NATIONAL OPEN UNIVERSITY OF NIGERIA

Outlined Programme Proposal (OPP) and Detailed Programme Proposal (DPP)

for

B. Sc. Cybersecurity

in the

Faculty of Computing

for

SENATE Approval

2024

1. Name of the Programme: B.Sc. Cybersecurity

Programme Code: 52

Overview

Recent developments in computing, network technologies, internet, and cloud technologies have generated the need for reliability and secure exchange of digital information that are vital to most human activities such as banking, medicine, infrastructure management and elections. As the use of information technology expands, so are the potential consequences of cyber-attacks, and the need for a skilled workforce to prevent and defend against them. However, the pool of available talent to build and certify applications designed to withstand attacks, diagnose and prevent security intrusions is inadequate to meet the growing needs all over the world. Government agencies, business organisations, industries and military are scrambling to find qualified professionals to safeguard their systems, businesses and infrastructures.

The focus of this programme is to equip students with sufficient knowledge, and skills to minimise and prevent cybersecurity threats and incidents. Students are also equipped with demonstrable abilities to gather, analyse, and present evidence of any cybersecurity bridges in organisation in a professional way. The graduates of this programme will understand the impact of cybercrime on business and the public and be able to identify and implement specific security practices, features and techniques to enhance the security of computers, computer-based systems and cyberspace.

2.0 Philosophy, Aims and Objectives

2.1 Philosophy

The philosophy of the B.Sc. Cybersecurity programme in NOUN leverages on the following key concepts:

The Department of Cybersecurity seeks to build and develop human capacity to high level through a comprehensive, flexible and accessible educational programme, research in collaboration with industry and the government. We hope to deliver an experience that prepares our students for success in their career, thus moulding them into job creators rather than job seekers after graduation.

The philosophy of the programme is to build capacity and develop human capital in the field of cybersecurity, to safeguard business transactions, corporate assets, critical infrastructure and all cyber operations in cyberspace, nationally and globally

The students will be grounded in theoretical and practical aspects of cybersecurity so that they are capable of finding effective solutions to real world problems using state-of-the arts skills acquired in the period of their study. They will be prepared and better equipped to safeguard business transactions, corporate assets, critical infrastructure and all cyber operations in cyberspace, nationally and globally.

2.2 Aim

The B. Sc Cybersecurity Programme aims at giving the undergraduate students a broad-based knowledge in areas network security, information security and security in the cyber space and to prepare them for specialization in these areas at the postgraduate levels.

2.3 Objectives

The B.Sc. Cybersecurity is designed mainly to make the students be up-to-date with emerging developments in Cybersecurity as well as develop sufficient skills in programming. Thus, at the end of the programme, graduates should be endowed with the following skills and abilities:

1) Possess requisite foundation knowledge of cybersecurity, skills and strategies that would enable them to detect and prevent cyber-fraud;
2) Capable of analysing cybersecurity threats, attacks and risks for organisations, with the capacity to develop detective codes and supportive software agents to address cybersecurity threats;
3) Possess knowledge of cryptography and steganography for privacy of information on computer systems and digital forensic science techniques for the detection of cybercrimes;
4) Critically think about cyber intelligence security issues, develop and implement tactics strategic to cybersecurity, drawing on national and international recent case studies;
5) Drive for self-employment, eligibility for cybersecurity-based job placement and professional practice in government and industries.

3.0 Unique Features of the Programme

The uniqueness of the cybersecurity programme is the introduction of big data analytics, cyber threat intelligence and cyber conflict, deep and dark web security, cyber threat hunting, monitors and controllers, artificial intelligence cyber defence application and surveillance in cyber defence operations.

3.1 Employability Skills

Cybersecurity skills are hard skills that are required in all jobs. The employability skills are grouped into soft and hard skills along with technical and implementation skills. Graduates

of Cybersecurity will have:

i. Soft skills of excellent presentation and communication skills, ability to clearly articulate complex cyber-concepts, and usage of active listening skills.

ii. Technical skills in understanding the architecture, administration, and management of operating systems, networking, and virtualization software; usability of firewalls and network load balancers; software development concepts and software analytics skills; common programming languages; and obtaining cybersecurity certifications essential and prerequisite for employment

iii. Implementation skills of cyber hunting, cyber intelligence, and cyber threat modelling, vulnerability assessment; identify the cybersecurity controls in place and how they are used, and use of the coding skills to write codes that automate cybersecurity tasks.

3.2 21st Century Skills

Cybersecurity students will be required to have the following 21st-century skills:
Problem-solving skills and critical thinking. Communication skills, Creativity, Collaboration; Information literacy, Global awareness. Innovation skills and social skills**.**

4.0 Entry and Graduation Requirements

Entry Requirements

To be admitted for the B. Sc. Cybersecurity programme, a candidate is expected to:

i. Have at least five credits passes in SSCE, NECO, GCE 'O' level or 6 merits in NABTEB or TC II examinations. The credit passes must include English, Mathematics, Physics as core courses and any other two credits passes from Chemistry, Biology, Further Mathematics, Computer studies and Agricultural Science at maximum of two (2) sittings

ii. Have the NCE level examination with merit pass in mathematics in addition to a credit pass in any other science subject preferably Physics or Chemistry for entry into 200 level of the programme in addition to (i) above for consideration into 200 level of the programme.

iii. Have JUPEB or its recognized equivalent qualifications or GCE Advance level in mathematics and physics or OND (upper class category) /HND/BSc in addition to (i) above for consideration into 200 level of the programme.

Graduation Requirement

To be eligible for the award of the Bachelor degree in Cybersecurity, a student must have:

i. Passed all the core courses, university and faculty/school required courses and electives.

ii. To graduate, a student must be found worthy in character throughout the period of his/her studentship and must accumulate the total units prescribed for the programme from Core, Faculty and General Studies courses as well as SIWES, Seminar and Final Year Project.

5.0 Programme Structure and Degree Rules

5.1 Outline of Course Structure.

The B. Sc., H*onours*, Cybersecurity programme is structured in 8 semesters as shown below. However, a 6-semester structure can be attempted if the entry level is at the 200 Level.

A. Outlined Programme Proposal

100 Level

First Semester					
Course Code	**Course Title**	**Unit(s)**	**Status**	**LH**	**PH**
GST101	Use of English and Communication Skills I	2	C	15	45
[1]GST103	Computer Fundamentals	2	C	30	45
COS101	Introduction to Computer Science	3			
GST107	The Study Guide for the Distance Learner	2	C	15	45
MTH101	Elementary Mathematics I	2	C	30	0
PHY101	Elementary Mechanics, Heat and Properties of Matter	2	C	30	0

PHY191	General Practical Physics I	1	C	0	45
STA111	Descriptive statistics	3	C	45	0
NOU-CYB-191	Cybersecurity Practical I	1	C	0	45
NOU-CYB-111	Fundamentals of Cyber Security	2	C	0	45
Total Compulsory					**20**
Total Elective					**0**
Total required					**20**
*** Students are expected to offer at least ONE elective course this semester. Also, they can only register a maximum of 25 units per semester**					
Second Semester					
GST 102	Use of English and Communication Skills II	2	C		
GST104	Use of Library	2	C		
MTH 102	Elementary Mathematics II	2	C	30	0
PHY 102	Electricity, Magnetism and Modern Physics	3	C	30	0
PHY 192	General Practical Physics II	1	C	0	45
COS102	Problem Solving Algorithm	3	C	30	45
NOU-CYB-122	Ethics and Professional Practice in Cybersecurity	2	C	45	0
NOU-CYB-192	Cyber Security (Tools) Practical II	1	C	0	45
NOU-CYB-126	Security in Social Networks	3	C	30	0

