and intelligent systems to protect cloud-based and virtualized environments from emerging and AI-driven attacks.
3. Perform cyber threat analysis, incident response, and digital forensics to identify, investigate, and respond to security incidents.
4. Analyse and address ethical, legal, and societal implications to make informed judgments regarding the social impact and responsible use of these powerful technologies
5. Communicate technical information and practice professional teamwork to develop and implement solutions for cybersecurity and AI challenges.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

1. Applicants must have a minimum of Certificate IV, NCQF Level 4 (TVET/GE) or equivalent
2. Candidates who do not meet the minimum academic qualifications stated above will be considered through the Recognition of Prior Learning (RPL) process which shall be administered according to the National RPL Policy. There will also be provision for Credit Accumulation Transfer to the learner in case they transfer in from another institution as per National Policy on CAT.

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

SECTION B	QUALIFICATION SPECIFICATION
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**

1. Apply machine learning models for threat detection to detect and classify cyber threats like malware, network anomalies, and phishing attempts	1.1. Correctly select and justify appropriate ML algorithms (e.g., supervised, unsupervised, deep learning) for detecting various cyber threats. 1.2. Preprocess and prepare real-world cybersecurity datasets for training and validation. 1.3. Implement ML models that detect and classify threats such as malware, anomalies, or phishing attempts with acceptable accuracy. 1.4. Evaluate model performance using appropriate metrics (precision, recall, F1-score, ROC/AUC) and optimize results. 1.5. Critically analyse limitations of the applied ML models and recommend improvements for real-world deployment.
2. Design and implement security architectures for cloud and virtualized platforms, incorporating AI-driven tools for threat detection, access control, and compliance management to protect against emerging attacks	2.1. Apply architectural principles to design secure frameworks for cloud and virtualized environments. 2.2. Integrate AI-driven tools for intrusion detection, access control, and compliance monitoring within the design. 2.3. Demonstrate correct implementation of identity and access management (IAM) and encryption mechanisms.

	2.4. Conduct security testing to validate resilience of the architecture against simulated AI-driven attacks. 2.5. Document and justify architectural decisions, showing alignment with compliance standards (e.g., ISO 27001, NIST).
3. Conduct advanced threat analysis and hunting analytics to proactively hunt for sophisticated threats, identify vulnerabilities, and develop data-driven hypotheses for potential attack vectors before they can cause harm.	3.1. Apply data-driven methodologies and analytics to proactively identify sophisticated and stealthy threats. 3.2. Use threat intelligence platforms and AI-based tools to detect anomalous behaviours. 3.3. Identify and prioritize vulnerabilities using risk-based approaches. 3.4. Formulate hypotheses and predictive models of potential attack vectors. 3.5. Produce a comprehensive report with recommendations for mitigation and proactive defence.
4. Develop and execute comprehensive incident response plans, apply digital forensics methodologies to investigate security breaches, and use AI-powered tools to analyse digital evidence for incident recovery and reporting.	4.1. Develop detailed, structured incident response playbooks aligned with industry standards (e.g., NIST, SANS). 4.2. Apply digital forensics methodologies to acquire, preserve, and analyse digital evidence. 4.3. Use AI-powered forensic and log analysis tools to reconstruct and interpret attack timelines.

	4.4. Communicate findings to both technical and non-technical stakeholders. 4.5. Produce an incident recovery and post-incident report that includes lessons learned and recommendations.
5. Analyse the professional, ethical, and societal implications of AI in cyber defence, including data privacy, algorithmic bias, accountability, and the responsible use of surveillance technologies.	5.1. Critically evaluate ethical dilemmas in deploying AI for surveillance, monitoring, and cyber defence. 5.2. Assess issues of algorithmic bias, fairness, and accountability in AI models for security. 5.3. Analyse data privacy concerns in compliance with international standards and human rights principles. 5.4. Apply ethical frameworks to justify or critique the responsible use of AI in security applications. 5.5. Present well-reasoned arguments on the societal impact of AI-driven cyber defence solutions.
6. Apply legal and regulatory frameworks, such as GDPR and data protection laws, when designing and deploying secure, intelligent systems	6.1. Correctly identify and interpret applicable laws (e.g., GDPR, HIPAA, local data protection laws) in cybersecurity design. 6.2. Apply compliance requirements to the development and deployment of secure AI-enabled systems.

