QUALIFICATION FILE – Standalone NOS

Essentials of Network Security Measures

☐ Horizontal/Generic ☐ Vertical/Specialization

☐ Upskilling ☐ Dual/Flexi Qualification ☐ For ToT ☐ For ToA

☐General ☐ Multi-skill (MS) ☐ Cross Sectoral (CS) ☒ Future Skills ☐ OEM

NCrF/NSQF Level: 5

Submitted By:

National Institute of Electronics and Information Technology (NIELIT)

NIELIT Bhawan,
Plot No. 3, PSP Pocket, Sector-8,
Dwarka, New Delhi-110077,
Phone: - 91-11-2530 8300
e-mail: - contact@nielit.gov.in

Table of Contents

Section 1: Basic Details 3
Section 2: Training Related 6
Section 3: Assessment Related 6
Section 4: Evidence of the Need for the Standalone NOS 7
Section 5: Annexure & Supporting Documents Check List 7
Annexure-I: Evidence of Level 8
Annexure-II: Tools and Equipment (lab set-up) 10
Annexure-III: Industry Validations Summary 11
Annexure-IV: Training Details 11
Annexure-V: Blended Learning 12
Annexure-VI: Performance Criteria details 12
Annexure-VII: Assessment Criteria 14
Annexure-VIII: Assessment Strategy 15
Annexure-IX: Acronym and Glossary 16

Section 1: Basic Details

<table>
<tr><td>1.</td><td>NOS-Qualification Name</td><td colspan="2">Essentials of Network Security Measures</td></tr>
<tr><td>2.</td><td>Sector/s</td><td colspan="2">IT-ITeS</td></tr>
<tr><td>3.</td><td>Type of Qualification ☒ New ☐ Revised</td><td>NQR Code & version of the existing /previous qualification: NA</td><td>Qualification Name of the existing/previous version: NA</td></tr>
<tr><td>4.</td><td>National Qualification Register (NQR) Code & Version (Will be issued after NSQC approval.)</td><td>NG-05-IT-04176-2025-V1-NIELIT</td><td>5. NCrF/NSQF Level: 5</td></tr>
<tr><td>6.</td><td>Brief Description of the Standalone NOS</td><td colspan="2">This course provides a comprehensive understanding of protecting networks from cyber threats through a blend of theoretical knowledge and hands-on practical training. It begins with the fundamentals of networking and the role of network security, emphasizing its importance in today’s cybersecurity landscape. Students explore various network attacks, including real-world case studies and attack simulations. The course delves into core security principles, such as configuring firewalls, VPNs, IDS/IPS systems, and secure access controls. It also covers network defence strategies, including risk assessment, incident response planning, penetration testing, and using SIEM tools. Finally, students learn about emerging trends in cybersecurity, including AI-based threat detection, the Zero Trust security model, cloud security, and blockchain technology, equipping them with up-to-date knowledge for real-world applications.</td></tr>
<tr><td>7.</td><td>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:
<table>
<tr><th>S. No.</th><th>Academic/Skill Qualification (with Specialization - if applicable)</th><th>Required Experience (with Specialization - if applicable)</th></tr>
<tr><td>1</td><td>UG Diploma</td><td>NA</td></tr>
<tr><td>2</td><td>2nd year of UG in CS/IT/EC/EE/ allied branches</td><td>NA</td></tr>
<tr><td>3</td><td>2nd year of diploma in CS/IT/EC/EE/ allied branches (after 12th)</td><td>NA</td></tr>
<tr><td>4</td><td>3-year Diploma in CS/IT/EC/EE/ allied branches after 10th</td><td>1.5 years experience in cyber security and allied subsector of IT</td></tr>
</table></td></tr>
</table>