Total Compulsory	**19**
Total Elective	**-**
Total required	**19**
*** Students are expected to offer at least one elective course per semester. Also, they can only register a maximum of 25 units per semester**	

200 Level

First Semester

Course Code	**Course Title**	**Unit(s)**	**Status**	**LH**	**PH**
GST201	Nigerian Peoples and Cultures	2	C	45	0
GST203	Introduction to Philosophy and Logic	2	C	45	0
COS201	Introduction to Programming Languages	3	C	45	0
CYB201	Introduction to Cybersecurity and Strategy	2	C	30	0
CYB203	Cybercrime, Law and Countermeasures	2	C	30	0
CYB299	SIWES I	3	C	0	135
SEN 201	Introduction to Software Engineering	2	C	30	0
NOU-CYB-211	Web Hacking	2	E	30	0
NOU-CYB-213	Information Security Models	2	E	30	0
Total Compulsory					**16**
Total Elective					**4**

Total required					**18**
*** Students are expected to offer at least ONE elective course this semester. Also, they can only register a maximum of 25 units per semester**					
Second Semester					
GST 202	Fundamentals of Peace Studies and Conflict Resolution	2	C	30	0
GST204	Entrepreneurship and Innovation	2	C	30	0
COS202	Computer Programming II	3	C	30	45
INS204	Systems Analysis and Design	3	C	30	45
NOU-CYB-222	Introduction to Networking	3	C	45	0
NOU-CYB-224	Python for Cyber security	2	C	15	45
NOU-CYB-226	Introduction to Cryptography	2	E	15	45
NOU-CYB-214	VoIP and Multimedia Security	2	E	30	15
Total Compulsory					**15**
Total Elective					**4**
Total required					**17**
*** Students are expected to offer at least one elective course per semester. Also, they can only register a maximum of 25 units per semester**					

NOTE: ***SIWES I and II will take place during long vacations of 200 Level and 300 Level.

300 Level

First Semester

Course Code	**Course Title**	**Unit(s)**	**Status**	**LH**	**PH**
CYB301	Cryptography Techniques, Algorithms and Applications	2	C	15	45
CYB303	Cybersecurity Risks Analysis, Challenges and Mitigation	2	C	30	0
CYB305	Digital Forensics and Investigation Methods	2	C	15	45
CYB399	SIWES II	3	C	0	135
CSC309	Artificial Intelligence	3	C	15	45
NOU-CYB-321	Network Security	2	C	30	45
NOU-CYB-323	IOT Security and Privacy	3	E	30	45
NOU-CYB-317	Cyber Privacy and Data Protection	2	C	45	0
NOU-CYB-319	Information Security Engineering	2	E	30	15
Total Compulsory					**16**
Total Elective					**4**
Total required					**18**
*** Students are expected to offer at least ONE elective course this semester. Also, they can only register a maximum of 25 units per semester**					
Second Semester					
ENT 312	Venture Creation	2	C	15	45
CYB302	Biometrics Security	2	C	15	45
CYB304	Information and Big Data Security	2	C	15	45

CYB322	Cybersecurity Innovation and New Technologies	2	C	15	45
NOU-CYB-308	Web Application Security	2	C	30	45
NOU-CYB-310	Information Security Audit	2	E	45	0
NOU-CYB-316	Cyberpreneurship	2	C	30	0
NOU-CYB-312	Critical National Information Infrastructure Protection	2	C	45	0
NOU-CYB-314	Application of Data Mining in Cyber Security	2	E	30	45
NOU-CYB-326	Project Management in Cybersecurity	3	C	30	45
Total Compulsory					**17**
Total Elective					**4**
Total required					**19**
*** Students are expected to offer at least one elective course per semester. Also, they can only register a maximum of 25 units per semester**					

400 Level

First Semester					
Course Code	Course Title	Unit(s)	Status	LH	PH
COS409	Research Methodology and Technical Report Writing	3	C	45	0
CYB401	Systems Vulnerability	2	C	15	45

	Assessment and Testing				
CYB403	Cyber Threat Intelligence and Cyber Conflict	2	C	30	0
CYB405	Ethical Hacking and Reverse Engineering	2	C	15	45
CYB499	Final Year Project I	3	C	0	135
NOU-CYB-415	Disaster and incidence Risk Management	2	E	45	0
NOU-CYB-489	Current Trends in Cybersecurity (Seminar)	3	C		
NOU-CYB-425	Cyber Warfare and Defense	2	E	30	45
Total Compulsory					**15**
Total Elective					**4**
Total required					**17**
*** Students are expected to offer at least ONE elective courses this semester. Also, they can only register a maximum of 25 units per semester**					
Second Semester					
CYB402	Steganography-Access Methods and Data Hiding	2	C	15	45
CYB404	Cloud Computing Security	2	C	30	0
CYB406	Deep and Dark Web Security	2	C	15	45
CYB498	Final Year Project II	3	C	0	135
NOU-CYB-414	Network Threats and Risk Assessment	2	C	30	45
NOU-CYB-422	Mobile Network Security	2	E	30	45

NOU-CYB-426	E-Business Security	2	E	15	45
Total Compulsory					**11**
Total Elective					**4**
Total required					**13**
*** Students are expected to offer at least one elective course per semester. Also, they can only register a maximum of 25 units per semester**					

SYNOPSES OF COURSES AND DETAILED PROGRAMME PROPOSAL (DPP)

GST 101 Use of English and Communication Skills I (2 Units)

Listening- enabling skills, listening and comprehending, note taking and information retrieval. Including data, figures, diagrams and charts, Listening for main idea, interpretation and critical evaluation. Effective reading, skimming and scanning. Reading and comprehension at various speed levels. Vocabulary development in various academic context. Reading diverse texts in narratives and expository. Reading and comprehension passages with tables, scientific texts. Reading for interpretation and critical evaluation.

GST 102 Use of English and Communication Skills II

Writing paragraphs: Topic sentence and coherence. Development of paragraphs: illustration, description, cause and effect including definitions. Formal letters: essential parts and stylistic forms; complains and requests; jobs, ordering goods, letters to government and other organisations. Writing reports; reporting event, experiments. Writing summaries; techniques of summarising letters and sounds in English, vowels and consonants. Interviews, seminar presentation, public speech making, articles, concord and sentences including tenses. Gerund, participles, active, passive and the infinitive. Modal auxiliaries.

GST103: COMPUTER FUNDAMENTALS (2 Units)

Introduction to Computer, basic concepts, classifications of computers, historical views of computer. Threats to computer system, Computer Hardware and Software. Overview of computer programming languages. Detailed discussion of Computer Applications in various field.

GST104: USE OF LIBRARY(2 Units)

Identifying sources of Information, concept of library and library services, history of libraries. ICT use in the library, Copyright, Plagiarism and bibliographic Citation & referencing, functions and services of research libraries.

GST 107: The Study Guide for the Distance Learner (2 Units)

Getting started: How to use the book, why read about skills, getting yourself organised ; what is studying all about, reading and note taking; Introduction, reactions to reading, your reading strategy, memory, taking notes, conclusion. Other ways of studying: Introduction, learning in groups, talks and lectures, learning from TV and radio broadcasts, other study media. Working with numbers; Getting to know numbers, describing the world, describing with the tables, describing with diagrams and graphs; What is good writing? The Importance of writing, what does an essay look like, what is a good essay? Conclusion. How to write essays: Introduction, the craft of writing, the advantages of treating essay writing as a craft, making your essay flow, making a convincing case, the experience of writing. Preparing for examination.

