# CCEK – NSQF ALIGNED PROGRAM

# COURSE SYLLABUS

# FOR

# Information and Cyber Security

# CCEK - NATIONAL SKILL DEVELOPMENT TRAINING PROGRAM

## Information and Cyber Security

CCEK – NSDC course package covers the following Qualification Packs and leads to the following NSDC certifications. The students who successfully completed the course programs are entitled to get NSDC certification after undergoing the assessment process of NSDC as per the rules and regulations stipulated by NSDC from time to time.

| SL. NO. | QUALIFICATIONS PACK | QUALIFICATIONS PACK CODE | NSQF LEVEL |
|---|---|---|---|
| 1 | **Analyst Application Security**<br><br>**Brief Job Description**:<br><br>Individuals at this job are responsible for vulnerability assessment for applications, performing source code review, testing the source code, suggesting remediation actions, perform hardening and monitor organizations traffic and logs for threats. | **SSC/Q0903** | **5** |

# COURSE DETAILS

**Information and Cyber Security**

# EXAMINATION DETAILS

| COURSE NAME | COURSE CODE | ELIGIBILITY | DURATION |
|---|---|---|---|
| Information and Cyber Security | G09 | Degree | 320 |

| SL. NO. | EXAM | EXAM CODE | MAXIMUM MARK | INTERNAL | TOTAL MARK |
|---|---|---|---|---|---|
| **THEORY PAPERS** | | | | | |
| 1 | Cyber Threats and Attack Strategies | T001 | 100 | 50 | 150 |
| 2 | Artificial Intelligence in Cyber Security | T002 | 100 | 50 | 150 |
| **PRACTICAL PAPERS** | | | | | |
| 1 | Setting Up a Secure Network Infrastructure | L001 | 100 | 50 | 150 |
| 2 | Building a Security Operations Center | L002 | 100 | 50 | 150 |
| **TOTAL MARKS** | | | | | |
| 1 | Total Examination Marks (THEORY Online + PRACTICAL Examination) | | | | 400 |
| 2 | Total Internal Marks | | | | 200 |
| 3 | **Total Marks (Total Internal Marks + Total Examination Marks )** | | | | **600** |

## Information and Cyber Security

## INTERNAL MARK CRITERIA FOR EACH

| SL NO. | MODULE | MODULE CODE | MAXIMUM MARK | INTERNAL MARK | TOTAL MARK |
|---|---|---|---|---|---|
| 1 | Cyber Threats and Attack Strategies | T001 | 100 | 50 | 150 |
| **2** | Artificial Intelligence in Cyber Security | T002 | 100 | 50 | 150 |
| **3** | Setting Up a Secure Network Infrastructure | L001 | 100 | 50 | 150 |
| **4** | Building a Security Operations Center | L002 | 100 | 50 | 150 |
| | TOTAL | | 400 | 200 | 600 |

| ATTENDANCE | GENERAL PERFORMANCE | INTERNAL EXAMINATIONS/ PROJECTS/ ASSIGNMENTS | TOTAL MARKS |
|---|---|---|---|
| 5 | 5 | 40 | 50 |

# COURSE SYLLABUS

# FOR

# Information and Cyber Security

| | | |
|---|---|---|
| **COURSE** | Information and Cyber Security | |
| **TOTAL MARKS** | Mark: 600 | Internal Mark: 200 |
| **TOTAL HOURS** | 320 Hrs | |

**DEFENITION OF CREDIT**

| | |
|---|---|
| 1 Credit | 15Hrs Theory/ 30Hrs Practical |
| Skill Components | 60 – 70 % of Total Credit |

**MODULES INCLUDED IN THIS SUBJECT**

| SL NO | MODULE NAME | CREDIT BREAKUP |
|---|---|---|
| 1 | Module 1: Information/Cyber Security-An Introduction | **1** |
| 2 | Module 2: Fundamental Concepts | **1** |
| 3 | Module 3: Application Vulnerabilities | **0.5** |
| 4 | Module 4: Identification of Vulnerabilities | **1** |
| 5 | Module 5: Threat/ Vulnerability Analysis | **1** |
| 6 | Module 6: Cybersecurity Policies, Procedures, Standards & Guidelines | **2** |
| 7 | Module 7: Technological Developments in Application Security | |
| 8 | Module 8 Fundamental Concepts | |
| 9 | Module 9: Application Hardening | |
| 10 | Module 10: Configuration Management | |
| 11 | Module 11: Web Application Secure Configuration | |

