SYLLABUS FOR BOARD OF STUDIES ADOPTION — generated from the live catalogue record

Cybersecurity Essentials and Digital Safety

C-07 · 3 days (configurable 1–5 days) · Informatics · Security · Years: 1st, 2nd, 3rd, PG

CONTENTS

1. Overview 2
2. Hours and credit position 2
3. Course outcomes 2
4. Course content — modules 2
5. Assessment scheme (100 marks) 2
6. CO–PO mapping 3
7. Every participant receives 3
8. Fee 3
9. Designed by 3

Catalogue C-07 · version 2 · generated 2026-10-11

OVERVIEW

Threat models, password and identity hygiene, secure coding basics, phishing simulation, incident response drill.

Relevant to every branch, and it is the natural first step for students considering the Cyber Security specialisation.

HOURS AND CREDIT POSITION

Contact hours: 24 Guided project: 6 Self-study: 0 Notional total: 30

Credit claim: 1
30 notional hours ÷ 30 hours per credit (NSQF track, UGC Micro-credentials Guidelines §5.3.3) = 1 credits.

COURSE OUTCOMES

CO1. Construct a threat model for an application, naming its assets and attack surfaces (K4)
CO2. Apply password, MFA and session hygiene to harden personal and organisational accounts (K3)
CO3. Identify phishing attempts and demonstrate the correct reporting response (K2)
CO4. Demonstrate how injection and XSS attacks work and how input handling defeats them (K3)
CO5. Conduct a structured incident-response drill from detection to post-mortem (K4)

COURSE CONTENT — MODULES

Hours shown are the recommended format; module time scales proportionally when the engagement runs 1–5 days.

Module 1 — Thinking like an attacker (4h recommended)
Theory: Threat models, attack surfaces, the CIA triad in plain language
Lab: Threat-model a familiar app in teams
Output: Threat model diagram

Module 2 — Identity hygiene (4h recommended)
Theory: Passwords, managers, MFA, session theft, account recovery
Lab: Audit and harden a set of demo accounts
Output: Hardening checklist applied

Module 3 — Phishing and social engineering (4h recommended)
Theory: Recognition patterns, pretexts, reporting; a live simulation
Lab: Phishing simulation and debrief
Output: Simulation analysis note

Module 4 — Secure coding basics (4h recommended)
Theory: Injection, XSS, secrets in code, dependency risk — by demonstration
Lab: Exploit then fix a deliberately vulnerable app
Output: Before/after fix log

Module 5 — Network and device safety (4h recommended)
Theory: Public Wi-Fi, HTTPS, updates, encryption at rest
Lab: Inspect real traffic with and without TLS
Output: Traffic capture comparison

Module 6 — Incident response drill (4h recommended)
Theory: Detection, containment, communication, the honest post-mortem
Lab: Tabletop incident drill in teams
Output: Incident report + capstone quiz

ASSESSMENT SCHEME (100 MARKS)

Continuous lab exercises — 40 marks
Capstone project & demonstration — 40 marks
Quiz & viva voce — 20 marks

CO–PO MAPPING

CO1 !’ PO2 (strength 2)
Threat modelling is security's analytical core.
CO2 !’ PO12 (strength 2)
Identity hygiene is a lifelong daily practice.
CO3 !’ PO1 (strength 2)
Recognition is the first defence for every user.
CO4 !’ PO3 (strength 2)
Seeing an exploit work makes the defence real.
CO5 !’ PO10 (strength 2)
Incident response is communication under pressure.

EVERY PARTICIPANT RECEIVES

- Certificate of completion
- Course material
- LMS access
- Interview question bank
- Mock interview & viva practice
- Optional nasscom NSQF assessment (priced per candidate on your quotation)

FEE

¹850 per student, incl. GST
Excludes the optional nasscom assessment where offered. Final pricing on your college's quotation.

DESIGNED BY

Venkat Kurela — Founder & Director, Kurela Cognisive Private Limited