QUALIFICATION FILE–Standalone NOS

Essentials of Embedded 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: 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

<table>
<tr><td>1.</td><td>NOS-Qualification Name</td><td colspan="2">Essentials of Embedded Security</td></tr>
<tr><td>2.</td><td>Sector/s</td><td colspan="2">Electronics</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</td><td>NG-05-EH-02900-2024-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 NOS provides a comprehensive introduction to embedded system security, covering key challenges and threats, the importance of security, and the distinction between safety and security. It delves into threat modeling, risk assessment, and secure coding practices to address common vulnerabilities.</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>Relevant Experience (with Specialization - if applicable)</th></tr>
<tr><td>1</td><td>2nd year of UG in Electronics and Communication Engineering/ Electrical Engineering/CS/IT/Physics/Electronics and allied branches</td><td>NA</td></tr>
<tr><td>2</td><td>3 Years of Diploma in Electronics and Communication Engineering/ Electrical Engineering/CS/IT/Physics/Electronics and allied branches after class 10th</td><td>1.5 Years</td></tr>
<tr><td>3</td><td>2 Year of diploma in Electronics and Communication Engineering/ Electrical Engineering/CS/IT/Physics/Electronics and allied branches after class 12th</td><td>NA</td></tr>
<tr><td>4</td><td>NSQF Level 4.5 in Electronics and Communication Engineering/ Electrical Engineering/CS/IT/Physics/Electronics and allied branches</td><td>1.5 Years</td></tr>
<tr><td>5</td><td>NSQF Level 4 Electronics and Communication Engineering/ Electrical</td><td>1.5 Years</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>Engineering/CS/IT/Physics/Electronics and allied branches</td><td></td></tr>
</table>
b. Age:18 years
</td></tr>
<tr><td>8.</td><td>Credits Assigned to this NOS-Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>2 Credits</td><td>9. Common Cost Norm Category (I/II/III) (wherever applicable):

Category I (Electronics System Design)</td></tr>
<tr><td>10.</td><td>Any Licensing Requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
<tr><td>11.</td><td>Training Duration by Modes of Training Delivery (Specify Total Duration as per selected training delivery modes and as per requirement of the qualification)</td><td colspan="2">☒Offline ☐ Online ☐ Blended
<table>
<tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>Total (Hours)</th></tr>
<tr><td>Classroom (offline)</td><td>30</td><td>30</td><td>60</td></tr>
</table>
Training shall be conducted in any of the 3 modes depending on the regional need.

(Refer Blended Learning Annexure-V for details)</td></tr>
<tr><td>12.</td><td>Assessment Criteria</td><td colspan="2">
<table>
<tr><th>Theory (Marks)</th><th>Practical (Marks)</th><th>Project/ Presentation /Assignment (Marks)</th><th>Viva/ Internal Assessment (Marks)</th><th>Total (Marks)</th><th>Passing %age</th></tr>
<tr><td>100</td><td>60</td><td>20</td><td>20</td><td>200</td><td>50</td></tr>
</table>
The centralized online assessment is conducted by the Examination Wing, NIELIT Headquarters.</td></tr>
<tr><td>13.</td><td>Is the NOS Amenable to Persons with Disability</td><td colspan="2">☒ Yes ☐ No
If “Yes”, specify applicable type of Disability:

a. Locomotor Disability: Leprosy Cured Person, Dwarfism, Muscular Dystrophy and Acid Attack Victims
b. Visual Impairment: Low Vision</td></tr>
<tr><td>14.</td><td>Progression Path After Attaining the Qualification, wherever applicable</td><td colspan="2">Embedded Software Engineer</td></tr>
</table>

15.	**How will the participation of women 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**	
18.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In the case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name:** Rajesh M **Email:** rajesh.m@nielit.gov.in **Website:** https://nielit.gov.in/ **Name:** Anirban Jyoti Hati **Email:** anirban@nielit.gov.in **Website:** https://nielit.gov.in/ **Name:** Ankit Kumar **Email:** ankit@nielit.gov.in **Website:** https://nielit.gov.in/	
19.	**Final Approval Date by NSQC: 25.07.2024**	**20. Validity Duration: 3 years**	**21. Next Review Date: 25.07.2027**

Section 2: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years) (as per NCVET guidelines)**	B.E./B. Tech in Electronics/ Electronics & Communication/ Electrical/ Electrical and Electronics/Instrumentation/ Electronics & Instrumentation / Instrumentation & Control /Computer Science/Information Technology Minimum 2 year of experience in the field of Embedded Systems Development
2.	**Master Trainer's Qualification and experience in the relevant sector (in years) (as per NCVET guidelines)**	B.E./B. Tech in Electronics/ Electronics & Communication/ Electrical/ Electrical and Electronics/Instrumentation/ Electronics & Instrumentation / Instrumentation & Control /Computer Science/Information Technology Minimum 3 year of experience in the field of Embedded Systems Development
3.	**Tools and Equipment Required for the Training**	☒ Yes ☐No Available at Annexure-II
4.	**In Case of Revised NOS, details of Any Upskilling Required for Trainer**	Not Applicable