		5 | Previous relevant Qualification of NSQF Level 4.5 | 1.5 years experience in cyber security and allied subsector of IT
8.	**Credits Assigned to this NOS-Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	**4 Credits** **9. Common Cost Norm Category (I/II/III)** *(wherever applicable)*: **Category-II**
10.	**Any Licensing Requirements for Undertaking Training on This Qualification** *(wherever applicable)*	No
11.	**Training Duration by Modes of Training Delivery** *(Specify **Total Duration** as per selected training delivery modes and as per requirement of the qualification)*	**☒Offline ☐Online ☐Blended** **Training Delivery Modes** | **Theory (Hours)** | **Practical (Hours)** | **Total (Hours)** **Classroom (offline)** | 45 | 75 | 120
12.	**Assessment Criteria**	**Theory (Marks)** | **Practical (Marks)** | **Project/Presentation/ Assignment (Marks)** | **Viva/Internal Assessment (Marks)** | **Total (Marks)** | **Passing %age** 100 | 60 | 20 | 20 | 200 | 50 The centralised online assessment is conducted by the Examination Wing, NIELIT Headquarters. *Assessment strategy shall be as per NIELIT Norms prevailing at times.
13.	**Is the NOS Amenable to Persons with Disability**	**☒ Yes ☐ No If "Yes", specify applicable type of Disability:** a. Locomotor Disability ● Leprosy Cured Person ● Dwarfism ● Muscular Dystrophy ● iv. Acid Attack Victims b. Visual Impairment c. Low Vision

14.	**Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)*	Cybersecurity Analyst	
15.	**How participation of women will be encouraged?**	Participation by women can be ensured through Government Schemes. Occasionally, exclusive batches for women would be run for the proposed courses. Funding is available for women's participation under other schemes launched by the Government from time to time.	
16.	**Other Indian languages in which the Qualification & Model Curriculum are being submitted**	Qualification file available in English & Hindi Language.	
17.	**Is similar NOS available on NQR-if yes, justification for this qualification**	**☐ Yes ☒ No URLs of similar Qualifications:**	
18.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name:** Shri Niladri Das **Email:** niladridas@nielit.gov.in **Contact No.:** 8794028299 **Website:** https://nielit.gov.in/index.php	
19.	**Final Approval Date by NSQC: 08.05.2025**	**1. Validity Duration: 3 Years**	**2. Next Review Date: 08.05.2028**

Section 2: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	A-Level/MCA/ B. Tech in CS/IT/M.Sc(IT/CS) allied areas with 1 years of Experience in training.
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	A-Level/MCA/ B. Tech in CS/IT/M.Sc(IT/CS) allied areas with 2 years of Experience in training.
3.	**Tools and Equipment Required for the Training**	☒Yes ☐No (If "Yes", details to be provided in Annexure-II)
4.	**In Case of Revised NOS, details of Any Upskilling Required for Trainer**	NA

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	A-Level/MCA/ B. Tech in CS/IT/M.Sc(IT/CS) allied areas with 2 years of Experience in training.
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	The assessor carries out theory online assessments through the remote proctoring methodology. Theory examination would be conducted online, and the paper comprise of MCQ. Conduct of assessment is through trained proctors. Once the test begins, remote proctors have full access to the candidate's video feeds and computer screens. Proctors authenticate the candidate based on registration details, pre-test image captured and I- card in possession of the candidate. Proctors can chat with candidates or give warnings to candidates. Proctors can also take screenshots, terminate a specific user's test session, or re-authenticate candidates based on video feeds.
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	External Examiners/ Observers (Subject matter experts) are deployed including NIELIT scientific officers who are subject experts for evaluation of Practical examination/ internal assessment / Project/Presentation/ assignment and Major Project (if applicable). Qualification is generally B.Tech.
4.	**Assessment Mode** *(Specify the assessment mode)*	Centralized online examination will be conducted
5.	**Tools and Equipment Required for Assessment**	☒ Same as for training ☐ Yes ☐ No (details to be provided in Annexure-if it is different for Assessment)

Section 4: Evidence of the Need for the Standalone NOS

Provide Annexure/Supporting documents name.

1.	Government /Industry initiatives/ requirement (Yes/No): Yes, Available at Annexure-A: Evidence of Need
2.	Number of Industry validation provided: 3
3.	Estimated number of people to be trained: 500
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): (Yes/No): NIELIT is recognized as AB and AA under Government Category. NIELIT is an HRD arm of MeitY, therefore, the Line Ministry Concurrence is not required.