MTH101 ELEMENTARY MATHEMATIC I: (3 Units)

(ALGEBRA AND TRIGONOMETRY)

Elementary set theory, subsets, union, intersection, complements, venn diagrams. Real numbers; integers, rational and irrational numbers, mathematical induction, real sequences and series, theory of quadratic equations, binomial theorem. Complex numbers; algebra of complex numbers; the Argand Diagram. Re Moivre's theorem, nth roots of unity. Circular measure, trigonometric functions of angles of any magnitude, addition and factor formulae.

MTH102 ELEMENTARY MATHEMATICS III: (3 UNITS) CALCULUS:

Function of a real variable, graphs, limits and idea of continuity. The derivative as limit of rate of change, Techniques of differentiation, Extreme curve sketching. Integration as an inverse of differentiation, Methods of integration, Definite integrals; Application to areas and volumes

PHY101: Elementary Mechanics, Heat and Properties of Matter (2 UNITS)

Space and Time: Physical quantities: Units and dimensions of physical quantities; Kinematics: Uniform velocity motion, uniformly accelerated motion; Dynamics: Newton's laws of motion; Impulse and Linear Momentum, Linear Collision, Newton's universal law of gravitation; Work, energy and power; Conservation laws; Concept of mechanical equilibrium; Centre of mass and centre of gravity; Moment of a force; Rotational kinematics and dynamics: Torque; Moment of Inertia; angular momentum; Total mechanical energy. Simple harmonic motion

Heat and temperature, work and heat, Quantity of heat: heat capacities, latent heat; Thermal expansion of solids, liquids and gases; Gas laws, heat transfer; Laws of thermodynamics: Isothermal and Adiabatic changes, Carnot cycle; Application kinetic theory of gases; van der Waals gas.

Classification of matter into (solids, liquids and gases, forces between atoms and molecules, molecular theory of matter, Elasticity, plasticity, Hook's Law, Young's Shear and bulk Moduli) Crystalline and non-crystalline materials, Hydrostatics: pressure, buoyancy, Archimedes' principle; Hydro-dynamics-streamlines, Bernouli and Continuity equations, turbulence, Reynold's number, Viscosity, laminar flow, Poiseuille's equation; Surface tension, adhesion, cohesion, capillary, drops and bubbles.

PHY102: ELECTRICITY, MAGNETISM AND MODERN PHYSICS (3 UNITS)

Electrostatics: Coulomb's law, Gauss's law, potential and capacitance, dielectrics, production and measurement of static electricity. Current: Ohm's law, resistance and resistivity, heating. Galvanometers, Voltmeters and Ammeters; D.C. circuits: sources of emf and currents, Kirchhoff's laws; Electrochemistry; The Earth's magnetic field; Magnetic fields and induction, Faraday's and Lenz's laws; Force on a current-carrying conductor. Biot-Savart law. Flemming's right and left-hand rules, motors and generators. A.C. Theory. Atomic structure; Production and properties of X-rays; Radioactivity; Photoelectric emission.

PHY191: INTRODUCTORY PRACTICAL PHYSICS I (1 UNIT)

Graphs, Measurement, Error Analysis, Determination of Acceleration due to Gravity by Means of Simple Pendulum, Determination of force constant of a spiral spring, Determination of effective mass of a spiral spring and the constant, Determination of surface tension of water, Determination of specific latent heat of fusion of ice, Determination of the co-efficient of limiting static friction between two surfaces, Determination of the co-efficient of static friction on two surfaces using an inclined plane, Determination of Relative Density of kerosene using the specific Gravity Bottle, Determination of the Relative Density of a Granular substance not soluble in water using the specific gravity bottle.

PHY 192: General Practical Physics II (1 UNIT)

This practical course is a continuation of PHY 107 and is intended to be taught during the second semester of the 100 level to cover the practical aspect of the theoretical courses that have been covered with emphasis on quantitative measurements, the treatment of measurement errors, and graphical analysis. However, emphasis should be placed on the basic physical techniques for observation, measurements, data collection, analysis and deduction.

STA111: Descriptive statistics (3 UNITS)

Permutation and combination. Concepts and principles of probability. Random variables.

Probability and distribution functions. Basic distributions: binomial, geometric, poisson, normal and sampling distributions; exploratory data analysis.

COS 101: Introduction to Computing Sciences (3 Units C: LH 30; PH 45)

Brief history of computing. Description of the basic components of a computer/computing device. Input/Output devices and peripherals. Hardware, software and human ware. Diverse and growing computer/digital applications. Information processing and its roles in society. The Internet, its applications and its impact on the world today. The different areas/programs of the computing discipline. The job specializations for computing professionals. The future of computing. Lab Work: Practical demonstration of the basic parts of a computer. Illustration of different operating systems of different computing devices including desktops, laptops, tablets, smart boards and smart phones. Demonstration of commonly used applications such as word processors, spreadsheets, presentation software and graphics. Illustration of input and output devices including printers, scanners, projectors and smartboards. Practical demonstration of the Internet and its various applications. Illustration of browsers and search engines. How to access online resources.

NOU-CYB-111: Fundamental of Cyber Security/ Cyber-Security I (2 UNITS)

Introduction to network and cyber security. Network design elements and components. Compliance and operational security. Cyber security threats and vulnerabilities. Types of cyber attacks. Risk mitigation strategies. Appropriate security controls. Disaster recovery plans and procedures. Application, data and host security. Access control and identity management. Cryptography introduction. Intrusion detection systems. Intrusion prevention systems. Firewall and access control. Security policies and controls. Responding to a security breach. Elements of security management. Cyber Essentials and the NIST standards. Incident response management.

NOU-CYB-113: Fundamental of Information Security & Criminal Justice (2 UNITS)

NOU-CYB-211: Web Hacking (2 UNITS)

Understanding the HTTP protocol: HTTP protocol basics, proxy tools, and techniques for information gathering, enumeration techniques and understanding the web attack surface. Additionally, issues with the Secure Sockets Layer (SSL) and Transport Layer Security (TLS), focusing on SSL/TLS misconfigurations, username enumeration, and faulty password reset mechanisms, attacks on authentication, and second-factor authentication bypasses. Broken access control, role-based authorization bypasses such as horizontal and vertical privilege escalation attacks, insecure direct object reference attacks, and security misconfigurations. Cross-Site Scripting (XSS), types of XSS attacks, session hijacking, and server-side request forgery (SSRF) attacks, including their impacts. SQL Injection (SQLi), SQL injection types and methods for both manual and automated exploitation, XML External Entity (XXE) attacks. Insecure file uploads, Attacking file upload functionality and Remote code execution through malicious file uploads. Components with known vulnerabilities, including the risks introduced by these vulnerabilities and examples such as Log4J attacks. Importance of logging and monitoring, evaluating logging events, and common pitfalls in logging and monitoring practices.

NOU-CYB**NOU-CYB-191: Cybersecurity Practical I (1 UNIT)**

Hands-on exposure that focuses more on the methodologies to put cyber security concepts into practice including tools and best practices for better success rate. By performing digital forensics, penetration testing, social engineering, and other ethical hacking attacks, students can have a good perspective into the mind of attackers. Hands-on training laboratory exercises that help students to better understand topics in the cyber security field by applying them in controlled virtual environments are developed. Exposure to skill based certifications at beginner's level is encouraged.