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	B.Tech or Equivalent as per NCrF + 3 years 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 comprises 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

Section 4: Evidence of the Need for the Standalone NOS

1.	Government /Industry initiatives/ requirement (Yes/No): Yes, Available at Annexure-A: Evidence of Need
2.	Number of Industry validations provided: 8
3.	Estimated number of people to be trained: 500 persons per year shall be trained.
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): 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.
5.	Latest Skill Gap Study (not older than 2 years) (Yes/No): Yes, Available in Annexure-A: Evidence of Need
6.	Latest Market Research Reports or any other source (not older than 2 years) (Yes/No): Yes, Available at Annexure-A: Evidence of Need

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 the 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:** Performance and Assessment Criteria *(Mandatory)*	*Available at* Annexure-VII: Detailed 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	*Available at* Annexure-C: 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	• Candidates should demonstrate a strong understanding of threat modeling and risk assessment principles in the context of embedded systems security. • In-depth knowledge of secure coding best practices, understanding of programming languages commonly used in embedded systems, familiarity with secure coding guidelines and standards. • Competence in cryptography fundamentals and their application in embedded systems, including symmetric and asymmetric encryption algorithms.	• Candidates need to grasp the foundational concepts of threat modeling and risk assessment, including identifying potential security threats, evaluating risks, and prioritizing mitigation strategies. • Theoretical knowledge in threat modeling guides the process of assessing and prioritizing threats, analyzing risks, and developing mitigation strategies for embedded systems. • Theoretical knowledge of cryptography enables individuals to apply encryption techniques to protect sensitive information in embedded systems.	5
Professional and Technical Skills/ Expertise/ Professional Knowledge	• Expertise in writing secure code for resource-constrained environments, ensuring robust and resilient embedded systems. • Skill in securing wireless communication and implementing authentication mechanisms for secure data transmission. • Competence in designing and implementing secure embedded system architectures, including secure boot and firmware integrity mechanisms.	• This outcome requires proficiency in optimizing code for memory and performance in resource-constrained embedded systems. • Technical skills in securing wireless communication involve implementing encryption algorithms, and authentication mechanisms to safeguard data exchanged wirelessly in embedded systems. • Designing secure embedded system architectures requires expertise in secure boot mechanisms, firmware integrity checks, isolation of critical components, and secure communication interfaces within the system.	5
Employment Readiness & Entrepreneurship Skills & Mind-	• Demonstrate a deep understanding of the various security challenges and threats specific to embedded systems.	• Equip candidates with the knowledge to identify and address unique security issues in embedded systems, making them valuable assets to potential employers. • Empower entrepreneurs to build robust security	5

set/Professional Skill	• Conduct comprehensive security testing and vulnerability assessments to identify and mitigate potential security issues. • Develop secure embedded solutions that address both safety and security requirements, enhancing the marketability and reliability of the product.	protocols into their products, fostering trust and credibility with customers and stakeholders. • Enable entrepreneurs to develop and market reliable and secure products, ensuring compliance with safety and security regulations and boosting product appeal and marketability.	
Broad Learning Outcomes/ Core Skill	• Proficiency in secure coding best practices, such as preventing buffer overflows and format string vulnerabilities, is essential for Embedded Software Developers focusing on security. • The ability to identify potential security threats, assess risks, and develop effective strategies to mitigate security vulnerabilities in embedded systems is crucial for an Embedded System Security Engineer. • The ability to architect secure embedded systems involves designing secure boot processes, implementing secure memory management techniques, and establishing secure communication protocols.	• Secure coding is a fundamental core skill for Embedded Software Developers focusing on security. It involves understanding and implementing coding practices that prevent common vulnerabilities like buffer overflows, format string vulnerabilities, and input validation issues. • The ability to identify potential security threats, conduct risk assessments, and formulate mitigation strategies is a foundational skill for Embedded System Security Engineers. • Designing secure embedded systems involves core skills such as developing secure boot processes, implementing secure memory management techniques, and establishing secure communication protocols.	5
Responsibility	• The primary responsibility of the job role would be designing, developing, and implementing secure embedded systems. • Another key responsibility would involve implementing secure communication protocols and authentication mechanisms to safeguard data transmission and protect the integrity of the embedded system. • The candidate would be responsible for evaluating the effectiveness of security measures, addressing any identified vulnerabilities, and ensuring compliance with security standards and regulations relevant to embedded system security.	• The primary responsibility of designing, developing, and implementing secure embedded systems is central to ensuring the integrity, confidentiality, and availability of embedded devices and systems. • Evaluating the effectiveness of security measures, addressing vulnerabilities, and ensuring compliance with security standards and regulations are key responsibilities for maintaining the security posture of embedded systems.	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 (750 Sq. ft to 1000 Sq. ft.)	30
2	Students Chair	30	30
3	Students Table	15 (2 students sharing 1 table)	15
4	Desktop computer with accessories / Laptop	Laptop with minimum specifications: Intel I3 or Celeron processor with at least 8GB RAM, 512GB SSD Hard disk integrated with graphics card, Display size 15.6-inch, Wi-Fi connectivity and Wired Optical Mouse	15
5	Internet Connectivity	Seamless internet connectivity with at least 100 Mbps without firewall	
6	Development Board & Tools	Development boards, secure bootloaders, cryptography libraries, communication modules (e.g., Wi-Fi, Bluetooth), security testing tools (e.g., static code analyzers, vulnerability scanners), and access to relevant documentation and standards.	15