	6.3. Evaluate system designs for conformity with global and local data protection regulations. 6.4. Recommend improvements to align existing security systems with evolving legal frameworks. 6.5. Demonstrate ability to balance security innovation with legal and regulatory obligations
7. Communicate technical and strategic cybersecurity concepts in a clear business-oriented manner.	7.1. Translate technical cybersecurity concepts into language understandable to non-technical stakeholders. 7.2. Develop structured written reports that are concise, accurate, and business-oriented. 7.3. Deliver clear oral or multimedia presentations on cybersecurity risks and solutions. 7.4. Tailor communication style to audiences ranging from technical peers to executive leadership. 7.5. Demonstrate professional use of visuals, charts, and data in communicating cybersecurity strategies
8. Work as an effective team member or leader on cybersecurity and AI projects, demonstrating project management skills, presenting work to clients, and reflecting on collaborative experiences.	8.1. Contribute effectively to collaborative decision-making and task distribution within a team.

	8.2. Demonstrate leadership by coordinating tasks, managing timelines, and resolving conflicts where required. 8.3. Apply project management tools and methodologies to plan and track project progress. 8.4. Present group project outcomes to clients or stakeholders professionally and persuasively. 8.5. Reflect critically on team collaboration, identifying strengths, challenges, and areas for personal improvement.

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

SECTION C	QUALIFICATION STRUCTURE				
COMPONENT	TITLE	Credits Per Relevant NCQF Level			Total Credits
		Level [6]	Level [7]	Level [8]	

FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Introduction to Computer Systems	**10**			**10**
	Programming Fundamentals (Python & C)	**10**			**10**
	Mathematics for Cybersecurity	**10**			**10**
	Digital Literacy and Professional Practice	**10**			**10**
	Networking and Cybersecurity Essentials	**10**			**10**
	Logic and Discrete Structures	**10**			**10**
	Introduction to Operating Systems	**10**			**10**
	Communication and Academic Literacy Skills	**10**			**10**
	Introduction to Web Technologies and Secure Coding	**10**			**10**

CORE COMPONENT Subjects/Courses/ Modules/Units	Database Systems and SQL Injection Basics		**10**		**10**
	Computer Networks and Security		**10**		**10**
	Information Security Governance & Compliance		**10**		**10**
	Ethical Hacking: Tools and Techniques		**10**		**10**
	Cybersecurity Laws and Ethics		**10**		**10**
	Cyber Threat Intelligence		**10**		**10**
	Penetration Testing Methodologies		**10**		**10**
	Data Privacy and Protection		**10**		**10**
	Machine Learning in Cybersecurity Analytics		**10**		**10**
	Security Policy and Risk Management		**10**		**10**
	Research Methods in Cybersecurity		**10**		**10**

	Cloud Security and Virtualization		**10**		**10**
	Incident Detection and Response		**10**		**10**
	Forensic Analysis and Malware Investigation		**10**		**10**
	Automation in Threat Detection and Response		**10**		**10**
	API Security and DevSecOps		**10**		**10**
	Blockchain and IoT Security		**10**		**10**
	Secure Cloud Application Development		**10**		**10**
	Applied Cryptography and PKI		**10**		**10**
	Software Security and Secure APIs		**10**		**10**
	Human Factors in Cybersecurity		**10**		**10**
	Quantum-Safe Cryptography		**10**		**10**

	SOC Operations and SIEM Engineering		**10**		**10**
	Advanced Cyber Defense and Threat Hunting		**10**		**10**
	Cybersecurity Leadership and Strategy		**10**		**10**
	Threat Modeling and Secure System Design		**10**		**10**
	Cloud Governance, Risk, and Compliance (GRC)		**10**		**10**
	Offensive Security and Exploit Development		**10**		**10**
	Cybercrime, Law & Digital Ethics		**10**		**10**
	Industrial Attachment (Internship)		**20**		**20**
	Capstone Project I: Research Proposal and Design		**15**		**15**

	Capstone Project II: Solution Implementation & Defense		**15**		**15**
STRANDS/ SPECIALIZATION	Subjects/ Courses/ Modules/Units	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [ ]	**Level [ ]**	**Level [ ]**	
1.					
2.					

