SNATIKA™

Boosting Careers of Professionals

BACHELORS PROGRAM IN CYBER SECURITY - UOG

18 - 24 MONTHS I ONLINE

www.snatika.com

WES Recognised

EDUCATION PARTNERS

QUALIFI APPROVED CENTRE | UNIVERSITY OF GLOUCESTERSHIRE | IDM

TABLE OF CONTENTS

SNATIKA™

Boosting Careers of Professionals

WHAT IS SNATIKA?

Back in 2020, we saw many hard-working senior professionals stuck in the same position without any prospect for growth. The simple but overlooked reason for this glass ceiling was the lack of reputed academic qualifications on their CV. This lack haunted their career prospects during the pandemic and the subsequent economic disruption. It might be even more so in the future.

The situation was unfair because, due to their commitments and age, senior professionals were deprived of opportunities to pursue any reputed qualifications without hurting their career prospects, financial stability, or family commitments. The idea of enrolling for a Degree/Diploma/Certificate moving away from their hometown, and quitting their jobs was impractical and scary.

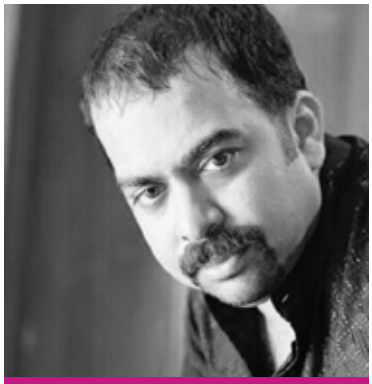
Being in the education industry for years, we wanted to help them out of this rough spot. Above all, we wanted to create an online platform where they could pursue their Degree, Diploma or Certificate programs without quitting their jobs, moving away from their families, or getting into debt without a source of income.

This is how SNATIKA was created in Mumbai, India. Our founders and the team had decades of experience in the education industry, which gave us a head start. We knew our adult learners needed nothing less than a reputed and globally recognised degree/diploma/certificate to make it to the top. We partnered with reputed international education institutions to provide our learners with relevant and prestigious academic qualifications. SNATIKA has also been ISO certified for its Admission Process and Academic Delivery Process. We continue to provide one of the largest bouquet of programs exclusively for senior professionals across different domains.

Our mission is to serve senior working professionals with a fair opportunity to pursue career-enhancing professional programs through our state-of-the-art Learning Management System.

Meet the TEAM

Get to know the team working behind the scenes to provide you with the highest-quality online education.



Sunil Janardhan

Founder Director

Sunil is a seasoned professional with 28 + years of rich experience in conceptualising and driving high-end strategic business models across diverse global economic hot-spots. Sunil has the privilege of travelling & doing business pan India & across 33 countries worldwide.

He has extensive hands-on experience and knowledge of Africa, Middle East, Asia & CIS markets. He has successfully managed different cultures, team members & partners across demographics/industries. He comes with expertise in International Business, Consulting, Sales & Marketing, Profit Centre Operations, Business Development, Key Account Management, Product Launches and Distributor/ Channel Management.

He has also been part of various strategic tie ups & JV's. Sunil specialises in finding new markets for sales growth. He has worked across large, medium & start-up organisations. He has associated with organisations like Aptech Ltd, ITI EdVest, Kuoni Travels, Kohinoor Technical Institute & Trade Wings.

Sunil has done his Post Graduation in International Business. He is based out of India.

Premjit Biswas

Founding Member
(Director of Education)

Premjit is a senior professional with over two and a half decades of experience in the Education and Training domain.

He brings in his immense experience of handling large operations across different geographies. Premjit also has considerable knowledge of entrepreneurship, innovation and skills development. He has experience in developing and managing partners and business operations in multiple countries.

He has also managed global projects. He firmly believes that the success or failure of a program lies in the impact it has had on the lives of the beneficiaries. Hence, programs should be designed keeping this as a focal point. That way the beneficiaries not only help themselves but help others and in turn continually increase the impact radius.

In his 20 years of corporate life, Premjit has been associated with large organisations like Aptech, Autodesk and Wadhwani Foundation. He was the founding member of a non-profit organisation - Tiksna Mission Trust. At Tiksna he worked relentlessly at the grassroots level, building a diverse environment to work & thrive in and enabling entrepreneurs.

Premjit is based out of India and has done his majors in Hospitality Management.

