QUALIFICATION FILE–Standalone NOS

Fundamentals of Information Security

☐ 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: 4

Submitted By:

National Institute of Electronics and Information Technology

**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

1.	**NOS-Qualification Name**	**Fundamentals of Information Security**	
2.	**Sector/s**	**IT-ITeS**	
3.	**Type of Qualification ☐ New ☒ Revised**	**NQR Code & version of the existing /previous qualification: 2022/EHW/NIELIT/05322**	**Qualification Name of the existing/previous version:** Foundation course in Information Security
4.	**National Qualification Register (NQR) Code & Version** *(Will be issued after NSQC approval.)*	NG-04-IT-04417-2025-V2-NIELIT	**5. NCrF/NSQF Level: 4**
6.	**Brief Description of the Standalone NOS**	The purpose of this qualification is to equip students with skills in Information Security, enhancing their employability in the IT and Computer Science fields. The aim is to demystify Information Security and empower the future workforce with the confidence to independently learn and apply these essential skills.	

7.	**Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee**	a. **Entry Qualification &Relevant Experience:**	

S. No.	Academic/Skill Qualification (with Specialization - if applicable)	Relevant Experience (with Specialization - if applicable)
1	12th with Science subjects or equivalent	No Experience required
2	2nd year of 3-year diploma in CS/IT/EC/EE/allied branches after10th	
3	Previous relevant Qualification of NSQF Level 3.5	1.5 year of experience in IT or allied sector
4	Previous relevant Qualification of NSQF Level 3	3 year of experience in IT or allied sector

8.	**Credits Assigned to this NOS-Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	**3 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)*	NA	

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 Only** ☐ **Online Only** ☐ **Blended**			
		Training Delivery Mode	**Theory (Hours)**	**Practical (Hours)**	**Total (Hours)**
		Classroom (offline)	**35**	**55**	**90**

12.	**Assessment Criteria**						
		Theory (Marks)	**Practical (Marks)**	**Employability Skills/Internal Assessment (Marks)**	**Project/OJT (Marks)**	**Total (Marks)**	**Passing %age**
		100	25	00	00	125	50

The centralized 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:** i. Locomotor Disability: Leprosy Cured Person, Dwarfism, Muscular Dystrophy and Acid Attack Victims ii. Visual Impairment: Low Vision

14.	**Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)*	**Professional:**
		 Information Security Associate
		 Academic:
		 i)Horizontal:
		   NSQF level 4 Courses in the area of Cyber Security, Information Security Tools, Networking
		 ii)Vertical:
		   After completion of this course, students can go for higher studies in the area Cyber Security and Cyber Forensics

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: Ankit Kumar** **Email: ankit@nielit.gov.in** **Contact No.: 9074841785** **Website:** https://www.nielit.gov.in	
19.	**Final Approval Date by NSQC: 08.05.2025**	**20. Validity Duration: 3 Years**	**21. 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 (IT)/MCA/ B.E/B. Tech in CS/IT/EC/EE/ allied areas with 1 year of relevant experience in training (cyber security).
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	MCA/B-Level (IT)/B.E/B. Tech in CS/IT/EC/EE/ allied areas with an relevant experience of 3 years 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)*	B.E/B. Tech in CS/IT/EC/EE/allied areas with 3 year of relevant experience.
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)*	An External Examiner/ Observer (Subject matter expert) are deployed including NIELIT scientific officers who are subject expert 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)*	Online for Theory. Online/Offline for other assessments.
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
2.	Number of Industry validation provided: 6
3.	Estimated number of people to be trained: 8640
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): (Yes/No): 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: Training Details**	Available at Annexure-IV: Training Details
4.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is Blended Learning)*	Available at Annexure-V: Blended Learning
5.	**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
6.	**Annexure:** Performance and Assessment Criteria*(Mandatory)*	Available at Annexure-VII: Detailed Assessment Criteria
7.	**Annexure:** Assessment Strategy*(Mandatory)*	Available at Annexure-VIII: Assessment Strategy
8.	**Annexure:** Acronym and Glossary *(Optional)*	Available at Annexure-IX: Acronym and Glossary
9.	**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	1. The job holder is expected to know the different frameworks and tools available for implementing cyber security measures, including network security, application security, and endpoint protection. 2. Knowledge of cyber security components such as firewalls, IDS/IPS, SIEM, and encryption protocols. 3. Develop the ability to analyze security alerts and logs to identify potential threats. 4. Develop, implement, and enforce security policies and procedures. 5. Evaluate the effectiveness of existing security measures and identify areas for improvement. 6. Stay updated with the latest security trends and technologies to enhance the organization's security posture.	• Possesses specialized operational knowledge and understanding of the work. • Have complete knowledge of the concept of time required for delivery; and Quality for a range of issues	4
Professional and Technical Skills/ Expertise/ Professional Knowledge	1. The candidate will be able to understand and utilize various security tools such as firewalls, IDS/IPS, SIEM, and encryption software. 2. Understand various data analysis techniques to identify potential security threats. 3. Ability to interpret security logs and alerts to detect and respond to incidents. 4. Develop the ability to troubleshoot and resolve security issues effectively. 5. The project will help in applying cyber security techniques to solve real-world security problems.	• Possesses specialized professional and technical skills; displays clarity of professional knowledge and technical skills in a broad range of activities/ tasks. • Have knowledge of collecting and interpreting the available information, drawing conclusions & communicating the same	4

Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	1. Career Development & Goal Setting 2. Communication Skills 3. Essential Digital Skills 4. Getting Ready for Apprenticeship & Jobs	• Can explain Entrepreneurial Mindset and describe the importance of it in the context of opportunity curation for future jobs • Can comfortably use most of the basic software with proficiency • Have the ability to relate to the 5 pillars of Social Emotional Skills and describe the similarities between SES and Emotional Intelligence.	4
Broad Learning Outcomes/Core Skill	1. Threat Detection and Response 2. Security Policy Implementation 3. Risk Management and Compliance 4. Continuous Improvement	• Students are able to know various types of threats and vulnerabilities • Have knowledge of Incident management and implementation of cyber security solution	4
Responsibility	1. Implementation of Security Solutions 2. Incident Management 3. Project Realization in Security Domains	Takes complete responsibility for delivery and quality of own work and output as also the subordinates.	4

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	30
3	Student Table	30	30
4	Desktop computer with accessories	Installed with: Virtual Kali Linux OS, Virtual Windows 10, 11 OS, Nmap, Wireshark,Firefox, OpenVas, Syslog, Autopsy, FTK Imager, Windows Firewall, iptables, Snort, sqlmap, jsql, Burpsuite, Nessus, Metasploit, Splunk, Axiom, SolarWinds, IDA.	30
5	Desk jet printer	1 Nos.	A4

Classroom Aids
The aids required to conduct sessions in the classroom are:

1. LCD Projector

2. Pin-up Board

3. White Board

Annexure-III: Industry Validations Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID
1	Sidhi Vinayak Academy	Tausif Alam	State Head	Shiv Narayan Kunj, B – Block, Shivaji Nagar, Hethu, Ranchi (JH)	8789326361	info.sidhiacadmey@gmail.com
2	Programmers Point,	Smt. Bela Rani Saha	Propritor	Ujan Abhoynagar, Manipuripara, Agartala, Tripura(West), Pin-799005	0381-3561096	programmerspoint.help@gmail.com
3	Software World	Akula	Founder	Ujan Abhoynagar, Manipuripara, Agartala, Tripura(West),	0381-7963527	www.softwareworld.co.in
4	POWER FORENSICS & DIGITAL INTELLIGENCE	Naveen Kumar Singh	Director	PROPERTY NO-101, 1ST FLOOR, ABOVE BANK OF BARODA, VILLAGE-PATPARGANJ, MAYUR VIHAR PHASE-1, NEW DELHI-110091,	+919958441173	info@powerforensics.in
5	Bankify Technologies Pvt Ltd	Rojalini Gouda	HR Executive	DCB 620, 6th Floor DLF Cybersecurity Infocity Square, Bhubaneswar, Odisha	9124653503	Rojalini@bankify.money
6	Lamzing Technologies Private Limited	Ailan Maibam	Managing Director	Software Technology Park of India, G- Floor, MIMS Building, Manipur University, Canchipur	9963382225	cantact@lamzing.com

Annexure-IV: Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training# of Women	Estimated training# of People with Disability
2025-26	2640	700	100
2026-27	3000	1200	150
2027-28	3000	1200	150

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

Annexure-V: Blended Learning

Blended Learning Estimated Ratio &Recommended Tools: NA

Annexure-VI: Standalone NOS- Performance Criteria details

1. Description:

This course offers a thorough understanding of fundamental concepts and practices in information security. Participants will gain hands-on experience with essential tools and techniques to protect data and systems from unauthorized access, breaches, and other security threats, ensuring a secure and compliant IT environment.