Section 5: Annexure & Supporting Documents Check List

Specify Annexure Name / Supporting document file name

1.	**Annexure:** NCrF/NSQF level justification based on NCrF/NSQF descriptors *(Mandatory)*	Available at Annexure-I: Evidence of Level
2.	**Annexure:** List of tools and equipment relevant for NOS *(Mandatory, except in case of online course)*	Available at Annexure-II: Tools and Equipment
3.	**Annexure:** Industry Validation	Available at Annexure-III: Industry Validation
4.	**Annexure:** Training Details	Available at Annexure-IV: Training Details
5.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is "Blended Learning")*	Available at Annexure-V: Blended Learning
6.	**Annexure/Supporting Document:** Standalone NOS- Performance Criteria Details Annexure/Document with PC-wise detailing as per NOS format (Mandatory- Public view)	Available at Annexure-VI: Standalone NOS- Performance Criteria details
7.	**Annexure:** Detailed Assessment Criteria *(Mandatory)*	Available at Annexure-VII: Assessment Criteria
8.	**Annexure:** Assessment Strategy *(Mandatory)*	Available at Annexure-VIII: Assessment Strategy

9.	**Annexure:** Acronym and Glossary *(Optional)*	Available at Annexure-IX: Acronym and Glossary
10.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	Available at Annexure-B: Model Curriculum

Annexure-I: Evidence of Level

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Professional Theoretical Knowledge/Process	The quips learners with the professional theoretical knowledge required for a network security specialist role. Graduates will understand fundamental networking principles, cybersecurity landscapes, and the importance of network security in securing digital infrastructures. They will develop expertise in identifying and analyzing network attacks, implementing security mechanisms like firewalls, IDS/IPS, VPNs, and access controls, and applying risk assessment and incident response strategies. Additionally, they will gain insights into penetration testing, vulnerability assessments, and security event management. With exposure to emerging technologies such as AI, Zero Trust, cloud security, and blockchain, learners will be well-prepared to address evolving cybersecurity challenges and design robust defence strategies for modern network environments.	The job role and outcomes align with aligning with NSQF Level 6 or 7, this course ensures that learners achieve a blend of technical mastery, professional competencies, and problem-solving skills, making them employment-ready professionals and potential cybersecurity entrepreneurs. It provides a pathway for career growth, industry certification, and further academic progression, supporting roles in network security, network defence.	**5**
Professional and Technical Skills/ Expertise/ Professional Knowledge	course develops both professional and technical skills required for a network security specialist role. Learners will gain hands-on expertise in configuring and managing firewalls, IDS/IPS systems, VPNs, and access control mechanisms to protect network infrastructures. They will acquire practical skills in network traffic analysis, vulnerability assessments, penetration testing, and incident response planning using industry-standard tools like Wireshark, Nmap, and SIEM solutions. Additionally, they will develop competencies in simulating cyberattacks, capturing attack traffic, and implementing security policies to mitigate threats. With exposure to emerging cybersecurity trends such as AI-driven security, Zero Trust architecture, cloud security, and blockchain-based protection	Factual knowledge of field of knowledge or study.	**5**

	mechanisms, learners will be equipped with cutting-edge skills to defend modern networks against evolving cyber threats.		
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	This qualification prepares learners for employment readiness and entrepreneurship by developing a strong cybersecurity skillset and a proactive problem-solving mindset. Graduates will be equipped with technical expertise in network security, attack prevention, incident response, penetration testing, and security management, making them industry-ready for roles such as network security specialists, cybersecurity analysts, and ethical hackers. Additionally, they will cultivate analytical thinking, risk assessment capabilities, and adaptability to emerging technologies like AI and blockchain. For entrepreneurship, learners will gain insights into cybersecurity consulting, managed security services, and developing innovative security solutions, enabling them to build and sustain businesses in the growing cybersecurity domain. The course fosters a professional work ethic, attention to detail, and a continuous learning mindset, essential for excelling in the ever-evolving field of network defence.	Recall and demonstrate practical skill, routine and repetitive in narrow range of application, using appropriate rule and tool, using quality concepts	**5**
Broad Learning Outcomes/Core Skill	They will be able to handle alone as well as in /with the team in the area as per the curriculum	Language to communicate written or oral, with required clarity, skill to basic arithmetic and algebraic principles, basic understanding of social political and natural environment.	**5**
Responsibility	This course will be responsible for securing network infrastructures by implementing defence mechanisms such as firewalls, IDS/IPS, VPNs, and access controls. They will actively monitor, detect, and respond to security threats, conduct risk assessments, penetration testing, and vulnerability analysis, and develop incident response and recovery plans to mitigate cyber threats. Additionally, they will be responsible for analyzing attack vectors, understanding cybersecurity trends, and leveraging technologies like AI, Zero Trust, and blockchain to enhance security frameworks. Ensuring compliance with industry standards, maintaining security logs, and effectively utilizing Security Information and Event Management (SIEM) tools will also be key responsibilities in safeguarding organizational networks against evolving cyber threats.	Responsibility for own work and learning.	**5**