Prof. Raj Gill

Advisory Member

An influential , entrepreneurial COO and Pro-Vice Chancellor, Professor Raj Gill has over 40 years' experience in Higher Education and has held senior posts in Higher Education in UK and internationally. His experience of Trans National Education (TNE) includes international marketing and Higher Education development in Asia, Africa and the Middle East.

Professor Gill has published widely in learned journals and publications, and has chaired numerous sessions and presented at international conferences and symposia.

Professor Gill is based out of the UK and has a degree in Manufacturing Engineering and a PhD in Computer Simulation for Manufacturing Processes.

Roger Chetty

Advisory Member

Roger is an entrepreneur and corporate strategist with more than 20 years' senior management experience across several industries including Motor, Construction, Manufacturing, Education and Management Consulting. His career began in market research and customer services with Blue chip brands such as BMW, DaimlerChrysler, Audi, Standard Bank, and the South African Chamber of Business.

He has served on various boards during his illustrious career and has also co-authored several university policies and procedure documents. Roger is known for forging relationships with governments, educational institutions, and corporates all across Africa and the Middle East. He has been associated with organisation like Sika South Africa, University of KwaZulu-Natal – South Africa and NCC Education - UK.

Roger currently lives in Cape Town, South Africa and has an MBA degree from the Maagement College of Southern Africa.

Thierry Cabou

Advisory Member

Thierry Cabou is an expert on finance and economics domains. He focuses on investment and business development activities across Europe, Africa and India. He is also a Founding Member, Lifetime member and Representative for Africa for the Africa India Economic Foundation (AIEF). He is advisor to Bank of Asia and Asia Pacific Development Bank. He is a Knight of the Sovereign Order of St John of Jerusalem of Rhodes and Malta.

Thierry provides advisory and management services to government and large institutions. With Merrill Lynch, his group has arranged for several African governments' investment facilities up to 600 million US dollars after receiving mandates from these governments. He has secured with his partners a 400 million Euros plan for the oil and refinery sector in Senegal.

Mr. Thierry Cabou is educated in Paris, France, where he got degrees in International Business Law from Pantheon Sorbonne University.

COUNT ON OUR QUALIFICATIONS

ISO 9001: 2015 Certified

Learners are guided by SNATIKA at each level to choose the right program, and the final decision to provide admission rests with SNATIKA. SNATIKA's admission process ensures that only those learners who are apt for the program get admitted to our programs. Learners are provided with the right resource material, academic support, and timely assistance for them to successfully complete their program. We are able to provide this across genders, races, time zones, and geographies because of a strong academic delivery process, which is aptly supported by our PhD/ Doctorate facilitators. SNATIKA's academic delivery process ensures this is done flawlessly.

SNATIKA is certified for ISO 9001:2015 for "Admission Process & Academic Delivery Process."

UCAM Universidad Católica de Murcia

Universidad Católica San Antonio de Murcia (UCAM) is a fully accredited European University founded in the year 1996. The university is strategically located in Murcia, Spain, with a Campus of more than 16,000 students and around 1,000 professors. The World University Ranking especially highlights the internationalisation capacity of UCAM. The university has a diverse academic offer, constantly adapting and consistent with the real needs of society. MBA degree is awarded by UCAM under the provision of university private degrees – Título Propio.

SNATIKA learners are awarded MBA degrees from UCAM.

othm qualifications

OTHM, UK, is an awarding body which is approved and regulated by Ofqual – Office of the Qualification and Examinations Regulations, UK (a UK government department). Ofqual is responsible for maintaining standards and confidence in international qualifications. Ofqual also regulates the National Curriculum Assessments in England. OTHM aims to support professions and industry by providing excellent qualifications that contribute for a highly qualified and experienced workforce.

SNATIKA is an accredited/ approved training partner of OTHM.

LONDON GRADUATE SCHOOL

London Graduate School, UK offers excellent university programmes designed for students to gain knowledge and skills for a fast-changing and complex world. LGS promotes learning and sharing of knowledge by offering a blend of teaching and learning methods that combine personal and professional development with world-class academic knowledge. We have partnered with LGS to provide UK university degrees.

SNATIKA learners are awarded MA, MSc, or MBA degrees from a UK University through LGS.

THE UNIVERSITY OF BUCKINGHAM

Buckingham University is the oldest of Britain's independent universities and the only one in the UK with a Royal Charter. The university is ranked in the Top 10 by The Complete University Guide 2023 for Student Satisfaction and by The Times and The Sunday Times Good University Guide 2022 for Teaching Quality. It has also been awarded the QAA Quality Mark for meeting or exceeding UK expectations for quality and standards.

