SHARDA UNIVERSITY
Beyond Boundaries

NAAC A+ ACCREDITED

SHARDA SCHOOL OF BUSINESS STUDIES

COURSE

Cyber Shield Safeguarding Business in the Digital Age (NVAC203)

VALUE ADDED
COURSE BROCHURE-30 HRS
2025-26

Vision and Mission of the School

Vision of the School

To become a world class institution imparting education based on values, fostering culture of research, innovation and entrepreneurial spirit and exhibiting professional excellence for better and sustainable society.

Mission of the School

M1. Building conducive learning ecosystem

M2. Creating socially responsible future business leaders and entrepreneurs

M3. Imparting cutting-edge application based curriculum

M4. Boosting industry-academia connect

Course Articulation Matrix

POs COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO(1)	PSO(2)	PSO (3)
CO1	1	1	-	-	-	-	2	2	3
CO2	-	-	-	-	1	-	1	1	1
CO3	2	-	2	1	3	-	-	1	-
CO4	2	1	3	2	2	-	-	-	-
CO5	2	2	3	2	1	-	1	-	1
CO6	2	1	3	2	2	-	2	-	-
Average	1.8	1.25	2.75	1.75	1.80	-	1.50	1.33	1.67

1-Slight (Low)
2-Moderate (Medium)
3-Substantial (High

ABOUT THE UNIVERSITY

Sharda University is a leading Educational institution based out of Greater Noida, Delhi NCR. A venture of the renowned Sharda Group of Institutions (SGI), The University has established itself as a high-quality education provider with a prime focus on holistic learning and imbibing competitive abilities in students.

ABOUT SCHOOL

Sharda School of Business Studies believes in preparing students to approach business obstacles and solve them the way established corporations do. Learning happens both inside and outside the classroom; hence, technology plays a big part in the core culture, and so do global exposure, project management, critical reasoning, and business communications skills.

ABOUT COURSE

The **'Cyber Shield: Safeguarding Business in the Digital Age' (NVAC203)** is a value-added course designed to equip future business leaders with the knowledge and tools to address the growing challenges of cybersecurity in an increasingly digitalized world. This course provides an in-depth understanding of how cyber threats can impact businesses, ranging from data breaches and ransomware attacks to phishing scams and insider threats. Students will learn about key cybersecurity concepts, including risk assessment, incident response planning, and the importance of robust data protection strategies. The course emphasizes the critical role of cybersecurity in maintaining business continuity, protecting intellectual property, and ensuring compliance with legal and regulatory standards. By integrating theoretical frameworks with real-world case studies, NVAC203 fosters practical skills in identifying vulnerabilities and implementing proactive security measures. The curriculum also highlights the importance of fostering a cybersecurity-aware organizational culture, emphasizing training, ethical hacking, and collaboration between IT and management teams. Students will explore emerging trends in cybersecurity, such as artificial intelligence, blockchain, and quantum computing, to understand how these technologies can both mitigate and amplify risks.

COURSE SCHEDULE

Week	Content	Details of Topic Covered	Duration Hrs.
1	**Understanding Cyber Threat Landscape**	Introduction to common cyber threats (e.g., malware, phishing, ransomware) and their impacts on businesses.	3
2	**Cybersecurity Frameworks**	Overview of major cybersecurity frameworks (e.g., NIST, ISO 27001) and their relevance to business operations.	3
3	**Importance of Cybersecurity**	The role of cybersecurity in protecting business continuity, reputation, and customer trust.	3
4	**Fundamentals of Risk Assessment**	Introduction to the process of identifying, analyzing, and evaluating cybersecurity risks.	3
5	**Risk Management**	Techniques for prioritizing risks and implementing mitigation strategies, including case studies.	3
6	**Cybersecurity Policies**	Designing effective access controls, data protection measures, and incident response procedures.	3
7	**Encryption & Awareness**	Understanding encryption techniques and strategies for training employees on cybersecurity best practices.	3
8	**Emerging Trends**	Exploring cutting-edge technologies like AI, blockchain, IoT security, and their implications for cybersecurity.	3
9	**Challenges and Careers**	Addressing challenges in securing emerging technologies and discussing career opportunities in cybersecurity.	3
10	**Compliance and Ethics**	Overview of regulatory frameworks, data privacy laws (e.g., GDPR, CCPA), and ethical considerations in cybersecurity.	3

PROFILES

Dr. Mahima Shukla:

Dr. Mahima shukla is an assistant professor in Sharda School of Business Studies, Greater Noida. She is B. Tech in computer science and M.B.A in Marketing & IT, also did her PhD in Management. She has also qualified National Eligibility Test (NET) Examination conducted by UGC, Government of India. She has a more than 6 years of experience in research and academics. She tends to research on subjects where marketing and technology come together to create an impact on business.

Dr. Shweta Gupta:

Dr. Shweta Gupta is a distinguished academician and researcher with a robust background in management and social work. She possesses a PhD in Management, MSW, and MBA , as well as MA(Lady Shri Ram College for Women,University of Delhi) with extensive teaching and research experience, Dr. Gupta has authored numerous research papers in esteemed publications, including Scopus-indexed journals, UGC-CARE listed journals, and book chapters. Her research focuses on organisational behavior, human resource management, and social work.