COS102: Problem Solving Algorithm (3 UNITS)

Introduction to the core concepts of computing. Problems and problem-solving. The identification of problems and types of problems (routine problems and non-routine problems). Method of solving computing problems (introduction to algorithms and heuristics). Solvable and unsolvable problems. Solution techniques of solving problems (abstraction, analogy, brainstorming, trial and error, hypothesis testing, reduction, literal thinking, meansend analysis, method of focal object, morphological analysis, research, root cause analysis, proof, divide and conquer). General Problem-solving process. Solution formulation and design: flowchart, pseudocode, decision table, decision tree. Implementation, evaluation and refinement. Programming in C, Python etc. Lab Work: Use of simple tools for algorithms and flowcharts; writing pseudocode; writing assignment statements, input-output statements and condition statements; demonstrating simple programs using any programming language (Visual Basic, Python, C)

NOU-CYB-122: Ethics and Professional Practice in Cybersecurity (2 UNITS)

Fundamental concept of ethics, Application of ethics in cybersecurity professional practice, Relationship between ethics and cybersecurity (relevant case studies), cybersecurity professional roles and duties, Significance of ethical issues in cybersecurity, Introduction to Ethical Frameworks and principles that guide Cybersecurity practice, Application of ethical principles in Decision-making involving Cybersecurity issues, common ethical challenges for Cybersecurity Professionals, Upholding ethical considerations while handling incident response, vulnerability disclosure and data storage, Obligations of Cybersecurity Professionals towards the Public, Ethical challenges of the use of Emerging Technologies, Application of

Professional Ethics in Cybersecurity Research and Development (R & D), Procedure for adhering to Ethical Guidelines while conducting Research in Cybersecurity

NOU-CYB-126: Security in Social Networks (2 UNITS)

FUNDAMENTALS OF SOCIAL NETWORKING: Introduction to Semantic Web, Limitations of current Web, Development of Semantic Web, Emergence of the Social Web, Social Network analysis, Development of Social Network Analysis, Key concepts and measures in network analysis, Historical overview of privacy and security, Major paradigms, for understanding privacy and security. SECURITY ISSUES IN SOCIAL NETWORKS: The evolution of privacy and security concerns with networked technologies, Contextual influences on privacy attitudes and behaviors, Anonymity in a networked world. EXTRACTION AND MINING IN SOCIAL NETWORKING DATA: Extracting evolution of Web Community from a Series of Web Archive, Detecting communities in social networks, Definition of community, Evaluating communities, Methods for community detection and mining, Applications of community mining algorithms, Tools for detecting communities social network infrastructures and communities, Big data and Privacy. PREDICTING HUMAN BEHAVIOR AND PRIVACY ISSUES: Understanding and predicting human behavior for social communities, User data Management, Inference and Distribution, Enabling new human experiences, Reality mining, Context, Awareness, Privacy in online social networks, Trust in online environment, What isNeo4j, Nodes, Relationships, Properties. ACCESS CONTROL, PRIVACY AND IDENTITY MANAGEMENT: Understand the access control requirements for Social Network, Enforcing Access Control Strategies, Authentication and Authorization, Roles-based Access Control, Host, storage and network access control options, Firewalls, Authentication, and Authorization in Social Network, Identity & Access Management, Single Sign-on, Identity Federation, Identity providers and service consumers, The role of Identity provisioning.

NOU-CYB-192: Cyber Security (Tools) Practical II (1 UNIT)

Overview of cyber security, Attack Vectors, Threat, Risk and Vulnerability, Cyber Security Career paths; Cyberprenuers, Pentesters, Forensics Investigator, Cybersecurity consultant, Educators etc., Open Source and Paid Tools, Firewalls and Packet Filters., Introduction to Windows and Linux Firewall, Attacks on Wireless Networks, Scanning for Web Vulnerabilities Tools and HTTP Utilities, Hacking Tools, External reconnaissance tools, Internal reconnaissance tools, Cloud Hacking Tools; Nimbusland, LolrusLove, Bucket Lists, FDNSv2 & Knock Subdomain Scan, Prowler 2.1, flAWS, etc., Red and Blue Team Tools for Mobile Devices: Snoopdroid, Androguard, Frida, Cycript, etc., Social Engineering Toolkit, Tools for Lateral Movement: Nmap: Sysinternals, Netcat, , PsExec. etc., Privilege Escalation tools; Metasploit, EternalBlue etc., Security Monitoring Tools: Microsoft Operations Management Suite (OMS), Azure Security Center, etc., Network, Segmentation Tools; Network Performance Monitor Suite from SolarWinds, etc., Open source tools for threat intelligence: FraudGuard, Azure Sentinel, etc., Risk management tools; RiskNAV, IT Risk Management App etc., Vulnerability Management Tools: Peregrine tools, LANDesk, Management Suit, StillSecure, McAfee's Enterprise etc., Vulnerability management tools: Intruder, Patch Manager Plus, InsightVM, Azure Threat & Vulnerability Management, OpenVAS, etc.

GST201: Nigerian Peoples and Culture (2 Units)

Study of Nigerian history, culture and arts in pre-colonial times, Nigerian's perception of his world, Culture areas of Nigeria and their characteristics, Evolution of Nigeria as a political unit, Indigene/settler phenomenon, Concepts of trade, Economics of self-reliance, Social justice, Individual and national development, Norms and values, Negative attributes and conducts (cultism and related vices), Re-orientation of moral and national values, Moral obligations of citizens, Environmental problems.

GST202: Fundamentals of Peace Studies and Conflict Resolution (2 Units)

Basic Concepts in peace studies and conflict resolution, peace as a vehicle of unity and development, Conflict issues, Types of conflicts, e.g. Ethnic/religious/political/economic conflicts, Root causes of conflicts and violence in Africa, Indigene/settler phenomenon, Peace – building, Management of conflict and security. Elements of peace studies and conflict resolution, Developing a culture of peace, Peace mediation and peace-keeping, Alternative Dispute Resolution (ADR), Dialogue/arbitration in conflict resolution, Role of international organizations in conflict resolution, e.g. ECOWAS, African Union, United Nations, etc.

GST203: Introduction to Philosophy and Logic (2 Units)

An Overview of Philosophy: Definition and Scope of Philosophy; Methods of Philosophy; Branches of Philosophy; Philosophy and other Disciplines Contents; The Usefulness of Philosophy; Sources of Knowledge and Criteria for Knowing. History and Development of Philosophy: The Ancient Age of Philosophy; Medieval and Renaissance Age of Philosophy;

Modern Period of Philosophy; Philosophical Movements in The Contemporary Period; The Idea of African Philosophy. Logic: Definition and Scope of Logic; Logic's Vocabulary I; Logic's Vocabulary II; Valid, Invalid, Deductive and Inductive Arguments; Language and Its Functions. Fallacies and Definitions: Fallacies (Part One); Fallacies (Part Two); Definitions (Part One); Definitions (Part Two); Categorical Propositions Contents. Argument Forms and Law of Thought: Argument Forms; Laws of Thought**.**

GST204: Entrepreneurship and Innovation (2 Units)

Development Entrepreneurship/Intrapreneurship: An Overview of the Definitions of Entrepreneurship and Intrapreneurship; Concepts and Theories of Entrepreneurship

The Entrepreneurship Culture; Brief Biographical Studies of Prominent Nigerian Entrepreneurs; Barrier to Entrepreneurial Practice. The Nigerian Entrepreneurial Environment: The Business External Environment; Identifying Business Opportunities and Threats; Strategies for exploring opportunities in the Environment; Approaches to addressing environmental barriers. Creativity and Intellectual Rights: Intellectual Properties and its Dimensions; Copyright Laws in Nigeria; Strategies for Protection of Intellectual Property (original ideas, concepts, products, etc.). Technological Entrepreneurship: The Interface between Technology Development and Entrepreneurship; Technological Development and Entrepreneurial Opportunities; Technological Environment and Business; New Technology and Entrepreneurship Opportunities. Management and Innovation: The Concept, Nature and Types of Innovation; Innovation Theory of Entrepreneurship; Financing Innovation and New Ventures; Change Management; Technical Change and Management of Innovation.