2. Scope:

The scope covers the following:

● Enhances career prospects by preparing individuals for roles in cybersecurity, IT security, and risk management.

● Equips participants to protect and manage information assets effectively, making them valuable assets in safeguarding organizational data.

● Extends to opportunities in securing various IT environments, understanding threat landscapes, and implementing robust security measures.

3. Elements and Performance Criteria

Elements	Performance Criteria
Understand the Fundamentals of Cyber Security and Threat Landscape	**PC1:** Explain the concept of the cyber world, types of cyber threats, and the importance of privacy on the Internet. **PC2:** Identify various types of cyberattacks including phishing, malware, ransomware, spyware, and deepfake attacks. **PC3:** Describe the different phases of hacking and recognize preventive measures for each phase.
Apply Security Measures for Devices, Networks, and Applications	**PC4:** Demonstrate methods to secure wireless networks and operating systems using built-in security settings, antivirus software, and file/folder protection techniques. **PC5:** Explain and configure firewalls, analyze logs, and implement application-level security controls. **PC6:** Identify and apply best practices for securing emails, social media accounts, digital payment platforms, and IoT devices.
Explore Advanced Cybersecurity Concepts and Emerging Technologies	**PC7:** Understand and explain the principles of cryptography and their application in data protection. **PC8:** Discuss the basics of cloud security, hardware security, and the risks associated with generative AI technologies such as deepfake attacks. **PC9:** Explain the role of cyber forensics and demonstrate the importance of log analysis in investigating cyber incidents.

4. Knowledge and Understanding (KU):

The individual on the job needs to know and understand:

KU1: Core concepts and principles of information security, including threat modeling, risk management, and security controls.

KU2: Regulatory requirements and industry standards related to information security, ensuring compliance and best practices.

KU3: Security technologies and tools, including their implementation, management, and role in protecting information systems.

KU4: Incident response strategies and procedures, including techniques for analyzing and managing security incidents effectively.

5. Generic Skills (GS):

The user/individual on the job needs to know how to:

GS1: Follow instructions, guidelines, and procedures related to information security, ensuring adherence to best practices and standards.

GS2: Communicate information clearly and accurately, including security protocols, risk assessments, and incident reports.

GS3: Apply formatting features to create secure and compliant documentation, ensuring clarity and accuracy in security-related materials.

Annexure-VII: Assessment Criteria

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

Elements	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks
Understand the Fundamentals of Cyber Security and Threat Landscape	**PC1.** Explain the concept of the cyber world, types of cyber threats, and the importance of privacy on the Internet. **PC2.** Identify various types of cyberattacks including phishing, malware, ransomware, spyware, and deepfake attacks. **PC3.** Describe the different phases of hacking and recognize preventive measures for each phase.	35	5
Apply Security Measures for Devices, Networks, and Applications	**PC4.** Demonstrate methods to secure wireless networks and operating systems using built-in security settings, antivirus software, and file/folder protection techniques. **PC5.** Explain and configure firewalls, analyze logs, and implement application-level security controls. **PC6.** Identify and apply best practices for securing emails, social media accounts, digital payment platforms, and IoT devices.	40	15
Explore Advanced Cybersecurity Concepts and Emerging Technologies	**PC7.** Understand and explain the principles of cryptography and their application in data protection.	25	5

	PC8. Discuss the basics of cloud security, hardware security, and the risks associated with generative AI technologies such as deepfake attacks. **PC9**. Explain the role of cyber forensics and demonstrate the importance of log analysis in investigating cyber incidents.		
		100	25
	Total Marks	**125**	

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.