| | | |
|---|---|---|
| 12 | Module 12: Patch Management | |
| 13 | Module 13: Monitoring and Logging of Application Events and Alarms | **2** |
| 14 | Module 14: Inclusive and Environmentally Sustainable Workplaces | **1** |
| 15 | Module 15: Introduction to Employability Skills | **1** |
| 16 | Module 16: Constitutional values - Citizenship | |
| 17 | Module 17: Becoming a Professional in the 21st Century | |
| 18 | Module 18: Basic English Skills | |
| 19 | Module 19: Career Development and Goal Setting | |
| 20 | Module 20: Communication skills | |
| | Total | **10.5** |

## Training Outcomes

- Explain the use cases, common roles, and basic operating procedures followed by organizations in the context of cybersecurity.
- Describe the security threats associated with network and ICT devices, and commonly used security solutions.
- Describe typical vulnerabilities observed in applications.
- Describe the methods to identify vulnerabilities in applications.
- Demonstrate the ways to perform vulnerability assessment in applications.
- Describe the policies, standards, procedures, and guidelines related to application security.
- Discuss the latest technological developments in application security.
- Discuss the fundamentals of programming and operating systems that are relevant to application security management.
- Describe the methods to perform application hardening.
- Describe the methods to secure application configuration across environments.
- Describe the methods to secure web application configurations.
- Apply different approaches to manage web server, web application, and accessibility patches as per the latest guidelines.
- Explain the use of SIEM tools in monitoring application security.
- Plan one's schedules and timelines based on the nature of work.
- Demonstrate how to communicate and work effectively with colleagues.
- Use different approaches to effectively manage and share data and information.
- Identify best practices to maintain an inclusive, environmentally sustainable workplace.

# MODULES

## Module 1: Information/Cyber Security-An Introduction

**THEORY**

- Explain the relevance of Cyber Security to the society
- Explain the various use-cases of Cyber Security in the industry
- Explain various cyber threats associated with networks, devices, and remote access technologies
- Describe the responsibilities of various roles in cybersecurity, especially those specific to the role under consideration (i.e., Analyst Application Security)
- Describe the fundamentals of operating procedure in organizations including SLA's, data integrity & confidentiality, information recording, reporting, compliance requirements, and scope of devices/tools, stakeholders, authorizing personnel, etc.

**PRACTICAL**

- Create a career map for roles in Information/Cyber Security
- Demonstrate the working mechanism of malicious codes such as virus, malware, logic bomb, ransomware, spyware, phishing, trojan, etc.

## Module 2: Fundamental Concepts

**THEORY**

- Describe commonly used ICT devices as well as web servers and web applications.
- Explain relevant networking fundamentals:networking concepts: load balancing OSI, Model/topology, TLS, SSL, etc protocols: TCP/IP, FTP, SFTP, SNMP, SSH, SSL, VPN, RDP, HTTPS etc devices: switches, routers, servers, transmission media, etc
- Explain the stages of cyberattack from reconnaissance to identification and prevention.
- Discuss commonly used Unix/windows security commands.
- Explain common security solutions such as firewall, intrusion detection or prevention systems (IDS/IPS), anti- virus, web security gateways, email security, etc.
- Describe standard Systems Development Lifecycle (SDLC) practices and processes.
- Explain the concepts of system architecture and design in the context of IT systems.
- Explain what applications are, types of applications, and common application security requirements.

**PRACTICAL**

- Demonstrate the use of various Network Protocols and bandwidth management tools.
- Demonstrate the application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, Encryption, etc.
- Demonstrate commonly used methods of data theft and unauthorized access
- Demonstrate the usage of basic methods/tools in preventing cyber- attacks.
- Demonstrate system architecture of sample information systems.
- Demonstrate the basic functionalities of the applications, their components and security features.

## Module 3: Application Vulnerabilities

**THEORY**

- Define the types of vulnerabilities commonly found in applications.
- Explain the procedure to identify application vulnerabilities.

**PRACTICAL**

- Demonstrate how to identify vulnerabilities in sample applications.
- Demonstrate the functionalities of sample application and database layer IPS/IDS appliance.