This partnership with the university is through LGS.

QUALIFI APPROVED CENTRE

QUALIFI, UK is recognised as an Awarding Organisation (AO) by Ofqual-Office of the Qualification and Examinations Regulations in the UK. QUALIFI must assure the regulators to continue the General Conditions of Recognition in England and that of the approved centres must meet the same exacting standards. And these qualifications combine UK standards with relevant international content, so learners can achieve their full potential in today's global economy.

SNATIKA is an accredited/ approved training partner of QUALIFI.

IDM Creating Opportunities Nurturing Achievers

IDM has over four decades of experience in the higher education sector. Having closely worked with the industry and brought global education to local students, IDM has pioneered the way forward in getting international recognition for talented students. The organisation aims at exceeding the Quality & Standard expectation and has been awarded the ISO 9001:2015 certification.

SNATIKA learners are awarded a BSc (Hons), BA (Hons), MA, MSc, or MBA degree from the University of Gloucestershire through IDM.

UNIVERSITY OF GLOUCESTERSHIRE

The University of Gloucestershire, a UK state university, is the degree awarding institution. It is located in the edge of the stunning Cotswolds and has three campuses which are based in Cheltenham and Gloucester. The University is a diverse, vibrant community of 12,000 students and 1,500 staff. The University has scored 90/100 and are placed in the top tier of the new SOS-UK net zero ranking. Ranked 6th globally in the Postgraduate Research Experience Survey, 2019.

This partnership with the university is through IDM.

SNATIKA BACHELORS PROGRAM IN CYBER SECURITY - UOG

This program is designed to train tomorrow's IT security professionals, combining fundamental concepts and principles with exposure to new technologies and solutions. Program provides a practical understanding of key issues relating to the design, analysis and implementation of modern IT security systems. Learners will specialise in identifying different cyber security attacks and mitigation techniques, detecting and responding to network-based intrusions, ethical hacking and testing approaches, and applied cryptography. And because other people's private data is involved, learners will also explore the legal and ethical implications and how they relate to cyber security. In doing so, the qualification looks to develop the cyber security team leaders, managers and leaders of the future through the creation and delivery of learning appropriate for that industry. By the time learners graduate, learners will have a set of skills that are in high demand in our technology-led world, across both the public and private sectors. This program is designed for individuals seeking to advance in their current career as well as those who wish to pursue Masters studies.

Who is it meant for?

SNATIKA provides globally recognised academic qualifications for professionals at their doorsteps. Bachelors Program in Cyber Security is suitable for

- Professionals looking for career progression
- Individuals aiming for a formal undergraduate qualification
- Professionals at junior / mid management level in cyber security industry

STAGE 1

This stage is delivered by SNATIKA. The program involves delivery through the online SNATIKA Learning Management System (LMS). On successful completion of the SNATIKA Bachelors program, learners are eligible for the following:

- Level 4 Diploma from QUALIFI, UK
- Level 5 Diploma from QUALIFI, UK
- Bachelors Program Certificate from SNATIKA

Eligibility

We believe you can only take full advantage of our programs if you have relevant work experience.

Eligibility criterion for SNATIKA's Bachelor programs are :

- A Levels / Grade 12 / Any Equivalent Qualification

and/or

- Minimum 2 years of work experience in the Cyber Security domain

MODULES

UNITS COVERED

- Cyber security threat and risk
- Network Security and Data communications
- Database Security and Computer Programming
- Incident Response, Investigations and Forensics
- Security strategies: Laws, Policies and Implementation
- Cyber Wars
- Cryptography
- Digital Investigations and Forensics
- Communications and Incident Management
- Strategic Leadership

OVERVIEW

SNATIKA's Bachelors Program in Cyber Security is delivered by SNATIKA through our own LMS. Our Subject Matter Experts have designed the pedagogy that will meet the demands and fulfil the needs of a busy working professional. Our PhD-level Masters Guides will help you through the program.

UNIT SPECIFICATIONS

Unit -1: CYBER SECURITY THREAT AND RISK

Unit Aims

Cyber security breaches cause significant personal and organisational damage and pose a clear and present risk to business profitability and resilience. In this unit the learner will be introduced to a variety of threats and risks emanating from the cyberspace. The unit will look at various methods of attack and will use case studies to analyse various threat vectors, including Malware, Botnets and Trojans. It will introduce and explain various models of measuring threats, risks and impacts.