Annexure-II: Tools and Equipment (lab set-up)

List of Tools and Equipment
Batch Size: 30

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	Classroom	1 (30 Sq.m)	30
2	Student Chair		30
3	Student Table		30
4	Desktop computer with accessories	• 12th Generation Intel® Core™ i5-12500T with Intel vPro® Enterprise • 8 GB DDR4-3200 MHz RAM (1 x 8 GB) • 512 GB PCIe® NVMe™ M.2 SSD • Intel® UHD Graphics 770 • Windows 11 Professional	30
5	Deskjet printer	1 No.	A4

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. LCD Projector/Smart Board
2. Pin-up Board
3. White Board, Markers

Annexure-III: Industry Validations Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID
1	Tripura University (A Central University)	Prof. Swanirbhar Majumder	Professor, Head of the Department, Department of Information Technology	Suryamaninagar, Tripura(W) Pin: 799022	9436229406	hod_it@tripurauniv.ac.in
2	NATIVEDEFENCE	Bishwajit Sutradhar	Director Cybersecurity Sales & Alliances	D-311 Ganesh Glory 11, Jagatpur Rd, Near BSNL Office, Off S G Highway, Jagatpur, Ahmedabad, Gujarat 382470	9748780073	bishwajit@nativesoc.com
3	Trend Micro India Pvt. Ltd.	Kanchan Mallick	Sr. Regional Account	10th floor, EROS Corporate Tower, Nehru Place, New Delhi – 110019	9903003292	-

Annexure-IV: Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training # of Women	Estimated training # of People with Disability
2025	100	50	10
2026	200	70	15
2027	200	70	15

Data to be provided year-wise for next 3 years.

Annexure-V: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools: NA

Annexure-VI: Performance Criteria details

1. **Description:**
   This course provides a comprehensive understanding of protecting networks from cyber threats through a blend of theoretical knowledge and hands-on practical training. It begins with the fundamentals of networking and the role of network defence, emphasizing its importance in today's cybersecurity landscape. Students explore various network attacks, including real-world case studies and attack simulations. The course delves into core security principles, such as configuring firewalls, VPNs, IDS/IPS systems, and secure access controls. It also covers network defence strategies, including risk assessment, incident response planning, penetration testing, and using SIEM tools. Finally, students learn about emerging trends in cybersecurity, including AI-based threat detection, the Zero Trust security model, cloud security, and blockchain technology, equipping them with up-to-date knowledge for real-world applications.

2. **Scope:**

The scope covers the following:

- This course covers foundational network security principles, common attack types, and defence mechanisms such as firewalls, IDS/IPS, VPNs, and access controls.
- It provides hands-on training in attack simulations, vulnerability assessments, incident response, and SIEM tools.
- It explores emerging trends like AI-driven security, zero-trust models, cloud security, and blockchain in network defence.

3. **Elements and Performance Criteria**

To be competent, the user/individual on the job must be able to:

Introduction to Network

PC1. Demonstrate understanding of fundamental networking concepts relevant to security management.

PC2. Explain the importance of network security and describe the key threats in the cybersecurity landscape.

Types of Network Attacks

PC3. Identify and explain common attack types (e.g., DoS/DDoS, Phishing, Malware, Man-in-the-Middle).

PC4. Analyze case studies of real-world network attacks.

Network Security Fundamentals

PC5. Configure and manage firewall rules to control network traffic based on security policies.

PC6. Implement Virtual Private Network (VPN) solutions to ensure secure remote communications.

Network Security Strategies

PC7. Identify and assess potential threats and vulnerabilities using established threat analysis and risk assessment methodologies to determine security risks.