## Module 4: Identification of Vulnerabilities

**THEORY**

- Explain the steps to gather relevant information for vulnerability assessment including:
  - source code
  - application type
  - security controls and application patching
  - application functionality and connectivity
  - application design and architecture
- Discuss the importance of documentation review in identifying vulnerabilities.
- Explain how to distinguish false positives form genuine security threats.
- Explain the methods to identify application vulnerabilities.
- Describe the methods and tools used in application penetration testing.
- Explain the difference between internal and external penetration testing.

**PRACTICAL**

- Perform source code review using suitable methods and tools to identify security issues.
- Demonstrate identification of potential threats by using threat scenarios from various sources.
- Perform root cause analysis of identified issues in sample applications.
- Demonstrate penetration testing processes and black box testing on sample applications using automatic scanning technologies and manual tests.
- Perform network penetration testing by capturing a variety of traffic, poisoning of a victim's proxy server, hiding of sensitive information, hijacking of a variety of sessions etc. for building secure infrastructure.
- Perform an external penetration test by creating topological network maps.
- Demonstrate methods to document application security requirements.
- Demonstrate methods to preserve data collected during the analysis.

## Module 5: Threat/ Vulnerability Analysis

**THEORY**

- Explain various vulnerability categories.
- Describe ways to identify the extent of vulnerability in an application.
- Describe the functionalities of commonly used vulnerability assessment tools and frameworks
- Discuss the best practices related to vulnerability assessment.

**PRACTICAL**

- Prepare a tracker in prescribed format to capture vulnerabilities and risk exposure data of sample applications.
- Demonstrate categorization of vulnerabilities based on level of weakness, sensitivity of information, relevance, root causes, risk criticality, and mitigation methods.
- Perform root cause analysis of identified vulnerabilities in sample applications.
- Prepare a report on vulnerability analysis including security requirements, vulnerabilities identified and recommended solutions.
- Demonstrate the procedure to securely store data collected during the assessment, vulnerabilities, analysis results, and mitigation recommendations.

## Module 6: Cybersecurity Policies, Procedures, Standards & Guidelines

**THEORY**

- Describe relevant legislation, standards, policies, and procedures for application security.
- List the organisational systems, procedures, and tasks/ checklists to maintain compliance with application security.

**PRACTICAL**

- Demonstrate the operating procedures that are applicable to application security.
- Apply standard tools and templates, including OWASP tools and methodologies in application security.

## Module 7: Technological Developments in Application Security

**THEORY**

- Evaluate next generation techniques for controlling advanced threats to applications.
- Describe improved ways of preventing remote applications by being compromised.
- Discuss the importance of staying abreast of technological upgradations in application security.
- List popular sources and platforms to gather information related to technological developments in application security.

**PRACTICAL**

- Perform research related to latest developments in application security and document the findings in prescribed formats.
- Demonstrate some of the advanced methods of securing applications found through research.

## Module 8: Fundamental Concepts

**THEORY**

- List all web servers and web applications on sample networks.
- Distinguish between the limitations of different programming, command line or scripting languages such as C/C++, Java, and JavaScript programming to read and write coded scripts.

**PRACTICAL**

- Demonstrate how to work on various operating systems.
- Demonstrate methods to read and write coded scripts.
- Demonstrate methods to modify and debug programs.
- Apply the most suitable programming languages to modify and debug programs.

## Module 9: Application Hardening

**THEORY**

- Discuss the steps involved in application hardening.
- Explain the methods and tools to harden applications across devices and environments.
- Discuss the best practices related to application hardening.

**PRACTICAL**

- Perform application hardening in sample applications.

## Module 10: Configuration Management

**THEORY**

- Explain the methods and tools to securely configure applications.
- Outline the importance of access controls in applications and databases.
- Describe various security technical implementation guides (STIGs).
- Discuss the best practices related to application configuration across environments.

**PRACTICAL**

- Demonstrate the process of securing administrative console using sample. web servers and applications
- Demonstrate ways to manage unauthorized instances and extraneous functionalities.
- Demonstrate the process of securing application configuration using tools and techniques such as application testing, code review, firewall, etc.

## Module 11: Web Application Secure Configuration

**THEORY**

- Describe the methods to configure web applications securely across environments for minimum exposure and weaknesses.
- Discuss the best practices related to web application configuration.