Family Business and Succession Planning: The Concept of Family Business Contents; The Cultural Contexts of Family Business; Roles and Relationship in Family Business; Ownership Transfer and Succession in Family Business. Women Entrepreneurship: The Concept of Women Entrepreneurship; Role orientation and Women Entrepreneurial Aspirations; Contributions of Women to National Socio-Economic and Human Development; Barriers to Women Entrepreneurial Practice.

Social Entrepreneurship: The Concept of Social Entrepreneurship; Social Entrepreneurship and Value Creation; The Roles of Non-governmental Organizations in Social Entrepreneurship; Social Entrepreneurship and Funding Opportunities; Social Entrepreneurship Enhancement Factors. Business Opportunity Evaluation: Sources of Business Opportunities in Nigeria; The difference between Ideas and Opportunities; Scanning Business Opportunities in Nigeria; Environment and New Venture Idea Generation.

CIT215/COS201: Introduction to Programming Languages/Computer Programming I (3 Units)

Essentials of computer programming. Types of programming: Functional programming; Declarative programming; Logic programming; object-oriented programming. Scripting languages; structured programming principles. Basic data types, variables, expressions, assignment statements, and operators. Basic object-oriented concepts: abstraction; objects; classes; methods; parameter passing; encapsulation. Class hierarchies and programme organisation using packages/namespaces. Use of API – use of iterators/enumerators, List, Stack, Queue from API. Searching; sorting; Recursive algorithms. Event-driven programming: event-handling methods; event propagation; exception handling. Introduction to Strings and string processing. Simple I/O; control structures; Arrays. Simple recursive algorithms; inheritance; polymorphism. Lab work: Programming assignments; design and implementation of simple algorithms, e.g., average, standard deviation, searching and sorting. Developing and tracing simple recursive algorithms. Inheritance and polymorphism

CYB201: Introduction to Cybersecurity and Strategy (2 Units)

Basic concepts: cyber, security, confidentiality, integrity, availability, authentication, access control, non-repudiation and fault-tolerant methodologies for implementing security. Security policies, best current practices, testing security, and incident response. Risk management, disaster recovery and access control. Basic cryptography and software application vulnerabilities. Evolution of cyber-attacks. Operating system protection mechanisms, intrusion detection systems, basic formal models of security, cryptography, steganography, network and distributed system security, denial of service (and other) attack strategies, worms, viruses, transfer of funds/value across networks, electronic voting, secure applications. Cybersecurity policy and guidelines. Government regulation of information technology. Main actors of cyberspace and cyber operations. Impact of cybersecurity on civil and military institutions, privacy, business and government applications; examination of the dimensions of networks, protocols, operating systems, and associated applications. Methods and motives of cybersecurity incident perpetrators, and the countermeasures employed by organisations and agencies to prevent and detect those incidences. Ethical obligations of security professionals. Trends and development in cybersecurity. Software application vulnerabilities. Evolution of cybersecurity and national security strategies, requirements to the typologies of cyber-attacks that require policy tools and domestic response. Cybersecurity strategies evolving in the face of big risk. Role of standards and frameworks.

CYB203: Cybercrime, Law and Countermeasures (2 Units)

General introduction on cybercrime. Definition of cybercrime. Types and categories of cybercrime and threats to the national critical infrastructure. Investigation process and procedure for cybercrime. Strategies of cybercrime perpetrators. Possible ways of curbing/preventing them. Technical aspects of computer cybercrime investigations, threats, and types of attacks and defences used by terrorists and criminals. Successful use of online social networks for cybercrime investigation. Concepts, trends, and methods in computer and network forensics investigations. Skills and knowledge in digital evidence collection and evaluation. Policies, legal issues, international jurisdiction, and privacy issues. Introduction to cyber law and countermeasures. Studies in cyber law application at the international and national levels with examples from European, North American, South American and Asian Countries. The cyber law framework in Nigeria. Challenges and opportunities for cyber law and countermeasure enforcement in Nigeria.

CYB299: SIWES (3 Units)

Students are attached to private and public organisations for a period of three months during the second year session long break with a view to making them acquire practical experience and to the extent possible, develop skills in all areas of Cybersecurity. Students are supervised during the training period and shall be expected to keep records designed for the purpose of monitoring their performance. They are also expected to submit a report on the experience gained and defend their reports.

SEN 201: Introduction to Software Engineering//Software Engineering I (2 Units)

Software Engineering concepts and principles. Design, development and testing of software systems. Software processes: software lifecycle and process models. Process assessment models. Software process metrics. Life cycle of software system. Software requirements and specifications. Software design. Software architecture. Software metrics. Software quality and testing. Software architecture. Software validation. Software evolution: software maintenance; characteristics of maintainable software; re-engineering; legacy systems; software reuse. Software Engineering and its place as a computing discipline. Software project management: team management; project scheduling; software measurement and estimation techniques; risk analysis; software quality assurance; software configuration management. Software Engineering and law.

NOU-CYB-211: Computer and Information Security (2 Units)

Introduction to computer and Information Security. Data security. Threat. Control. Tools and Techniques. Risk Analysis. Vulnerability. Application Security. Information Security. Network Security. End point Security. Internet Security. Security Controls. OS Security. Firewalls. IDS. Security Policy. Physical Security

NOU-CYB-213: Information Security Models (2 Units)

Basic concepts, Access control list (ACL), Bell-La Padula model, Biba model, Brewer and Nash model, Capability-based security, Clark-Wilson model, Context-based access control (CBAC), Graham-Denning model, Harrison-Ruzzo-Ullman (HRU), Lattice-based access control (LBAC), Mandatory access control (MAC), Multi-level security (MLS), Non-interference (security), Object-capability model, Role-based access control (RBAC), Take-grant protection model, Protection ring, High-water mark (computer security)

COS 202: Computer Programming II (3 Units)

Review and coverage of advanced object-oriented programming - polymorphism, abstract classes and interfaces. Class hierarchies and programme organisation using packages/namespaces. Use of API – use of iterators/enumerators. List. Stack. Queue from API. Searching. Sorting. Recursive algorithms. Event-driven programming: event-handling methods; event propagation; exception handling. Applications in Graphical User Interface (GUI) programming. Lab work: Programming assignments leading to extensive practice in problem-solving and programme development with emphasis on object-orientation. Solving basic problems using static and dynamic data structures. Solving various searching and sorting algorithms using iterative and recursive approaches. GUI programming.

INS204: Systems Analysis and Design (3 Units)

Structured approach to analysis and design of information systems for businesses. Software development life cycle. Structured top-down and bottom-up design. Dataflow diagramming. Entity relationship modelling. Computer aided software engineering. Input and output, prototyping design and validation. File and database design. Design of user interfaces. Comparison of structured and object-oriented design. Lab work: Practical exercises on software development life cycle (SDLC) activities with different case studies. Use of different information systems case studies to apply the knowledge of structured top-down and bottom –up design, dataflow diagram and entity relationship models.