Electives	Fundamentals of Entrepreneurship		**10**		**10**
	Logical Representation and Reasoning		**10**		**10**
	Small Business Management		**10**		**10**
	Parallel and Distributed Systems Security		**10**		**10**
	Integrative Programming		**10**		**10**
	Human-Computer Interaction		**10**		**10**
	Mobile Computing and Security		**10**		**10**

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
6	90
7	390
TOTAL CREDITS	**480**

Rules of Combination:

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

The qualification requires:

- 90 credits of Fundamental courses: Completed in Level 6 (Year 1), providing foundational knowledge in computer systems, programming, and cybersecurity principles.
- 340 credits of Core courses: Spread across Level 7 (Years 2 and 3), covering advanced cybersecurity and AI topics, including practical components like Industrial Attachment (20 credits) and Capstone Projects (15 credits each for Proposal and Implementation, totaling 30 credits within the 360).
- 50 credits of Elective courses: Selected from the available options in Level 7 (Years 2 and 3), allowing specialization in areas like entrepreneurship or distributed systems security.
- Total Qualification Credits: 480.
  Each year comprises two semesters, with 60 credits per semester. Progression requires a minimum 50% pass in all modules per semester; 120 credits per year must be completed to advance. Electives: Students select one 10-credit elective per semester in Years 2 and 3 to reach 60 credits. RPL exemptions up to 120 credits are available.

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

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.

1. **Formative assessment**

The Formative assessment shall contribute 50% of the final grade.

2. **Summative assessment**

Summative assessment shall contribute 50% of the final grade.

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

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

Vertical Articulation

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

- Master of Science in Data Science and Artificial Intelligence.
- Master of Science in Computer Science.
- Master of Science in Applied Cybersecurity.
- Master of Science in FinTech Security.
- Master of Science in Computer Information Systems.
- Master of Science in Statistics.

Employment Pathways

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

- AI/Machine Learning Security Engineer
- Cybersecurity Analyst
- AI Security Specialist
- Threat Intelligence Analyst
- Penetration Tester
- Incident Response Coordinator
- IoT Security Engineer
- Cloud and Enterprise Security Architect
- Security Operations Center (SOC) Analyst
- Quantum Security Specialist

QUALIFICATION AWARD AND CERTIFICATION

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

   To be awarded a Bachelor of Science in Cybersecurity and Artificial Intelligence qualification, a candidate must complete a minimum of 480 credits as prescribed for the qualification.

2. Certification

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

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

The proposed BSc in Cybersecurity and AI at CIC Botswana is a 4-year, 480-credit qualification (NCQF Level 7) designed to equip learners with advanced skills in AI-enhanced cybersecurity and threat management. There are no similar qualifications with tittle, but the following qualifications benchmarked against with some similar modules:

1. Nelson Mandela University South Africa Bachelor of Information Technology, NQF Level 7 360 credits
2. University of Warwick (UK) BSc Cyber Security, Level 6 of the Regulated Qualifications Framework (RQF),.360 UK credits, 3 years
3. University of Warwick (UK) BSc Cyber Security, Level 6 of the Regulated Qualifications Framework (RQF), 360 UK credits, 3 years
4. University of Chester (UK) BSc Cybersecurity with Artificial Intelligence RQF Level 6, ~360 credits, 3 years

Similarities

- All are undergraduate-level qualifications intended to prepare graduates for cybersecurity/IT roles or further study. UK honours BSc programmes are typically 3 years (~360 credits) and share common module types (programming, networks, cryptography, project). South African BIT follows NQF/bachelor conventions with core IT fundamentals and elective streams. Assessments across institutions combine coursework, labs, projects and exams. SAQA University of Warwick Manchester Metropolitan University

Differences (major):

- Focus & scope: Mandela's BIT is broader IT with optional streams (IT applications in sectors), while Warwick/MMU BSc degrees are specifically focused on cyber security with in-depth technical and socio-technical content. Cybersecurity AI qualification introduces explicit ML/AI learning outcomes and modules not always present in standard cyber degrees. SoitUniversity of Warwick University of Chester
- National frameworks & credit language: South Africa uses NQF levels and SAQA registration language; UK uses credit totals per academic year (and Honours classification rules). This affects how minimum standards and progression rules are expressed and regulated. SAQA Manchester Metropolitan University

- Industry alignment: Some UK programmes highlight NCSC/GCHQ alignment or employer links (Warwick/WMG); the vocational emphasis and certification alignment may differ by provider and influences employability routes

Conclusion

The proposed BSc in Cybersecurity and AI represents a specialized path within cyber security, blending foundational security knowledge with AI advancements to address evolving threats and automate security systems and therefore offering a competitive edge over qualifications benchmarked with

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**	