SKILLS PROGRAME DOCUMENT					
Skills Programme Title	**Cybersecurity Defender**				
NQF Level	4	Credits	60	Duration in days	75
Skills Programme ID	SP - 220330				
Skills Programme Status	Approved		Start Date	End Date	
			11/03/2022	11/03/2027	
Last date for enrolment	11/03/2028	Last date for achievement	11/03/2031		

SKILLS PROGRAMME DETAILS

1.	**Title**	Cybersecurity Defender
2.	**Sub Title**	OFO Code: 252901 OFO Occupation: ICT Security Specialist
3.	**NQF Level**	4
4.	**Duration**	600 Hours (75 Days)
5.	**Credits**	60
6.	**Quality Assuring Body**	Quality Council for Trades and Occupations (QCTO)
7.	**Skills Programme Rationale**	This qualification will support the recommendations of the Presidential Commission on the 4th Industrial Revolution. This report forefronts human capital and the future of work and refers to growing skills instability. The 4th Industrial Revolution (4IR) is a fusion of advances in artificial intelligence (AI), robotics, process automation, the Internet of Things (IoT), genetic engineering, quantum computing, cyber security, cloud computing and data science. These will bring enormous changes to the world of work in which cybersecurity will play an increasingly pivotal role in the execution of tasks, manufacturing and services. The COVID pandemic caused a global shift towards remote and hybrid work environments and forced organisations to engage in a huge shift of how the workforce engage in day-to-day work activities. Similarly, the pandemic influenced the cyber threat landscape, creating a cyber pandemic in its wake. Companies are now forced to strengthen their cyber resilience strategy through continuous improvements to cyber security mechanisms. In South Africa the first piece of legislation was promulgated, namely the Cybercrimes Act of 2020, which will have an impact on how Cybersecurity Specialists and Defenders will operate. It is therefore of imperative importance that Cybercrime Defenders are trained and prepared for this demanding work environment. Currently, as hacking and data breaches increase, the demand for cybersecurity professionals is outpacing the supply. No similar skills programmes that have been approved by the QCTO Cybercrime has demonstrated that it can have detrimental effects on companies, governments and individuals. Nobody is secure against these malicious attacks; cybercrimes causing loss of data, loss of money and loss of privacy, thus impacting on all levels of society and the economy. A well-trained Cybersecurity workforce will benefit the full range of possible victims of cybercrime. The sector will benefit by being able to supply the much-needed Cybersecurity Defenders for deployment in the market. Currently, as hacking and data breaches increase, the demand for Cybersecurity professionals is outpacing the supply. The target group for this learning is school leavers wanting to pursue a career in cybersecurity.

		No formal registration is required to operate as a Cybersecurity Defender. However, international certification programmes are available and it will be to the benefit of the learner to achieve these certifications. Cybersecurity Defenders can be employed in any economic sector, e.g., finance, insurance, healthcare, energy, environment, government, transport, agriculture and food. They can be employed in positions such as Cybersecurity Defenders, Junior Penetration Testers and so forth.	
8.	**Related registered qualification/s**	Occupational Certificate: Cybersecurity Analyst, NQF Level 5	
9.	**Purpose**	Cybersecurity Defenders are responsible for proactively protecting organisations' systems from attacks, they are the first line of defence against cyberattacks, the first responders to cybersecurity breaches and are responsible for the hardening of the information systems of organisations ensuring compliance with legislation. The tasks that the learner will be able to know, do and understand after achievement of the skills programme include: • Detecting cybersecurity threats and vulnerabilities in the cybersecurity posture of the organisation • Defending against threats to ensure cybersecurity of the organisation • Evaluating the security posture to enhance resilience	
10.	**Content**	**<u>Knowledge component</u>** • 900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7 • 900103-000-00-KM-02, Cyber Threats and Attacks, NQF Level 4, Credits 7 • 900103-000-00-KM-03, Cybersecurity, NQF Level 4, Credits 7 • 900103-000-00-KM-04, Responding to Cybersecurity Incidents, NQF Level 4, Credits 5 Total credits: 26	**<u>Application component</u>** • 900103-000-00-PM-01, Protect Against Cybersecurity Threats, Intrusions and Attacks, NQF Level 4, Credits 11 • 900103-000-00-PM-02, Detect Cybersecurity Threats, Intrusions and Attacks, NQF Level 4, Credits 11 • 900103-000-00-PM-03, Conduct Penetration Testing Techniques to Determine Security, NQF Level 4, Credits 12 Total credits: 34
11.	**Minimum entry requirements**	NQF level 3 (Gr 11) with Computer Literacy, English and Mathematics Literacy	
12.	**Exit Level Outcomes (ELO) and Associated Assessment Criteria (AAC)**	**Exit Level Outcomes (ELO) 1**	