NOU-CYB-222: Introduction to Networking (3 Units)

Introduction to Computer Networking. Overview of computer networking. The role of networking in modern computing. Basic network components. Types of Computer Networks. Local area networks (LANs). Wide area networks (WANs). The Internet. Networking Protocols. TCP/IP protocol suite. Internet Protocol (IP). Transmission Control Protocol (TCP). User Datagram Protocol (UDP). HTTP, FTP, and SMTP protocols. Network Devices. Routers, switches, and hubs. Network interface cards (NICs). Wireless access points. Firewalls. Network Security. Basic security concepts

NOU-CYB-224: Python for Cyber security (2 Units)

Introduction to code programming. Python installation. PyCharm IDE installation. Creating Project & Python Environment configuration. Basic Syntax, String Formation & code Execution. For Loops, over Lists. While Loops. Break & Continue Uses. Strings Manipulation. Combining Loops & Conditions. Variables with Different Data Types. User's Input. Operators, Comparative & Arithmetic. Type Casting. Condition's, logic and syntax. Dictionary, Tuple & lists. Nested Lists. File Permissions - Create, Append, read & Write. OS System Module Functions. Platform Module Functions. Log File Parsing. Web Communication library. Requests GET functions. Requests Sessions. Requests with Parameters. Extracting Data from Web. Introduction to SOCKET library. Creating Client Socket. Creating Server Socket. Sanding & Receiving Data. Set Echo Communication, Client Vs Server. Retrieving Data using OS Module.

NOU-CYB-226: Introduction to Cryptography (2 Units)

Fundamental understanding to cryptography, Roles of cryptography in computer and network security, Number Theory (Euler Theorem, Fermat Theorem, Euclid Algorithm, Chinese

Remainder Theorem and Discrete Logarithm), GCD, Modular Mathematics, Classical Cryptography, Modern Block Ciphers, Substitution Technique and Transposition Techniques. Block Ciphers, Data Encryption Standards, AES, Mode of operations, Stream ciphers, Concept of stream cipher, Advantage and disadvantages of this method in securing information, The one time pad and pseudo random key streams properties and generation, Asymmetric Cryptography, Diffie Hellman key exchange, One-Way Functions and trapdoors, RSA, El Gamal cryptosystem

Key Management, Discussion of the importance of good key management and some relevant standards, Public Key Infrastructure, certificates, certification authority, Digital signature & Message Integrity, Method of digital signature, Hash function, Digital Signature Systems, Authentication and Identification, Protocols, challenge and response, The Application of Cryptography in modern world, Discuss some issues relating to modern applications, Faster technology, Cryptography Act

NOU-CYB-214: VoIP and Multimedia Security (2 Units)

Introduction to multimedia traffic security. General knowledge and techniques for streaming data traffic, such as VoIP and multimedia. The security challenges unique to such traffic will be covered in detail, including disruption of service, theft of service, and violation of confidentiality. Relevant data encryption and authentication techniques will also be covered in detail.

CYB301 Cryptography Techniques, Algorithms and Applications (2 Units)

Introduction to cryptography, symmetric and asymmetric cryptography, key management, and encryption algorithms. Introduction to simple cryptosystems. Cryptanalysis. Stream ciphers, Block ciphers and Feistel ciphers. Multiple encryption. Hash functions. Data integrity, authentication, and perfect secrecy. Public-key cryptography and discrete algorithms-ELGamal cryptography. Algorithms for the discrete logarithm problem. Algorithmic number theory. Probabilistic primality testing. Security of ELGamal and RSA Encryption, and RSA Key Generation. Discrete logarithm cryptographic schemes. Conventional and public-key cryptography. Selected cryptosystems, including Data Encryption Standard (DES) and RivestShamir-Adleman (RSA) algorithm. AES encryption algorithm, a symmetric 128-bit block data encryption technique. PKI, SSL, and VPN. Digital signatures, pseudo-random number generation, cryptographic protocols and cryptanalytic techniques. Use of protocols, hashing and certificates and certificate authorities. Policies, procedures, and methods for the proper use of cryptography in secure systems. Applications of cryptography to signal. Lab work: Practical exercise on writing cryptography algorithms. Work on cryptographic techniques. Practice cryptanalysis of cipher and how to use protocols. Understand hash functions and learn how to hash, produce secured digital signatures and certificates. Learn the procedures and methods for the proper use of cryptography in secure systems. Practice primality testing. Practical assignments on ELGamal, DES and RSA encryption security, generation of RSA key and discrete logarithm cryptographic schemes

CYB303: Cybersecurity Risks Analysis, Challenges and Mitigation (2 Units)

Principles of applied information security management. Cybersecurity challenges. Cybersecurity risks, challenges and the path forward. Recognising risks. Overview of decision and risk analysis techniques. Mitigating risks and vulnerabilities. Effective use of assessments for cybersecurity risk mitigation. Mitigating cybersecurity risk with the cloud. Proactive measures mitigate critical cybersecurity challenges. Critical corporate and military cybersecurity risks. Evolving challenges in cyber risk management. The social implication of information technology to national development, cyber-attacks, control, distribution and safety of information. Economic and geopolitical factors that have made African countries vulnerable to cyber-attacks and the steps that can be taken to address this. Governance and security policy. Threat and vulnerability management. Incident management, risk assessment and risk management frameworks. Information leakage, crisis management and business continuity. Legal and compliance, security awareness and security implementation considerations. ISO 27000 series and the Plan-Do-Check-Act model. Assessment of threats and vulnerabilities. Incident response, forensics and investigations. Dealing with classified/sensitive data. Legal and regulatory drivers and issues. Certification. Common criteria, security education and training. Practical considerations when implementing the frameworks to address current and future threats. Lab work: Practical approach to cyber hygiene. Practice cybersecurity risk mitigation in the cloud and how to use proactive measures to mitigate the learned challenges. Work on applying the decision and risk analysis techniques. Master how to mitigate risks and vulnerabilities

CYB305: Digital Forensics and Investigation Methods (2 Units)

Introduction to digital forensics, digital evidence, and increasing awareness of digital evidence. Challenging aspects of digital evidence. Best practices in securing, processing, acquiring, examining and reporting on digital evidence. Cyber trail and challenging aspects of the cyber trail. Brief history of computer crime and cybercrime investigation. Cyber auditing. Evolution of investigative tools. Language of computer crime investigation. The role of computers in crime, technology and law, jurisdiction, pornography and obscenity, child pornography, privacy, copyrights and the “theft” of digital intellectual property. The investigative process and investigative reconstruction, with digital evidence. Examine techniques and tools used by computer forensics investigations such as acquisition, preservation, recovery, and analysis of evidence obtained from portable and stationary computer storage devices, personal digital assistants (PDAs), and cell phones. Current technologies and methods as well as leading edge techniques with practical based exercises/projects and research opportunities. Lab work: Practical exercises on how to make use of various techniques and tools for computer forensics investigations and cyber trail during cybercrime investigations. Practice cyber auditing skills. Work on applying the best practices in securing, processing, acquiring, examining and reporting on digital evidence with current technologies and methods in forensics investigation.

CYB399: SIWES II (3 Units)

Students are attached to private and public organisations for a period of three months during the third-year session-long break with a view to making them acquire additional practical experience in all areas of Cybersecurity over and above what is gained in CYB 299. Students are supervised during the training period and shall be expected to keep records designed for the purpose of monitoring their performance. They are also expected to submit a report on the experience gained and defend their reports.

NOU-CYB-323: IOT Security and Privacy (3 Units)

Introduction to IoT. IoT Vulnerabilities, Attacks, and Countermeasures. Heterogeneous Intelligent Transportation System. Security Engineering for IoT Development. The IoT Security Lifecycle. Smart Attendance Monitoring IoT-Based Device Using Cloud Services. Cyber Attack Analysis and Attack Patterns in IoT-Enabled Technologies. A Review of Cyber Attack Analysis and Security Aspect of IoT-Enabled Technologies. Encryption of Data in Cloud-Based Industrial IoT Devices. Cryptographic Fundamentals for IoT Security. Cryptographic security APIs. Identity and Access Management Solutions for the IoT. Authorization and access control in IoT. Mitigating IoT Privacy Concerns. Mitigating IoT Privacy Concerns. Physical Layer Security Approach to IoT. Setting Up a Compliance Monitoring Program for the IoT. Cloud Security for the IoT.

