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

Cyber Security Awareness for Faculty and Staff

FDP-06 · 2 days (configurable 1–5 days) · Informatics · Security

CONTENTS

Catalogue FDP-06 · version 1 · generated 2026-08-27

OVERVIEW

The attacks that actually reach a college, and what staff can do about them.

Colleges hold student records, fee data and identity documents. The attacks that succeed are ordinary ones, and awareness is the cheapest control available.

HOURS AND CREDIT POSITION

Contact hours: 12 Guided project: 2 Self-study: 2 Notional total: 16

Credit claim: none

Offered as a non-credit programme. The hours above are stated for transparency; the college may position it inside value-added / add-on frameworks at its discretion.

COURSE OUTCOMES

CO1. Identify the attack patterns that most often succeed against institutions (K2)
CO2. Apply account and device controls that resist credential attacks (K3)
CO3. Classify student data by sensitivity and describe how each class may be shared (K4)
CO4. Recognise an incident in progress and take the correct first containment step (K3)
CO5. Explain the institution's reporting obligations when personal data is exposed (K2)

COURSE CONTENT — MODULES

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

Module 1 — How colleges get breached (4h recommended)
Theory: Phishing, credential reuse, unpatched systems, insider error
Lab: Walk a real breach timeline
Output: Annotated breach timeline

Module 2 — Protecting accounts and data (4h recommended)
Theory: Passwords, second factors, device hygiene, safe sharing of student data
Lab: Audit your own account posture
Output: Personal security checklist

Module 3 — Responding and reporting (4h recommended)
Theory: Recognising an incident, containment, who to tell, DPDP obligations
Lab: Tabletop exercise on a simulated incident
Output: Departmental response note

ASSESSMENT SCHEME (100 MARKS)

Account posture audit — 30 marks
Tabletop exercise — 40 marks
Departmental response note — 30 marks

CO–PO MAPPING

CO1 !’ PO1 (strength 2)
Attack patterns are the domain knowledge the rest depends on.

CO2 !’ PO5 (strength 3)
Account and device controls are the practical tool outcome.

CO3 !’ PO8 (strength 3)
Classifying student data is the professional-ethics outcome.

CO4 !’ PO4 (strength 2)
Recognising an incident is investigation under time pressure.

CO5 !’ PO6 (strength 2)
Reporting obligations are the institutional and societal outcome.

EVERY PARTICIPANT RECEIVES

- Certificate of completion
- Course material
- LMS access

FEE

On your college's quotation
Excludes the optional nasscom assessment where offered. Final pricing on your college's quotation.

DESIGNED BY

Venkat Kurela — Founder, Kurela Cognisive Pvt Ltd