PC8. Develop and implement effective incident response, recovery plans, and security testing procedures

Emerging Trends and Technologies in Network Security

PC9. Exploring AI-based threat detection tools.

PC10. Explain the core principles of the Zero Trust Security Model and apply them to design secure enterprise networks.

PC11. Identify key security challenges in cloud environments and remote work scenarios, and implement appropriate mitigation strategies.

4. Knowledge and Understanding (KU):

The individual on the job needs to know and understand:

KU1. Develop a solid understanding of network security principles, attack methodologies, and defence strategies.

KU2. Gain practical experience in configuring security tools, analyzing threats, and implementing secure network solutions.

KU3. Explore emerging technologies like AI, zero-trust security, and blockchain to address modern cybersecurity challenges.

5. Generic Skills (GS):

User/individual on the job needs to know how to:

GS1. Follow instructions, guidelines and procedures

GS2. Listen effectively and communicate information accurately

GS3. Apply formatting features to achieve the desired results

Annexure-VII: Assessment Criteria

Detailed PC-wise assessment criteria and assessment marks for the NOS are as follows:

NOS/Module Name	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks	Project Marks	Viva Marks
Essentials of Network Security Measures **NOS Code: NIE/ITS/N0917**	**Introduction to Network:** **PC1.** Demonstrate understanding of fundamental networking concepts relevant to security management. **PC2.** Explain the importance of network security and describe the key threats in the cybersecurity landscape.	20	10	4	4
	Types of Network Attacks: **PC3.** Identify and explain common attack types (e.g., DoS/DDoS, Phishing, Malware, Man-in-the-Middle). **PC4.** Analyze case studies of real-world network attacks.	20	15	4	4
	Network Security Fundamentals: **PC5.** Configure and manage firewall rules to control network traffic based on security policies. **PC6.** Implement Virtual Private Network (VPN) solutions to ensure secure remote communications.	20	15	4	4
	Network Security Strategies: **PC7.** Identify and assess potential threats and vulnerabilities using established threat analysis and risk assessment methodologies to determine security risks.	20	10	4	4

	PC8. Develop and implement effective incident response, recovery plans, and security testing procedures				
	Emerging Trends and Technologies in Network Security: **PC9.** Exploring AI-based threat detection tools. **PC10.** Explain the core principles of the Zero Trust Security Model and apply them to design secure enterprise networks. **PC11.** Identify key security challenges in cloud environments and remote work scenarios, and implement appropriate mitigation strategies.	20	10	4	4
Total Marks		**100**	**60**	**20**	**20**

Annexure-VIII: Assessment Strategy

This section includes the processes involved in identifying, gathering, and interpreting information to evaluate the Candidate on the required competencies of the program.

Assessment of the qualification evaluates candidates to ascertain that they can integrate knowledge, skills and values for carrying out relevant tasks as per the defined learning outcomes and assessment criteria.

The underlying principle of assessment is fairness and transparency. The evidence of the outcomes and assessment criteria. competence acquired by the candidate can be obtained by conducting Theory (Online) examination.

About Examination Pattern:

1. The question papers for the theory exams are set by the Examination wing (assessor) of NIELIT HQS.
2. The assessor assigns roll number.
3. The assessor carries out theory online assessments. Theory examination would be conducted online and the paper comprise of MCQ
4. Pass percentage would be 50% marks.
5. The examination will be conducted in English language only.

Quality assurance activities: A pool of questions is created by a subject matter expert and moderated by other SME. Test rules are set beforehand. Random set of questions which are according to syllabus appears which may differ from candidate to candidate. Confidentiality and impartiality are maintained during all the examination and evaluation processes.

Annexure-IX: Acronym and Glossary

Acronym

Acronym	Description
AA	Assessment Agency
AB	Awarding Body
NCrF	National Credit Framework
NOS	National Occupational Standard(s)
NQR	National Qualification Register
NSQF	National Skills Qualifications Framework

Glossary

Term	Description
National Occupational Standards (NOS)	NOS define the measurable performance outcomes required from an individual engaged in a particular task. They list down what an individual performing that task should know and also do.
Qualification	A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards
Qualification File	A Qualification File is a template designed to capture necessary information of a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification.
Sector	A grouping of professional activities on the basis of their main economic function, product, service or technology.