Gautam Buddha University (GBU)

A Globally Acclaimed University in NCR,
Established by UP Gautam Buddha University Act No 9 of 2002,

In Association with

Institution of Electronics and Telecommunication Engineers (IETE)

designated as

Scientific and Industrial Research Organisation (SIRO) by DST, GoI

and Educational Institution of Eminence by GoI

Announces One-Year Post Graduate Diploma in Cyber Security

Secure Your Future in the Digital World

Three Tracks Covered Over Three Trimesters

(360 hours of extensive classroom sessions, online and offline lab sessions, industry visits and projects. Additionally assignments, project research work and project report preparation to be done outside of the formal classroom sessions in own time)

(Choose one of the tracks, a combination of any two tracks or all three tracks)

| Track I | Track II | Track III |
|---|---|---|
| Cyber Security Operations | Cyber Security Governance | Secure Software development |
| **Basics of Information Security (Common to all three tracks)** | | |

| | |
|---|---|
| **Track I**<br><br>**Cyber Security Operations**<br><br>Upon successful completion of the Track I, get a "IETE *Certificate in Cyber Security Operations*" | **Introduction to Cyber Security Operations**<br>1. Introduction to Cyber Security: Overview of cyber threats, attack vectors, and the importance of cyber security operations.<br>2. Networking Fundamentals: Understanding network protocols, architecture, and common vulnerabilities.<br>3. Operating Systems Security: Basics of securing different operating systems (Windows, Linux, macOS) and hardening techniques.<br>4. Security Tools: Introduction to essential security tools like firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus, and anti-malware.<br>**Threat Detection and Analysis**<br>1. Security Information and Event Management (SIEM): Understanding SIEM systems, log management, and correlation of security events.<br>2. Intrusion Detection and Prevention: Deep dive into IDS/IPS, signature-based and behaviour-based detection, and response strategies.<br>3. Security Incident Management: Incident response lifecycle, handling incidents, and creating incident response plans. |

| | |
|---|---|
| | 4. Malware Analysis: Basics of analysing malicious software, identifying indicators of compromise (IOCs), and understanding different malware types.<br>**Vulnerability Management and Penetration Testing**<br>1. Vulnerability Assessment: Identifying vulnerabilities in systems, applications, and networks using scanning tools.<br>2. Patch Management: Strategies for keeping systems up-to-date and protected against known vulnerabilities.<br>3. Ethical Hacking and Penetration Testing: Introduction to penetration testing methodologies, tools, and techniques. Hands-on practice with safe environments.<br>4. Web Application Security: Common web vulnerabilities (SQL injection, XSS, CSRF) and techniques to secure web applications.<br>**Defensive Techniques and Emerging Trends**<br>1. Network Security: Advanced concepts in network security, including VPNs, network segmentation, and securing wireless networks.<br>2. Cloud Security: Security considerations in cloud environments (IaaS, PaaS, SaaS), shared responsibility model, and securing cloud resources.<br>3. Identity and Access Management (IAM): User authentication, authorization, multi-factor authentication (MFA), and role-based access control (RBAC).<br>4. Emerging Trends: Exploring new and evolving threats, such as IoT security, AI/ML in cyber security, and the impact of regulations like GDPR and CCPA.<br>5. Legal and Ethical Aspects: Understanding legal frameworks related to cyber security, ethical hacking, and privacy laws.<br>**Project Work & industry visit: Bringing together concepts learned** |
| **Track II**<br><br>**Cyber Security Governance**<br><br>Upon successful completion of the Track II, get a "IETE *Certificate in Cyber Security Governance*" | **Introduction to Cyber Security Governance**<br>1. Introduction to Cyber Security Governance: Understanding the role of governance in cyber security, its importance for organizations, and key concepts.<br>2. Cyber Security Frameworks: Overview of popular frameworks such as NIST Cybersecurity Framework, ISO/IEC 27001 including 27701, and CIS Controls.<br>3. Security Policies and Procedures: Developing and implementing security policies, standards, guidelines, and best practices.<br>4. Regulatory Compliance: Understanding industry regulations and compliance requirements (e.g., DPDPA 2023, GDPR, HIPAA, SOX) and their impact on cyber security.<br>**Risk Management and Assessment**<br>1. Cyber Risk Management: Principles of risk assessment, risk identification, risk analysis, and risk treatment strategies.<br>2. Risk Assessment Tools: Introduction to risk assessment tools and methodologies, including qualitative and quantitative risk assessment.<br>3. Vendor and Third-Party Risk Management: Evaluating and managing risks associated with third-party vendors and service providers.<br>4. Business Impact Analysis: Assessing the potential impact of cyber incidents on business operations, reputation, and financials.<br>**Security Governance and Compliance Management**<br>1. Security Governance Structure: Establishing cyber security governance structures, roles, and responsibilities within an organization.<br>2. Security Audits and Assessments: Conducting internal and external security audits, vulnerability assessments, and penetration tests.<br>3. Incident Response Planning: Developing and testing incident response plans, communication strategies, and coordination with stakeholders.<br>4. Security Awareness and Training: Creating security awareness programs for employees and educating stakeholders about security policies. |