		Demonstrate knowledge and understanding of cybersecurity, cyber threats and attacks and cyber defence **Associated Assessment Criteria (AACs)** • Basic governance principles and concepts related to cybersecurity are understood. • Basic concepts and principles of cybersecurity are understood. • Basic concepts and principles of cyber threats and attacks are understood. • Basic concepts and principles of cyber defence are understood. • Ethical considerations in ethical hacking and penetration testing are understood. • Procedures to respond to cybersecurity incidents are understood. **Exit Level Outcomes (ELO) 2** Protect against cybersecurity intrusions and attacks **Associated Assessment Criteria (AACs)** • User and host identities are verified. • Mechanisms are put in place to prevent system intrusions. • Automated tools are used to guard against intrusions. • Network confidentiality is ensured. • The security posture is evaluated to detect vulnerabilities and to enhance resilience. **Exit Level Outcomes (ELO) 3** Detect cybersecurity threats and attacks **Associated Assessment Criteria (AACs)** • Threats to the cybersecurity of the company are detected. • Adversary techniques, tactics and practices (TTPs) are emulated using an emulation platform. • Network traffic is monitored and analysed using a suitable platform. • Incidents are identified, responded to and reported. **Exit Level Outcomes (ELO) 4** Use different penetration testing tools to identify vulnerabilities in the security posture of an organisation **Associated Assessment Criteria (AACs)** • Foot-printing tools are used against a target and intelligence is gathered. • Vulnerabilities are identified using penetration testing tools. • Servers and devices are attacked to build better defences. • Clients are manipulated to uncover internal threats. • Targets are exploited to increase cybersecurity. Antivirus and intruder detection systems (IDS) are tested
13.	**Continuous Assessment & Final Supervised Assessment (FISA)**	**Continuous Assessment** The SDP must ensure that all learners are enrolled with the QCTO at the start of training (within 5 days) in the format required by the QCTO. Continuous assessments are set by the SDP in accordance with the assessment criteria for each module in a contextualised manner.

		This may consist of a variety of methods, e.g. practical or written assessments, assignments, projects, demonstrations, presentations or any other form of assessment to assist the learner in the learning process. During training, it is mandatory for formal summative assessments to take place at the end of each module/topic. These results must be formally recorded, and be available for monitoring and/or evaluation by the QCTO. **Final Integrated Supervised Assessment (FISA)** All learners gain entrance to the Final Integrated Supervised Assessment by successfully completing all formal summative assessments conducted by the SDP. Format of FISA: A practical assessment integrating the relevant Exit Level outcomes, with simultaneous verbal assessment of embedded knowledge by the assessor before, during or after the FISA. All FISAs must be supervised, and virtual FISAs must be recorded throughout the assessment. All Exit Level Outcomes must be covered in the FISA. In the FISA, the learner must demonstrate applied knowledge and skills to prove that the competencies of the Skills Programme have been achieved. The FISA may not contain any assessments used in the "Continuous Assessment" process (thus no re-assessment). Special considerations should be made for candidates with special learning needs. **Standards for Final Integrated Supervised Assessment (FISA):** The learner should be provided with a brief/job card/task to demonstrate what the learner should show, know or produce in a product, relevant to the Exit Level Outcomes. This is the section where the learner must show applied competency (what the learner must be able to do, and to what expected standard) The FISA INSTRUMENT (Written case study, scenario or brief/task [similar to a job card]) must be developed and moderated by the SDP and conducted in a supervised environment. It is assessed by means of a RUBRIC developed by the SDP for this purpose: A candidate must demonstrate that they are competent at proactively protecting organisations' information systems from attacks, respond to cybersecurity breaches and harden the information systems of organisations ensuring compliance with legislation. The candidate must be given access to internet connection, applicable sofware and hardware as well as a **simulated** platform or lab environment with applicable tools and virtual machines with sufficient information. Candidates must be provided with a scenario related to the company cybersecurity posture, health, attacks and development.