LEARNING OUTCOMES

- Understand complex business cyber security threats and risks
- Understand recent mega breaches and explain malware and ransomware attacks
- Understand how threats and malicious hackers are advancing and developing customised intrusion tools

Unit -2: NETWORK SECURITY AND DATA COMMUNICATIONS

Unit Aims

In this unit the learner will look at the component parts of digital communications and interoperability with IT networks, hardware, firmware and software components. The inherent insecurity of the internet will be described and discussed. What are the basics of computer science and technology? How do computers communicate with one another? How can networks communicate and how can we plan their security architecture in a more proactive and organised manner? The second half of this unit will look at security planning and core concepts including 'security engineering', systems hardening and cyber resilience.

LEARNING OUTCOMES

- Understand how computers and digital devices communicate with one another over a network
- Understand, at a strategic level, how computer networking, web applications and software can be exploited
- Understand methods of security prevention and systems hardening
- Understand key network security and systems resilience tools, terminology and models

Unit -3: DATABASE SECURITY AND COMPUTER PROGRAMMING

Unit Aims

Database security concerns the use of a broad range of information security controls to protect databases against compromises of their confidentiality, integrity and availability. In this unit the learner will explore security risks to database systems and mitigation techniques. Understanding the function of computer programming is essential to understanding the dark arts of 'Black Hat Hackers'. Learners will examine (as a rolling case study) Python as a popular contemporary programming language. The symbiotic link between developments in computer programming and vulnerabilities to hacking will be examined and explored.

LEARNING OUTCOMES

- Understand the broad range of information security controls to protect databases
- Understand types of database categories of control
- Understand the underpinning concepts and models of cloud-based storage solutions
- Understand the relationship between computer programming and computer hacking
- Understand the 'interpreted' general-purpose programming language, Python

Unit -4: INCIDENT RESPONSE, INVESTIGATIONS AND FORENSICS

Unit Aims

In this unit the learner will examine Incident Response, Computer Emergency Response Teams (CERTS), and events requiring investigative techniques. Learners will identify and examine aligned business tasks and task forces including Disaster Recovery, Business Continuity Management and Crisis Management. The unit then focuses on exploring cyber-related incident investigations, including evidential analysis gathering, logging and reporting.

LEARNING OUTCOMES

- Understand the role and composite parts of Incident Response as a business function and how CERTS operate
- Understand aligned task/task forces for Business Continuity, Disaster Recovery and Crisis Management
- Understand how major computer incidents are formally investigated
- Understand laws and guidance in relation to the conduct of planned and structured major incident investigations

Unit -5: SECURITY STRATEGIES: LAWS, POLICIES AND IMPLEMENTATION

Unit Aims

Knowing how to build a cyber defence strategy, what legal tools require consideration, how policies can be written and embedded, are all vital ingredients to successful in-house cyber security practices. In this unit the learner will bring together knowledge acquired from previous units and build on this in relation to developing plausible strategic plans, executive buy-in and legal compliance.

LEARNING OUTCOMES

- Understand the concept of strategy, strategic management, planning and buy-in in relation to cyber security
- Understand how legislation, formal industry standards, training and accreditations support cyber security
- Understand how to implement Plan, Do, Check and Act security and risk management policies
- Understand the future legal and technical environment and the impact on cyber security planning and digital risk management
- Understand how to plan and design a security audit for a cyber network

Unit -6: CYBER WARS

Unit Aims

In this unit the learner will look at the emerging cyber offensive and defensive strategies of nation states that reportedly engage in what is called 'cyber war' or 'information warfare'. What nation-state governments have the most advanced cyber capabilities? How might they be used to defend or attack an institution, group or infrastructure? Why is this knowledge important for cyber security practitioners based within businesses? As part of this unit learners will analyse geopolitical considerations in relation to cyber security incidents and also explore the direct, likely implications, for their business organisations, and surrounding Critical National Infrastructure (CNI), that might get caught up in widescale disruption and long-term power outage.