CSC 309 Artificial Intelligence (3 Units)

Overview of Artificial Intelligence. History of AI. Goals of AI. AI Technique. Types of AI. Branches and applications of AI. Advantages and Disadvantages. Introduction to Intelligent Agents. Agent Performance, Examples of Agents, Agent Faculties, Rationality, Agent Environment. Agent Architectures. Search. General Classes of AI Search Algorithm Problems. Problem Solving by Search. Types of AI Search Techniques and Strategies. Introduction to the types of problems and techniques in AI. Problem-Solving methods. Major structures used in AI programmes. Knowledge Representation. KR and Reasoning Challenges. KR Languages. Knowledge representation techniques such as predicate logic, non-monotonic logic, and probabilistic reasoning. Semantic Network - types of relationships, semantic network inheritance, types and components. Introduction to Frames. Natural Language Processing (NLP). Introduction to natural language understanding and various syntactic and semantic structures. Introduction to Expert Systems - characteristics, components, types, requirements, technology, development. Programming Languages for AI. Introduction to computer image recognition. Lab work: Group practical in (i) Turing test practical - Students can act out their own version of the Turing test (iii) Facial recognition practical to aid in teaching students how machine learning works with students simulating a facial recognition algorithm. Practical applications of NLP in groups – (i) Question Answering focuses on building systems that automatically answer the questions asked by humans in a natural language (ii) Spam detection application for detecting unwanted e-mails getting to a user's inbox (iii) Sentiment analysis/opinion mining should be used on the web to analyse the attitude, behaviour, and emotional state of the sender, implemented through a combination of NLP and statistics (iv) Practical exercise of machine translation used to translate text or speech from one natural language to another natural language such as the Google Translator (v) Developing a model to provide word processor software for the spelling correction (vi) Developing a model for speech recognition for converting spoken words into text (vii) Implementing a Chatbot to provide the staff/student's chat services. OR Group Practical exercise on agents and its environment using simulation of a colony of ants foraging for food; model simulating a message between agents; model simulating the flocking behaviour of birds; model to apply standard search algorithm to the classic search problem of missionaries and cannibals, and how to use communicating agents for searching networks. Some computer AI animation exercises for any branch of AI. Practical exercise on simple robots coupling and programming. Group project of building a lawn robot for trimming grasses, or any simple design and implementation of robotics.

NOU-CYB-321: Network Security (2 Units)

Modern Network Security, Threats, Securing Network Devices, Authentication, Authorization, Accounting (AAA) and Implementing Firewall Technologies. Implementing Intrusion Prevention, Securing the Local Area Network, Network protocols, Cryptography protocols. Implementing Virtual Private Networks, Implementing Virtual Private Networks, Implementing Site-to-Site IPSec, VPN, implementing a Remote Access VPN, Implementing a Remote Access VPN and Zone-Based Policy Firewall. Managing a Secure Network. Types of Firewall. This course is aligned with CCNA Network Security.

NOU-CYB-317: Cyber Privacy and Data Protection (2 Units)

Privacy: Legal Issues, Landscape & Chronology, Developing A Privacy Program, Privacy Governance, Privacy Program Frameworks, Legal Jurisdiction and Global Data Flows, Data Assessments, Documentation, Privacy Rights, HIPAA Framework, Security & Breach Notification, Training and Awareness, Information Security and Protection of Data, Managing a Security Breach, Continual Improvement, The US Federal Government Branch and Information Privacy, US Healthcare Privacy Related Laws and Privacy Compliance, Global Data Protection and Information Privacy Laws

NOU-CYB-319: Information Security Engineering (2 Units)

System and management view of information security, Requirements for information security, Systems-design process and life-cycle security management of information systems. Basic policies on information security and methodologies. Information-security risk management, security policies, security in the systems-engineering process, Laws related to information security and management of operational systems

ENT 312: Venture Creation (2 Units)

Opportunity Identification (Sources of business opportunities in Nigeria, Environmental scanning, Demand and supply gap/unmet needs/market gaps/market research, Unutilised resources, Social and climate conditions, and technology adoption gap). New business development (business planning, market research). Entrepreneurial finance (venture capital, equity finance, microfinance, personal savings, small business investment organisations, and business plan competition). Entrepreneurial marketing and e-commerce (Principles of marketing, customer acquisition & retention, B2B, C2C and B2C models of e-commerce, first mover advantage, e-commerce business models and successful e-commerce companies,). Small business management/family business: Leadership & Management, basic bookkeeping, nature of family business and family business growth model. Negotiation and business communication (Strategy and tactics of negotiation/bargaining, traditional and modern business communication methods). Opportunity discovery demonstrations (business idea generation presentations, business idea contest, brainstorming sessions, idea pitching). Technological solutions (the concept of market/customer solution, customer solution, and emerging technologies, business applications of new technologies- Artificial Intelligence (AI), Virtual/Mixed Reality (VR), Internet of Things (IoT), Blockchain, Cloud Computing, renewable energy, etc. digital business and e-commerce strategies).

CYB302: Biometrics Security (2 Units)

Contents Introduction to biometrics and digital image processing. Matlab in biometric image/signal processing. Biometric algorithms and systems with emphasis on face, fingerprint, eyes (iris), speech (voice). Automated biometric identification multimodal biometrics. Biometric data: raw data, template data, and data methods. Biometric matching basics: biometric authentication, enrolment, correct user, and incorrect user. Match threshold and matching performance. Setting a threshold. Biometric authentication: matching data, ground truth, calculating errors rates and graphs. Biometric data: Storage of biometric data elements, transactions, errors and quality upgrades. Data security and integrity. Privacy issues and other aspects of biometrics. Applications of biometrics and future trends. Challenging issues: security strength and recognition rates. Alternatives of passwords and smart cards. Lab work: Practical exercise on biometric capture, image processing, matching threshold and performance. Learn the practical aspect of automated biometric identification of multimodal, authentication and calculation of error rates. Work on biometric algorithms, privacy and security of stored biometric data.

CYB304: Information and Big Data Security (2 Units)

Introduction to big data. Small data vs. big data. What is big data? The evolution of data/big data. Big data characteristics-3Vs/6Vs. Unique features of big data. Importance of big data? Why does big data matter? Sources of big data. Formats of data. Applications of big data. Use case-issues and solutions. Big data technology. Big data as an opportunity. Example of big data. Big data statistics. Business intelligence vs. big data vs. data mining. Big data handling and techniques. Using the cloud for big data. Big data challenges/problems. How businesses are utilising big data. Big data technologies. Operational and analytical big data. Big data skills. Big data adoption. Big data analysis in practice. Case study session, preparation of case study report and presentation. The big data platform and key aspects. Governance for big data. Big data components. Big data driven organisational change and essential analytical tools and techniques. Develop big data solutions. System and management view of information and big data security. Requirements for information and big data security. Systems-design process and lifecycle security management of information systems. Basic policies on information security and methodologies. Information-security risk management, security policies, security in the systems-engineering process. Laws related to information security and management of operational systems. Apply machine learning techniques and other big data programming languages. Analyse big data recommendations. Cloud-based big data analysis. Lab work: Practice on data acquisition and how to initiate discovery on raw data using discovery systems. Learn Big Data analytics skills. Practical procedure for the crafting of an enterprise-scale cost-efficient Big Data and machine learning solution to uncover insights and value from data. Use the practical exercises to bridge the gap between the theoretical world of technology with the practical ground reality of building corporate Big Data and data science platforms. Hands-on exposure to Hadoop and Spark (or any of the BD tools), build machine learning dashboards using R and R Shiny, create web-based apps using NoSQL databases. Practical assignment of information and BD security.