Classroom Aids for offline and blended mode of training:

The aids required to conduct sessions in the classroom are:

1. LCD Projector/Smart Board

Annexure III: Industry Validations/ Government Recognition Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID
1	Aajivika Global Skill Private Limited	Mukesh Kumar Verma	Director	Beside Vishal Trade, dasmile chowk, Khunti Road Ranchi, Jharkhand-835221	9507952882	aajivikaglobal@gmail.com
2	AISECT Ltd.	Teena Panthi	Assistant Manager	AISECT Ltd. 1-1-387, 3rd floor, Flat No. 403/404, GNR Heights, Above SBI,Bakaram Road, Musheerabad, Hydrabad-500020	7879982075	Teena.panthi@aisect.org
3	B. G. Infotech	Amal Das	Centre Head	Kakdihi, Mecheda, Purba, Medinipur	9434996748	Bginfotech2007@gmail.com
4	Devendra Nath Institute of Information Mation Technology (DNIIT)	Amit Kumar Tripathy	Director	Uska Road, Near Naveen Sabji Mandi, Tetari Bazar, Siddharth Nagar-272207	8765562815	aktjob@gmail.com
5	Inditech Software Wizard Pvt. Ltd.	Sandip Ghosh	Course Coordinator	Mohiari Chanpiritala, Po: Andul Mouri, PS: Domjur, Distt: Howrah, West Bengal-711302	9230027415	swizardrecruitment@gmail.com
6	Prasanthi Polytechnic	D. Prasad	Principal	Duppituru (Vill), Atchutapuram (Md). Visakhapatnam (Dist), Andhara Pradesh-531011	9849952573	prasadreddy.1279@gmail.com
7	Sidhi Vinayak Academy	Neha Verma	Director	Shiv Narayan Kunj, B Block, Shivaji Nagar, Hethu, Ranchi, JH-834002	8789837772	sidhiacadmey@gmail.com
8	Surekha IT Services	Anjani K	Manager	8-3-191/84/302, Sharan Residency, Vengalrao Nagar, Hyderabad-500038, Telangana	8125134134	info@surekhaitservices.com

Annexure IV: Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training# of Women	Estimated training# of People with Disability
2024-25	500	200	20
2025-26	500	200	20
2026-27	1000	200	20

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

Annexure V: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools:

S. No.	Select the Components of the Qualification	List Recommended Tools – for all Selected Components	Offline : Online Ratio
1	Theory/ Lectures - Imparting theoretical and conceptual knowledge	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	70:30
2	Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	70:30
3	Showing Practical Demonstrations to the learners	Through Virtual Software and Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	70:30
4	Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	Through Virtual Software and Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	70:30
5	Tutorials/ Assignments/ Drill/ Practice	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	70:30
6	Proctored Monitoring/ Assessment/ Evaluation/ Examinations	NIELIT Remote Proctored Software	Online: 100% Theory Offline: 100% Practical
7	On the Job Training (OJT)/ Project Work Internship/ Apprenticeship Training	Virtual Software Platform	Either 100% online in a virtual environment Or 100% offline in the Industry.

Annexure VI: Standalone NOS- Performance Criteria details

1. Description

This NOS provides a comprehensive introduction to embedded system security, covering key challenges and threats, the importance of security, and the distinction between safety and security. It delves into threat modeling, risk assessment, and secure coding practices to address common vulnerabilities.

2. Scope

The scope of this course encompasses a thorough exploration of embedded system security, including understanding security challenges and threats, risk assessment, and secure coding practices.

3. Elements and Performance Criteria

Threat Modeling and Risk Assessment:

- Students can demonstrate the ability to identify and categorize potential security threats specific to embedded systems based on industry-relevant examples.
- Students can Conduct a comprehensive risk assessment for a given embedded system scenario, including analyzing the impact of identified threats and vulnerabilities.
- Students can develop a detailed risk mitigation strategy that effectively addresses the identified risks, prioritizes vulnerabilities, and aligns with security best practices.