LEARNING OUTCOMES

- Understand how nation states are potentially engaged in cyber defence and offensive capability strategy
- Understand the motivations and causes behind nationstate-linked cyber-attacks and breaches
- Understand how private sector industry has been targeted by potentially state sanctioned cyber-crime groups and/or armies
- Understand how CNI has been targeted by state backed cyber-crime groups and/or armies

Unit -7: CRYPTOGRAPHY

Unit Aims

The process of encrypting and decrypting information forms the basis of much computer, device and network security. Cryptography is designed and used to protect the confidentiality, integrity and authenticity of information. From the very beginnings of computing, and throughout the industry's evolution, the establishment of policies, guidelines and laws has shaped the disciplines of information security and organisational resilience in profound and, often, unintended, ways. In this unit learners will be introduced to the concept and history of cryptography, and its subdisciplines (including cryptology), and how cyber-enabled networks and devices have their communications security underpinned by cryptographic methods and sector standards. Learners will explore methods of attack, including side-channel, additional encryption methods and escrow principles and key. Learners will look at how businesses can deploy encryption to enhance their information security approaches. Learners will develop an understanding of security technical and generic management and leadership teaching.

LEARNING OUTCOMES

- Understand key cryptographic principles and modes
- Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption enabled networks and devices
- Design an encryption plan and courses of action for a given organization.

Unit -8: DIGITAL INVESTIGATIONS AND FORENSICS

Unit Aims

This unit describes and explains how to conduct investigations with cyber-enabled equipment, including on public-internet-facing networks, or other network environments. Much evidence is lost or ruled inadmissible within courts and tribunal environments because it has been mishandled and corrupted (or could have been) by investigators, or those with a perceived chain of custody over the data. Moreover, in a planet of several billion cyber-enabled devices, but few qualified cyber investigators, it is now the case that many organisations have to manage part or all of a cyber incident investigation, because the national CERT or police/security agencies are otherwise prioritised. In this unit learners will examine the requirements for digital investigations including team formations and tools, understanding the prospects of recovering information, gathering evidential data (including from mobile and IoT devices), safeguarding evidential integrity, as well as the complexity and challenges of storing and presenting evidence within legal environments. Learners will develop an understanding of security technical and generic management and leadership teaching.

LEARNING OUTCOMES

- Understand the core principles of digital investigations
- Apply the types of tool that support professional digital investigations at a strategic level
- Plan for an investigations and forensics teams
- Understand the importance of safeguarding evidential integrity in digital investigations

Unit -9: COMMUNICATIONS AND INCIDENT MANAGEMENT

Unit Aims

In this unit learners will explore the types of site, personnel and equipment required in relation to planning for Incident Management and forming an organisational CERT team (Computer Emergency Response Team). They will then explore the core sub-disciplines and side-disciplines of Cyber Incident Management: Disaster Recovery, Business Continuity Management and Crisis Management. Learners will discuss the importance of the business organisational requirement for skilled and planned communications to operate in combination with advanced and developed management responses and strategy.
Learners will develop an understanding of the security technical and generic management and leadership teaching.

LEARNING OUTCOMES

- Understand the physical and human resources required to manage a major suspected cyber security incident
- Apply Business Continuity Management to major incident planning and response
- Understand how Disaster Recovery and Crisis Management are integrated into a suspected major cyber-enabled incident
- Evaluate the potential impact of NOT planning crisis communications and incident response

Unit -10: STRATEGIC LEADERSHIP

Unit Aims

In this unit learners will develop an understanding of the key features of tech leadership and performance management. Learners will evaluate strategic leadership and management approaches, within a tech sector setting, and what it means to be a 'senior level influencer'.
Learners will also develop an understanding of security technical and generic management and leadership teaching.

LEARNING OUTCOMES

- Understand the role senior leaders and strategic leadership
- Evaluate the management streams and performance monitoring mechanisms that relate to information security
- Understand how threat and risk identification and management is integrated
- Understand how data protection legislation impacts considerations of strategy-setting and strategic leadershi

STAGE 2

This stage is of 12 months duration and is delivered by the University through IDM. Upon successful completion of Stage 1, learners can progress to the top-up of the Cyber Security program from University of Gloucestershire, UK. Stage 2 is also delivered online via the university Learning Management System (LMS) by faculties from IDM and the university. On successful completion of Stage 2, learners will be awarded BSc (Hons) Cyber Security from University of Gloucestershire, UK.

UNITS

- Advanced Topics in Technology and Innovation
- Cyber Security Management
- Advance Networking and Security
- Dissertation Research Methods
- Secure Coding
- Dissertation

UNIT SPECIFICATIONS

Unit -1: ADVANCED TOPICS IN TECHNOLOGY AND INNOVATION

Unit Aims

The unit provides the learner with the opportunity to research current innovative issues in technology. The topics will be introduced in a series of lectures and then discussed in seminars with the student contributing written and verbal content.