Currently, Dr. Gupta serves as Assistant Professor at Sharda University, Greater Noida, where she has played a vital role in organizing grand-scale events and workshops. Her expertise extends beyond academia, as she is a sought-after corporate trainer, conducting sessions for esteemed organizations.

Dr. Gupta's dedication to imparting knowledge and skills has significantly impacted her students and corporate clients. Additionally, she is the founder of LAKSHYA, an NGO promoting health and education in Etah district, Uttar Pradesh.

Dr. D. Saravanan:

Dr. D. Saravanan has 23 years of experience in Teaching & Research. He holds Ph.D., in Marketing and Ph.D., in Human Resource. He has worked in Overseas for 10 years as an Associate Professor. In India, he has worked as a Dean, HoD, Professor, Associate Professor, etc., in Tamilnadu, Puducherry, Andhra Pradesh. He has published 15 research papers in peer review journals. He has evaluated 30+ PhD thesis as a foreign examiner, 45+ thesis as an Indian examiner and 4 Ph.D., Viva-voce examiner for various Indian universities.

Dr. S. Thiruselvan :

Dr. S. Thiruselvan, an Assistant Professor at the School of Business Studies, Sharda University, Greater Noida has over 14 years of experience in teaching, research, and academic leadership in the field of commerce and management. He holds a Ph.D. in Commerce

His areas of specialization include Marketing, Financial Accounting, and Income Tax. His academic contributions include research publications in UGC CARE and Scopus-indexed journals, and presentations at national and international conferences.

School: SSBS **Programme: BBA/B.Com.** **Branch:**	**Batch : 2024-27** **Current Academic Year: 2025-26** **Semester: IV**	
1. Course Code	NVAC203	
2. Course Title	Cyber Shield: Safeguarding Business in the Digital Age	
3. Credits	Audit Course	
4. Contact Hours (L-T-P)	30 Hours	
Course Type	Value added course	
5. Course Objective	This course aims to equip students with essential knowledge and skills to effectively safeguard businesses against cyber threats in the digital age. Through a blend of theoretical understanding and practical application, students will develop a comprehensive understanding of cybersecurity principles, tools, and strategies. The course places a strong emphasis on enhancing employability by integrating real-world case studies and practical scenarios to provide students with hands-on experience in addressing contemporary cybersecurity challenges faced by businesses.	
6. Course Outcomes	**CO1:** The student will be able to define key terms and concepts related to cybersecurity. **CO2:** The student will be able to explain risk assessment methodologies. **CO3:** The student will be able to apply access controls and data protection measures. **CO4:** The student will be able to analyse cutting-edge technologies and trends. **CO5:** The student will be able to evaluate the impact of regulatory non-compliance. **CO6:** The student will be able to discuss the impact of cybersecurity events.	
7. Course Description	In today's interconnected world, businesses are increasingly vulnerable to cyber threats ranging from data breaches to ransomware attacks. The course is designed to provide students with a holistic understanding of cybersecurity principles and practices tailored specifically for businesses. The course will explore topics such as threat intelligence, risk assessment, security architecture, incident response, and regulatory compliance. By delving into real-world case studies and practical scenarios, students will gain valuable insights into the complexities of cybersecurity management within the context of modern business operations. Through hands-on exercises and interactive discussions, students will develop the skills necessary to analyse, mitigate, and respond to cyber threats effectively, thereby enhancing their employability in the rapidly evolving field of cybersecurity.	
8. Outline syllabus		CO Mapping
Unit 1	**Introduction to Cybersecurity in Business**	
A	Understanding Cyber Threat Landscape	CO1
B	Overview of Cybersecurity Frameworks	CO1
C	Importance of Cybersecurity in Business Operations	CO1
Unit 2	**Risk Assessment and Management**	
A	Fundamentals of Risk Assessment	CO2
B	Identifying and Prioritizing Cyber Risks	CO2
C	Implementing Risk Mitigation Strategies	CO2
Unit 3	**Designing effective Cyber security policies and procedures**	
A	Implementing access controls and data protection measures	CO3
B	Encryption techniques	CO3
C	Educating employees on cybersecurity best practices and awareness programs	CO3
Unit 4	**Emerging Trends in Cybersecurity**	
A	Exploring cutting-edge technologies and trends in cybersecurity (e.g., AI-driven security, blockchain, IoT security)	CO4
B	Addressing challenges in securing emerging technologies and trends	CO4,CO6
C	Future directions in cyber defence and cybersecurity career opportunities	CO4,CO6
Unit 5	**Regulatory Compliance and Ethical Considerations**	
A	Overview of Regulatory Compliance Frameworks	CO5
B	Data Privacy and Protection Regulations	CO5
C	Ethical Considerations in Cybersecurity Practices	CO5,CO6
Mode of examination	Assignments/Quizzes	