Secure Coding Practices:

- Students can apply secure coding techniques to write code that effectively prevents common vulnerabilities such as buffer overflows, integer overflows, and format string vulnerabilities in embedded systems.
- Students can demonstrate the ability to optimize code for resource-constrained embedded environments while ensuring security best practices are maintained.
- Students can evaluate and refactor existing code snippets to identify and rectify security flaws, ensuring compliance with secure coding guidelines and industry standards.

Secure Communication Protocols:

- Students can Implement secure communication protocols for wireless environments in a simulated embedded system setup, ensuring data confidentiality and integrity.
- Students can Design and deploy authentication mechanisms to authenticate communication endpoints and establish secure data transmission channels in embedded systems.
- Students can demonstrate proficiency in configuring and testing encryption protocols within embedded systems to safeguard information exchanged over communication channels.

4. **Knowledge and Understanding (KU):**

The individual on the job needs to know and understand:

- Knowledge of threat modeling methodologies and risk assessment techniques.
- Understanding of attack vectors and the threat landscape relevant to embedded systems.
- Familiarity with techniques for secure memory management and writing secure code in resource-constrained environments.
- Understanding of key management practices and cryptographic techniques for ensuring data confidentiality, integrity, and authenticity in embedded systems.

5. Generic Skills (GS):

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

- Critical Thinking: Ability to analyze complex security challenges in embedded systems, assess risks, and develop effective solutions.
- Problem-Solving: Skill in identifying security vulnerabilities, implementing secure coding practices, and addressing potential threats.
- Communication: Ability to communicate security concepts, risks, and mitigation strategies effectively to diverse stakeholders, including technical and non-technical audiences.
- Collaboration: Capability to work collaboratively in multidisciplinary teams to design and implement secure embedded systems solutions.

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 /Presentation /Assignment Marks	Viva/ Internal Assessment (Marks)
NOS1:Essentials of Embedded Security **NOS Code: NIE/ELE/N0231**	*Threat Modeling and Risk Assessment:*	**30**	**20**	-	**6**
	• Students can demonstrate the ability to identify and categorize potential security threats specific to embedded systems based on industry-relevant examples.	-	-	-	-
	• Students can Conduct a comprehensive risk assessment for a given embedded system scenario, including analyzing the impact of identified threats and vulnerabilities.	-	-	-	-
	• Students can develop a detailed risk mitigation strategy that effectively addresses the identified risks, prioritizes vulnerabilities, and aligns with security best practices.	-	-	-	-
	Secure Coding Practices:	**40**	**20**	-	**7**
	• Students can apply secure coding techniques to write code that effectively prevents common vulnerabilities such as buffer overflows, integer overflows, and format string vulnerabilities in embedded systems.	-	-	-	-
	• Students can demonstrate the ability to optimize code for resource-constrained embedded environments while ensuring security best practices are maintained.	-	-	-	-
	• Students can evaluate and refactor existing code snippets to identify and rectify security flaws, ensuring compliance with secure coding guidelines and industry standards.	-	-	-	-

	Secure Communication Protocols:	**30**	**20**	-	**7**
	• Students can Implement secure communication protocols for wireless environments in a simulated embedded system setup, ensuring data confidentiality and integrity.	-	-	-	-
	• Students can Design and deploy authentication mechanisms to authenticate communication endpoints and establish secure data transmission channels in embedded systems.	-	-	-	-
	• Students can demonstrate proficiency in configuring and testing encryption protocols within embedded systems to safeguard information exchanged over communication channels.	-	-	-	-
		100	**60**	**20**	**20**
	NOS Total	**200**			

Annexure VIII: Assessment Strategy

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), Practical assessment, internal assessment, Project/Presentation/ Assignment, Major Project. The emphasis is on the practical demonstration of skills & knowledge gained by the candidate through the training. Each OUTCOME is assessed & marked separately. A candidate is required to pass all OUTCOMES individually based on the passing criteria.

About Examination Pattern:

1. The question papers for the theory and practical 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 through remote proctoring methodology. Theory examination would be conducted online and the paper comprise of MCQ. Conduct of assessment are through trained proctors. Once the test begins, remote proctors have full access to

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.

4. An External Examiner/ Observer may be deployed including NIELIT officials for evaluation of Practical examination/ internal assessment / Project/ Presentation/. Major Project (if applicable) would be evaluated preferably by external/ subject expert including NIELIT officials.

5. Pass percentage would be 50% marks in each component.

6. Candidates may apply for re-examination within the validity of registration (only in the assessment component in which the candidate failed).

7. For re-examination prescribed examination fee is required to be paid by the candidate only for the assessment component in which the candidate wants to reappear.

8. There would be no exemption for any paper/module for candidates having similar qualifications or skills.

9. 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.