LEARNING OUTCOMES

- Develop knowledge and understanding of key contemporary computer science topics and issues
- Explore, grasp, and debate the underlying technologies behind a range of emerging, bleeding-edge technologies with an emphasis on computing technologies that are highly likely to reach the market within the next 5-10 years
- Demonstrate research skills through critical review and evaluation of research publications as well as through the publication of a scientific paper-style report.

Unit -2: CYBER SECURITY MANAGEMENT

Unit Aims

The unit aims to critically evaluate and synthesize cybersecurity management. It addresses the socio-technical elements of cyber security. Learners will learn about the strategic components of cyber security; governance, and aligning cyber security strategy with business requirements, goals, and objectives. It explains about protecting organizations, threat identification, risk assessment and management, security context, breach management, cyber security roadmaps, and frameworks. The unit enables the learner to understand how to design a cyber-intelligence framework for organizations.

LEARNING OUTCOMES

- Critically evaluate and synthesize cyber security management components to understand and develop a cyber-intelligence framework for organizations;
- Critically analyze and evaluate the components of cyber security governance to sustain and improve the security posture of an organization;
- Analyse and evaluate the legal, ethical, and privacy concerns and frameworks of cyber security management
- Critically evaluate cyber security policies, standards, processes, guidelines, and baselines;
- Evaluate and synthesize the components of risk management, operational security, auditing, assurance, and review;
- Effectively communicate the various areas and topics of cyber security management, present arguments, and analysis clearly and concisely to stakeholders and management.

Unit -3: ADVANCED NETWORKING & SECURITY

Unit Aims

This unit aims to defend and protect the network infrastructure, architecture, protocols, and applications to deliver secured protocols, applications, services, and data. The cyber security framework of identifying, protecting, detecting, responding, and recovering network security will be evaluated and critically analyzed during the module.

LEARNING OUTCOMES

- Critically analyze and evaluate risk analysis and management strategies to address the associated risks, threats, vulnerabilities, and attack vectors against network architectures to secure the operational and service delivery requirements;
- Critically evaluate the organizational security requirements for a network security solution against known regulations, standards, legislation, policies, and procedures to develop a systematic solution to the network and organizational security requirements;
- Demonstrate the ability to understand and synthesize the principles of network security architectures and security frameworks and models;
- Critically analyze and evaluate network security controls and mitigation techniques: network monitoring, firewalls, traffic filtering, intrusion detection and prevention systems, intrusion analysis, anti-malware, cryptography, securing network protocols, services, applications, and data to mitigate the identified risks of the evaluated system;
- Analyse several advanced networking topics and future networking direction;
- Critically evaluate and communicate network security alternatives arguments, assumptions, abstract concepts, and data to make judgments, and to frame appropriate questions to achieve a solution - or identify a range of solutions - to a given problem, to both technical and non-technical stakeholders.

Unit -4: DISSERTATION RESEARCH METHODS

Unit Aims

The unit aims to provide learners with an in-depth study of the practical and theoretical skills required to read, understand, and undertake academic research in computing-related disciplines. It includes planning and preparing a detailed proposal for a project suitable for learners. Both qualitative and quantitative methods are also covered including practical data collection and analysis. Research paradigms and research ethics for research with or without human participants are outlined and explored.

LEARNING OUTCOMES

- Critically analyze, evaluate and synthesize academic and other suitable research materials
- Design a research methodology to identify and address the research gap
- Justify your choice of research methodology and tools
- Develop an appropriate/relevant primary research project proposal that will form the foundation of your Dissertation

Unit -5: SECURE CODING

Unit Aims

The unit explores a range of recognized software security problems using motivational examples. It looks at the fundamental sources of vulnerabilities arising at the programming level including inadequate handling of exception situations, poor understanding of the details of the programming language in use, incomplete descriptions of the interface between components, and insufficient care in the treatment of concurrency and threading issues, and how these relate to evolving threat models.