| | |
|---|---|
| | **Strategic Planning and Emerging Trends**<br>1. Security Strategy Development: Creating a comprehensive cyber security strategy aligned with business objectives and risk appetite.<br>2. Security Metrics and Reporting: Measuring the effectiveness of security measures, defining key performance indicators (KPIs), and reporting to stakeholders.<br>3. Board and Executive Engagement: Effectively communicating cyber security matters to the board and executives, emphasizing business impact.<br>4. Emerging Trends and Future Challenges: Exploring emerging threats, technologies (such as AI/ML in cyber security), and regulatory changes that will impact governance.<br>**Project Work and industry visit: Bringing together concepts learned** |
| **Track III**<br><br>**Secure Software Development**<br><br>Upon successful completion of all three tracks, get a "*Post Graduate Diploma in Cyber Security from Gautam Buddha University*" | **Fundamentals of Secure Software Development**<br>1. Introduction to Secure Software Development: Understanding the importance of security in the software development lifecycle (SDLC).<br>2. Secure Coding Principles: Teaching best practices for writing secure code, including input validation, output encoding, and error handling.<br>3. Threat Modelling: Identifying potential threats and vulnerabilities in software design and architecture.<br>4. Authentication and Authorization: Implementing secure user authentication and authorization mechanisms.<br>**Secure Software Design and Architecture**<br>1. Secure Design Patterns: Exploring design patterns that enhance security, such as least privilege, separation of duties, and defence in depth.<br>2. Secure API Design: Designing and implementing secure APIs, including input validation, authentication, and access control.<br>3. Database Security: Protecting sensitive data through proper database design, encryption, and access controls.<br>4. Security in DevOps: Integrating security into the DevOps pipeline, including continuous integration, continuous delivery, and automated testing.<br>**Secure Coding Practices and Testing**<br>1. Input Validation and Output Encoding: Preventing common vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).<br>2. Buffer Overflows and Memory Safety: Understanding memory-related vulnerabilities and techniques to prevent them.<br>3. Code Reviews and Static Analysis: Conducting code reviews and using static analysis tools to identify security issues.<br>4. Dynamic Application Security Testing (DAST): Using tools to perform runtime testing for vulnerabilities.<br>**Advanced Topics and Secure Development Lifecycle**<br>1. Cryptographic Techniques: Implementing encryption, hashing, and digital signatures securely.<br>2. Secure Software Development Lifecycle (SDLC): Integrating security into every phase of the SDLC, from planning to deployment.<br>3. Secure Code Refactoring: Techniques for improving the security of existing codebases through refactoring.<br>4. Security Testing and Assessment: Performing security assessments like penetration testing and vulnerability scanning.<br>5. Secure Software Deployment: Strategies for securely deploying applications and managing updates.<br>**Major Project:** |

**Course Fee**

A. Any one track – Rs 50,000/- plus certificate exam fee of Rs 1500.00
B. Combination of any two tracks – Rs 100, 000/- plus certificate exam fee of Rs 3000.00
C. All three tracks – Rs 150000.00 plus university fee (admission, library, exam, refundable security fee of Rs 18,000.00)

**Discounts**

A. Early bird discount if full fee deposited by 15 Nov 23 – 20%
B. Early bird discount if full fee deposited by 30 Nov 23 – 10%
C. Additional discount for defence personnel (over and above early bird discount) – 10%
**D. Note: There will be no discount in the University Fee**

**Education Loan.** Education loan can be availed for the PGD Cyber Security Course.

**Class Timings.**

A. Weekend classes – 4-5 hours on Saturday and 4 hours on Sunday conducted in hybrid mode.

B. 3 days of physical presence for each track mandatory. Expenses towards travel, board and lodge for physical presence will be borne by the students.

**Examinations**. MCQ based written examinations for each track and assessment of projects through project presentation and project report.

**Placement.** Placement assistance will be provided with reputed companies and originations