GANPAT UNIVERSITY

FACULTY OF MANAGEMENT STUDIES

Programme	MBA	Branch/Spec.	Tech MBA (MBA Technology Management)
Semester	IV	Version	2.0.0.0
Effective from Academic Year	2025-26	Effective for the Batch admitted in	January 2025
Course Code	**IVB04DFI**	Course Name	**Digital Forensics and Incident Response**

Teaching Scheme						Examination Scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	2	0	0		2	Theory	100		100
Hours	2	0	0		30	Practical			

Pre-requisites

Course Outcomes

On successful completion of the course, the students will be able to:

CO1	The students will be able to explain the strategic importance of Digital Forensics and Incident Response (DFIR) and the legal and regulatory drivers for its implementation.
CO2	The students will be able to analyze the components of a corporate incident response plan and the managerial decisions required at each stage of the response lifecycle.
CO3	The students will be able to evaluate the business principles of digital forensics, including evidence management, and its role in supporting internal investigations and litigation.
CO4	The students will be able to formulate a high-level crisis management and communication strategy for a major cyber incident, considering the financial, legal, and reputational impacts.

Theory Syllabus

Unit	Content	Hrs.
1	Foundations of Incident Response & Forensics, The Business Impact of a Cyber Incident, Digital Forensics vs. Incident Response: A Manager's View, The Integrated DFIR Lifecycle, Legal & Regulatory Drivers for DFIR (e.g., GDPR, HIPAA), Core Principle: Evidence Preservation & Chain of Custody, The Incident Response Team (IRT/CSIRT): Roles & Structure	6
2	Strategic Incident Response Management, The Incident Response Plan (IRP): A Strategic Document, The NIST IR Lifecycle: Preparation, Detection, Containment, Eradication, Recovery, Preparation: Tabletop Exercises & War Gaming, Detection & Analysis: From Alert to Verified Incident, Containment Strategies & Business Impact Trade-offs, Eradication & Recovery: Restoring Business Operations, Post-Incident Activities: The Critical "Lessons Learned" Phase.	8
3	Digital Forensics for Business Leaders, The Goals of a Corporate Forensic Investigation, Sources of Digital Evidence: Networks, Endpoints, Cloud, Forensic Principles: Repeatability, Integrity & Authentication, e-Discovery & Litigation Support, Managing Forensic Teams: In-House vs. Outsourced Retainers, Investigating Insider Threats & Intellectual Property (IP) Theft, Challenges of Cloud & Mobile Forensics (Conceptual), Interpreting a Forensic Executive Summary for Business Decisions.	8
4	Crisis Management, Communication & Leadership, Leading Through a Cyber Crisis: The Leader's Role, Formulating a Crisis Communication Strategy, Managing Stakeholder Communications (Board, Employees, Customers, Media), Engaging Legal Counsel, PR Firms & Cyber Insurers, Financial Triage: Business Continuity & Cost Management, Mandatory Breach Notification & Reporting Obligations, Building Organizational Resilience & an Anti-Fragile Culture, Capstone: Simulating a Board-Level Breach Response Discussion	8

1

Practical, assignments and tutorials are based on above syllabus.

Text Books

1	Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown, 2014.

Reference Books	
1	Krebs, Brian. Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door. Sourcebooks, 2015.
2	Singer, P.W., and Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.
3	Bejtlich, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.
4	Harvard Business Review. HBR's 10 Must Reads on Managing Risk. Harvard Business Review Press, 2020.
5	NIST Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide. National Institute of Standards and Technology.
6	Bernstein, Jonathan. Manager's Guide to Crisis Management. McGraw-Hill, 2011.
7	Clinton, Larry. Cybersecurity for Business. Routledge, 2018.
8	Shostack, Adam. Threat Modeling: Designing for Security. Wiley, 2014.
9	Ligh, Michael, et al. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley, 2014. (For conceptual understanding).
10	Sheffi, Yossi. The New (Ab)Normal: Reshaping Business and Supply Chain Strategy for a Post-Pandemic World. MIT CTL Media, 2020. (For resilience concepts).
ICT/MOOCs Reference	
1	Coursera: Cybersecurity Specialization — University of Maryland
2	Udemy: Digital Forensics & Incident Response (DFIR) Bootcamp

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PSO 1	PSO 2	PSO 3
CO1	2	3	2	1	2	3	1	2	3	3	2	3
CO2	3	3	3	2	2	2	1	2	3	3	2	2
CO3	2	3	2	1	2	3	1	1	2	2	2	3
CO4	3	2	3	2	3	3	1	2	3	2	2	3