**PRACTICAL**

- Demonstrate the process of securing web application configuration using tools and techniques such as application testing, code review, web application firewall, etc.
- Apply suitable programming tools and techniques to configure, modify and debug

application codes.

## Module 12: Patch Management

**THEORY**

- Describe patch management life cycle.
- Define measures to effectively patch an application.
- Outline the guidelines in relation to application patching and hardening.
- Explain mechanisms to ensure implementation of security updates and patches on all application assets.
- Describe the process of application hardening.

**PRACTICAL**

- Apply checks on front-end and back- end platforms for the reported vulnerabilities, and available patches or updates.
- Demonstrate the implementation of latest or updated patches on all applications.
- Demonstrate the integration of patch management with the operational cycle of IT infrastructure management.
- Demonstrate the process of application hardening to reduce vulnerability.
- Develop a strategy for management of patches and updates.
- Demonstrate how to align or reengineer IT infrastructure processes as per the applications' patch management requirements.

## Module 13: Monitoring and Logging of Application Events and Alarms

**THEORY**

- Describe the scope of sample applications and system components to be monitored.
- Describe various monitoring and data collection methods and tools following organizational procedures and policies.
- Describe operational processes for log management.
- Explain the process of analysing application traffic.
- Describe the process of determining the occurrence frequency of identified risks, and their potential impact.
- List the actions required mitigate identified risks.
- Explain the process of documenting the results of monitoring, incident logging and closure activities.
- Explain incidence response workflows, incident/breach management plan and technical or tactical measures to detect and report security incidents commonly implemented in IT firms.
- Discuss the role of CND staff in identifying network alerts.

**PRACTICAL**

- Demonstrate the process of monitoring application consoles using Security Information and Event Management (SIEM) tool.
- Demonstrate the usage of prescribed tools/ software to track application traffic, security events and activity logs.
- Perform time stamping and server synchronization across logs.
- Demonstrate traffic analysis techniques to identify atypical activities and potential cyber threats.
- Apply telemetry monitoring to identify security issues.
- Perform event correlation using suitable tools.
- Demonstrate the workflows of threat response such as:
  – raising incidents
  – categorizing tickets
  – determining a turn-around time
  – assigning tickets to the relevant person according to the risk type
  – using escalation matrix for unresolved tickets
- Prepare a tracker of security incidents related to applications.
- Demonstrate methods to evaluate and categorize identified risks.
- Apply suitable methods to mitigate the identified security risks.

## Module 14: Inclusive and Environmentally Sustainable Workplaces

**THEORY**

- Describe different approaches for resourceful energy utilisation and waste management
- Describe the importance of following the diversity policies
- Identify stereotypes and prejudices associated with differently abled people and its negative consequences
- Discuss the importance of promoting, sharing and implementing gender equality and PwD sensitivity guidelines at organization level

**PRACTICAL**

- Practice the segregation of recyclable, non-recyclable and hazardous waste generated
- Demonstrate different methods of energy resource use optimization and conservation
- Demonstrate essential communication methods in line with gender inclusiveness and PwD sensitivity

## Module 15: Introduction to Employability Skills

**THEORY**

- Discuss the Employability Skills required for jobs in various industries
- List different learning and employability related GOI and private portals and their usage

## Module 16: Constitutional values – Citizenship

**THEORY**

- Explain the constitutional values, including civic rights and duties, citizenship, responsibility towards society and personal values and ethics such as honesty, integrity, caring and respecting others that are required to become a responsible citizen
- Show how to practice different environmentally sustainable practices

## Module 17: Constitutional values – Citizenship

**THEORY**

- Discuss importance of relevant 21st century skills.
- Exhibit 21st century skills like Self-Awareness, Behaviour Skills, time management critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn etc. in personal or professional life.
- Describe the benefits of continuous learning

## Module 18: Basic English Skills

**THEORY**

- Show how to use basic English sentences for everyday conversation in different contexts, in person and over the telephone
- Read and interpret text written in basic English
- Write a short note/paragraph / letter/e -mail using basic English

## Module 19: Career Development and Goal Setting

**THEORY**

- Create a career development plan with well-defined short- and long-term goals

## Module 20: Communication skills

**THEORY**

- Demonstrate how to communicate effectively using verbal and nonverbal communication etiquette.
- Explain the importance of active listening for effective communication
- Discuss the significance of working collaboratively with others in a team