		1. Apply measures to detect cybersecurity threats, intrusions, attacks and vulnerabilities in the cybersecurity posture of the organisation. 2. Apply threat and vulnerability defense mechanisms and procedures to defend and protect against cybersecurity intrusions and attacks to ensure cybersecurity of the organisation 3. Apply different penetration testing tools to identify vulnerabilities in the cybersecurity posture of an organisation to enhance resilience The maximum time for the above is 6 hours. Pass mark is 75%. Whilst conducting the above, strategic, well-timed questions should be asked of the learner to assess embedded knowledge gained during the skills programme, as well as critical thinking and problem-solving skills: for e.g. • "Why.....?" • "What would happen if …?" • "When ….. is done, what would the result be?" • "How would you deal with …..?" • Etc. The marking rubric/compliance checklist used to assess these competencies must include a section for the assessor/facilitator used in this session to make a note of competencies shown, (or not shown), as well as the questions that were asked, and a summary of the learner's answers, and state whether these are of the acceptable standard or not. The marking rubric/compliance checklist compiled should contain specific areas marked with an asterisk (*) as compulsory sections in order for the learner to be declared C (Competent). Compulsory sections are when the safety of the candidate or others would be affected if incorrectly completed. **Submission of final results** Final results must be submitted to the QCTO in the required format, within 21 days of the date of the FISA, together with the following: • Completed QA Verification Report on the FISA (QCTO template: relevant sections). • A copy of the final Assessment Instrument used, as well as the marking guideline / rubric.
14.	**Recognition of Prior Learning**	• Learners will gain access to the skills programme through RPL for access as provided for in the QCTO RPL Policy. RPL for access is conducted by accredited education institution, skills development provider or workplace accredited to offer that specific skills programme. • Learners who have acquired competencies in skills programme will be credited for such topics through RPL.

		• RPL for access to the Final Supervised Assessment: Accredited providers and approved workplaces must apply the internal assessment criteria specified in the skills programme document to establish and confirm prior learning and achievement of required competencies for the skills programme.
15.	**Work Opportunities/further learning**	Cybersecurity Defenders can be employed in any economic sector, e.g., finance, insurance, healthcare, energy, environment, government, transport, agriculture and food. They can be employed in positions such as Cybersecurity Defenders, Junior Penetration Testers and so forth.
16.	**Skills Development Provider Accreditation Requirements**	1. Provider must provide or have access to a learning platform that can simulate the above exercises **OR** existing product 2. Platform must report on simulated exercises 3. Learner must be given access to an individual laptop or PC and access to the internet and must have environment in place (able to use platform to participate in training sessions and record the training session) for the duration of the skills programme. 4. Must be able to store recording offline and in an archiving system and have it available on demand 5. Instructor must be: o competent in the NQF 5 Cyber Security with minimum of 6 months experience in cybersecurity or o equivalent with 6 months experience in cybersecurity or o internationally recognised certification with 6 months experience in cybersecurity **Knowledge Modules** *Physical Requirements:* • The provider must have lesson plans and structured learning material or provide learners with access to structured learning material that addresses all the topics in all the knowledge modules as well as the applied knowledge in the application modules. • QCTO/ MICT SETA requirements *Human Resource Requirements:* • Lecturer/learner ratio of 1:20 (Maximum) • Qualification of lecturer (SME): o NQF 5 qualified in industry recognised qualifications with 1 years' experience in the IT industry o Cybersecurity vendor certification • Assessors and moderators: accredited by the MICT SETA *Legal Requirements:*

		• Legal (product) licences to use the software for learning and training • OHS compliance certificate • Ethical clearance (where necessary) **Application Module:** *Physical Requirements:* • Valid licenses software and application, including OS. • Internet connection and hardware availability. • Examples and information specified in the scope statement and all the case studies, scenarios and access to hardware and software implied in the scope statements of the modules. • Remote learners: Provider must provide business IT simulation system (e.g. invoice processing). *Human Resource Requirements:* • Qualification of lecturer (SME): ○ NQF 5 industry recognised qualification with 1 year relevant experience • Assessors and moderators: accredited by the MICT SETA *Legal Requirements:* • Legal (product) licences to use the software for learning and training • OHS compliance certificate • Ethical clearance (where necessary)

****