

Information Security & Cyber Defence-Integrated MCA

Integration: 4 Credits | 42 Hours | 3 Global Certifications | Fee: 70,000 INR per Semester

GJIMT offers a unique 4 Semester Integrated MCA Program in Information Security and Cyber Defence **with Industry-Benchmarked Shadow Projects & Embedded GSDC Certifications**

Why you should do this Program:

- ✓ 4 enterprise-grade security projects
 - ✓ 3 globally recognized GSDC certifications
 - ✓ Hands-on SOC, Cloud & AppSec exposure
 - ✓ Security reports & audit documentation
 - ✓ Job-ready Information Security graduates
-

SEMESTER 1

Computing Foundations + Security Basics

Core Focus:

Mathematical Foundations for Computing, Programming in C / Python, Computer Organization & Architecture, Data Structures, Professional Communication

Information Security Skill Layer

- Fundamentals of Information Security
- CIA Triad, Threats & Vulnerabilities
- Linux fundamentals for security
- Networking basics (TCP/IP, OSI)
- Git & documentation standards

Benchmarked Shadow Project 1

(Google-Style Secure System Baseline Project)

Students perform security hardening & baseline assessment of a computing environment.

Key Deliverables

- Secure OS configuration checklist
- User & permission hardening
- Password & access policies
- Threat model documentation

Benchmark: Google internal secure system baselines & CIS benchmarks

SEMESTER 2

Networks, Systems & Defensive Security

Core Focus:

Object Oriented Programming, Operating Systems, Database Management Systems, Software Engineering

Information Security Skill Layer:

- Network security (Firewalls, IDS/IPS)
- Cryptography fundamentals
- Secure coding practices
- Vulnerability assessment basics

GSDC Certification – 1

GSDC Certified Information Security Foundation

Benchmarked Shadow Project 2

(IBM-Style Enterprise Network Defence Project)

Students design and secure a corporate network infrastructure.

Key Deliverables

- Network architecture diagram
- Firewall & IDS rule sets
- Vulnerability scan report
- Risk mitigation plan

Benchmark: IBM enterprise SOC network defence models

SEMESTER 3

Application, Cloud & SOC Security

Core Focus:

Computer Networks, Web Technologies, Elective I (Cloud / AI / Data Analytics)

Information Security Skill Layer

- Web application security (OWASP Top 10)
- Cloud security fundamentals (AWS / Azure)
- Identity & Access Management (IAM)
- Security monitoring & SIEM basics

GSDC Certification

GSDC Certified Cyber Security Professional

Benchmarked Shadow Project 3

(Microsoft-Style Secure Cloud Application Project)

Students secure a cloud-hosted enterprise application.

Key Deliverables

- Threat modeling (STRIDE)
- Secure API & authentication
- Cloud security controls
- SIEM-based log analysis

Benchmark: Microsoft Azure Security Reference Architectures

SEMESTER 4

Cyber Defence, Risk & Capstone

Core Focus:

Major Project, Seminar & Viva, Elective II (Advanced specialization)

Information Security Skill Layer

- SOC operations & incident response
- Digital forensics fundamentals
- Risk management & compliance (ISO 27001, GDPR)
- Security audit & reporting
- Placement readiness

GSDC Certification – 3

GSDC Certified Ethical Hacking Practitioner

Benchmarked Shadow Capstone Project

(Palo Alto / Deloitte-Style Cyber Defence Project)

Students solve a realistic enterprise security problem.

Capstone Options

- SOC incident response simulation
- Enterprise penetration testing & audit
- Cloud security posture assessment
- Ransomware attack analysis & mitigation

Capstone Deliverables

- Security architecture & audit report
- Incident response playbooks
- Risk assessment & compliance mapping
- Viva-style defence

JOB ROLES AFTER PROGRAM

- Information Security Analyst
- SOC Analyst (L1 / L2)
- Cyber Security Engineer
- Cloud Security Associate
- GRC & Risk Analyst
- Penetration Testing Associate

INDUSTRY BENCHMARKING

- Aligned with NIST, ISO 27001, OWASP
- Comparable to SOC analyst & cyber defence programs
- Strong fit for enterprise & consulting roles