LEARNING OUTCOMES

- Explain and evaluate the fundamental theories of a range of security failures that are due to software vulnerabilities.
- Apply techniques, tools, and understanding for implementing secure software to avoid flaws.
- Critically evaluate security-enhanced programming models and use appropriate tools which help ensure security goals.
- Analyse security-critical code fragments and incorporate appropriate practices within a systems development methodology

Unit -6: DISSERTATION

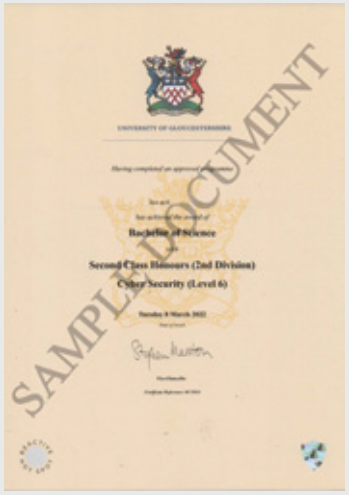
The dissertation should be of approximately 15000 words

WHAT YOU WILL EARN

You will receive the following certificates after the successful completion of the program:

Level 5 Diploma
QUALIFI, UK

Level 4 Diploma
QUALIFI, UK



Bachelors Degree
University of Gloucestershire, UK

Bachelors Program Certificate
SNATIKA

Disclaimer: The above images are for reference purposes only.

WHY CHOOSE SNATIKA?

SNATIKA programs offer the best value for the investment that a learner makes in her/his education.

- Level 5 Diploma from QUALIFI, UK
- Level 4 Diploma from QUALIFI, UK
- Bachelors Degree from University of Gloucestershire, UK
- Bachelors Program Certificate from SNATIKA

Accreditation ensures that quality and regulatory standards are met.

SNATIKA is an approved learning centre of Qualifi, UK. Qualifi is an awarding organisation in the UK, which is regulated by the OFQUAL (Office of Qualifications and Examinations Regulation) and Qualifications Wales. Since Ofqual also regulates the National Curriculum Assessments in England, SNATIKA students get to study the same course units as their peers taking the same qualification in the UK.

QUALIFI APPROVED CENTRE

IDM Creating Opportunities Nurturing Achievers

SNATIKA has also partnered with IDM to award their learners UK graduate and masters' degrees.

IDM has over 4 decades of experience in the higher education sector. Having closely worked with the industry, and bringing in global education to local students, IDM has pioneered the way forward in getting international recognition to talented students.

The University of Gloucestershire, a UK state university, is the degree-awarding institution.It is located in the edge of the stunning Cotswolds and has three campuses which are based in Cheltenham and Gloucester.

The credits earned for the Diploma from Qualifi (approved and regulated by Ofqual, UK) while doing the bachelors program from SNATIKA are recognised by the University of Gloucestershire. This partnership with the university is through IDM.

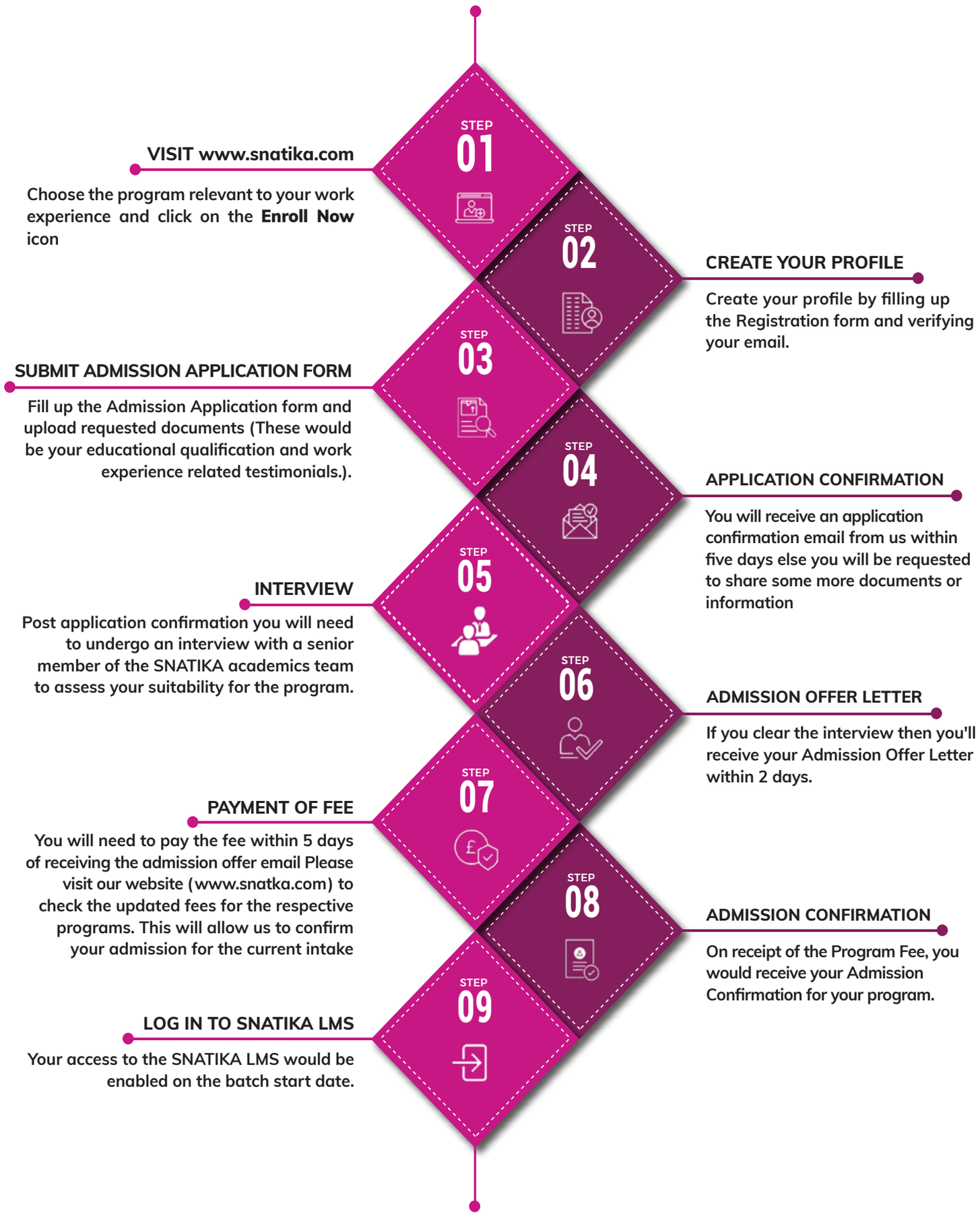
UNIVERSITY OF GLOUCESTERSHIRE

The qualifications earned through SNATIKA are awarded by government bodies and respected by businesses globally.

Admission Process

SNATIKA has limited seats for each program. Therefore we follow a first-come, first-served process of admission and applications are evaluated as soon as they are received. The earlier you apply, the better your chances are for securing your admission to our Bachelors program given that all the documents and requirements are satisfied.

The step-by-step admission process is outlined below.



For more details visit : **www.snatika.com**

INFORMATION

State of the art LMS

The program delivery happens through the robust and user friendly SNATIKA LMS (Learning Management System). It is accessible 24x7 from anywhere in the world.

The SNATIKA pedagogy

Our Bachelors programs have been designed by SNATIKA's Subject Matter Experts who have decades of experience in the education industry. The pedagogy is smartly designed to fit the program content into the busy schedules of professionals. You will need just 2 - 3 hours of daily input to succeed in the program.

The immersive nature of the syllabus, coupled ideally with the learner's experience, makes the program easier to comprehend and complete in the shortest duration. The assignment based assessment makes the learner grasp the concepts from the roots and enhances the research, critical thinking, and writing skills thereby.

PhD Level Guides

SNATIKA learners will be supported by our PhD level Guides upon the batch start date. SNATIKA's PhD level Subject Matter Experts will help you with all the challenges you face academically throughout the program.

Session Dates

Aspiring candidates may join in any one of our yearly sessions.

You can check the website (www.snatika.com) for current information on the closing date of admissions and the batch start date.

Selection Process

Selection is based on the details provided during the application process. Admission is granted on a first-come-first-served basis.

INFORMATION

Program Format- Online

The entire duration of the bachelors program is delivered through state-of-the-art Learning Management Systems.

You'll study the first stage through SNATIKA's LMS and the second stage is delivered through the our partner's LMS.

Duration of the Program

The duration of the program is 18 - 24 months. The initial six - twelve months are for Stage 1 (Mandatory Units) and the last twelve months are for Stage 2 (university top-up).

This duration only changes in case you fail to meet the requirements of the assignment and the deadline passes.

Program Fees

Please visit our website (www.snatika.com) to check the updated fees for the respective programs.

All learners are required to deposit the fee in full within 5 days of receiving the admission offer letter email.

To ease the financial burden on your shoulders, we offer an Instalment option for depositing the program fee.

SNATIKA™

Boosting Careers of Professionals

For further details

web: www.snatika.com | email: info@snatika.com

INDIA	NIGERIA	SOUTH AFRICA	REST OF THE WORLD
+91 8047183355	+234 1 8880209	+27 21 8259877	+ 44 20 3287 6900