CYB322: Cybersecurity Innovation and Entrepreneurship (2 Units)

Fundamental concepts of innovation, and business ideas in general. Product development. Business leadership. Digital marketing. Entrepreneurial opportunities in Cybersecurity. Legal issues and business ethics. New venture creation process. Business feasibility planning. Market research. Business strategy. Business models and business plans. Technical presentations. Report on a successful entrepreneurial outfit

NOU-CYB-308: Web Application Security (3 Units)

Definitions of Web Application. Important of web applications the business world. Overview of web application security. Importance of web application security. Threats and risks associated with web applications. Understanding of common security terminology and concepts. Overview of web application architecture. Different types of web applications and their security implications. Understanding the role of servers, and databases in web application security. Security considerations for web application design and deployment. Common web application vulnerabilities (e.g., injection attacks, cross-site scripting etc). Security testing techniques and tools. Best practices for secure coding and development. Web application firewalls and other protective measures. Incident response and handling security breaches. Legal and ethical considerations in web application security

NOU-CYB-310: Information Security Audit (2 Units)

Information Security Overview. Audit Planning and Preparation. Audit Techniques and Collecting Evidence. Information Security Standards ISO. Asset Management. Security Risk Assessment. Security Governance: Tier four Risk Management, Tier four Performance management. Framing Information security Governance. Information System and IT Governance Evolution. Information Security Governance (ISG) Planning Process. ISG Audit Testing and Evaluation of Controls. ISG Audit Controls reporting. Cyber Security Audit Planning Process. IT Governance and Information Security: Guides and Standards. IT Governance in Organizations:

A Maturity Framework Based on COBIT 5. IT Service Management as a Key Pillar for IT Governance: A Maturity Framework Based on ITILv4. Cloud Computing as a Key Pillar for Agile IT Governance. Information Security Governance: Best Practices in Organizations. Information Security Governance: A Maturity Framework Based on ISO/IEC 27001. Information Security Policy: A Maturity Framework Based on ISO/IEC 27001.

NOU-CYB-312: Critical National Information Infrastructure Protection (2 Units)

Fundamentals of CNI: classification of critical infrastructures, importance of CNI. CNI Access Control: prevention of unauthorized users and devices on CNI networks. CNI Application Security: CNI applications encryptions, Security measures on hardware and software to lock down potential vulnerabilities. CNI Firewalls: Gatekeeping devices. Network vulnerabilities in CNI systems: telecommunication networks, Smart Grid network, aviation, oil and gas operational streams (upstream, midstream and downstream), environment and climate change system networks. Types and countermeasure of attacks on CNI network components: Information Technology (IT) Operational Technology (OT), Advanced Metering Infrastructure (AMI), Home Area Networks (HANs) Supervisory Control and Data Acquisition (SCADA) components etc. CNI vulnerability testing: implementing remote monitoring and access control, tools and phases of vulnerability testing

NOU-CYB-314: Application of Data Mining in Cyber Security (2 Units)

Concepts of data mining, Knowledge discovery process, An overview of the Knowledge Discovery Process, Mining on different kinds of data, Mining for different kind of knowledge, Applications of data mining, Descriptive data summarization, Data cleaning methods, Data integration and transformation methods, Basic data reduction methods, Discretization and concept hierarchy generation, Concept and architecture of data warehouse, The dimensional data model, OLAP Operations, Basic concepts of classification, Evaluation of classification, Bayesian classification, Decision tree and decision rule induction, Linear models for classification, Basic concepts of nonlinear classification, Classification by lazy evaluation, Emsemble classifier, Cluster and Outlier Analysis, Text Mining and Web Mining, Social impact of data mining, Data mining and privacy, Standardization efforts, Data mining system products

NOU-CYB-316: Cyberpreneurship (2 Units)

Cybersecurity portfolio, Continued learning, Foundational Knowledge, Technical Skills, Soft Skills, Challenges, Certification, Proficiency in each area of Cybersecurity framework, The Panama Papers, a real cyber attack, Cyber threats and the methods that hackers use, Consequences of cyber attacks for small and medium enterprises, Tools and preventative strategies that you can put in place to protect your organization

NOU-CYB-326: Project Management in Cybersecurity (3 Units)

Fundamentals of project and project management; Importance of project management in cybersecurity; Project management methodologies in cybersecurity; Risk management in cybersecurity projects; Evaluation of strengths and weaknesses of cybersecurity projects; Features of project lifecycles, Cybersecurity considerations in project lifecycle: (Risk assessment, Security by design, Digital trust and Compliance); Role of Service Level Agreements in cybersecurity projects: (Stakeholders, Agreement overview, Service performance, Exclusion and Penalties); Concept of risk in cybersecurity projects; Methodologies for cybersecurity project risk management: (Risk assessment, SWOT analysis, Reverse analysis and PESTLE); Potential risks within various cybersecurity projects; Principles of risk mitigation in cybersecurity projects; Risk management strategies across cybersecurity project phases (applications in real-world scenarios); Role of project management tools; Significance of project management tools in cybersecurity; Features linking project management tools with cybersecurity projects: (Compliance, Reporting, Team collaboration, Bug tracking); Explain common international standards for project management in cybersecurity: (PMI, PRINCE2, ISMS); Significance of the application of International Standards in managing Cybersecurity projects. N/B: This course should have case studies and hands on practice for relevant topics.

COS 409: Research Methodology and Technical Report Writing (3 Units)

Foundations of Research. Types of Research. Research Approaches. Significance of Research. Research Methods versus Methodology. Research Process. Criteria and Strategy for Good Research. Problems Encountered by Researchers in Nigeria. Principles of Scientific Research. Scientific investigation. Problem formulation. Definition and technique of the Research Problem. Selection of Appropriate Method for Data Collection- Primary Data and Secondary Data. Guidelines for Constructing Questionnaire/Schedule. Guidelines for Successful Interviewing. Difference between Survey and Experiment. Eloping Research Proposal and Research Plan. Formulation of working hypothesis and Testing. Literature review. Procedure for reviewing related relevant studies and referencing cited works. Types of Reports. Technical Report Writing. Layout and mechanics of writing a Research Report. Standard Techniques for Research Documentation. Sampling Design. Different Types of Sample Designs. Steps in Sampling Design. Criteria of Selecting a Sampling Procedure. Methods of analysis. Processing and Analysis of Data Elements/Types of Analysis. Interpretation and Presentation of results. How to prepare References and Bibliography.

CYB401: Systems Vulnerability Assessment and Testing (2 Units)

Definition of systems vulnerability. Methods and the testing methods using different techniques. Mitigation of risks and how to enhance the security of a company's infrastructure. Penetration testing methodologies, test planning and scheduling. Information gathering. Password cracking. Penetration testing and security analysis. Social engineering, Internal and external penetration testing. Router penetration testing, security analysis, reporting and documentation. Operating systems fingerprinting. Remote network mapping. Software and operational vulnerabilities. Attack surface analysis. Fuzz testing. Patch management. Security auditing. Lab work: Practical exercise on systems vulnerability, assessment methods and the testing methods using techniques to effectively identify and mitigate risks to the security of a company's infrastructure. Perform penetration testing using various methodologies, along with the test planning and scheduling. Work on password cracking and social engineering penetration testing and security analysis. Identify software and operational vulnerabilities in a given environment and how to overcome these vulnerabilities. Execute attack surface analysis, fuzz testing, patch management, and perform security auditing.

CYB403: Cyber Threat Intelligence and Cyber Conflict (2 Units)

Techniques for detecting, responding to and defeating organised cybercrimes and cyberwar activities. Analysing successful and unsuccessful advanced persistent threats and malware campaigns. Analyse divergent national and international policies for combating cyber terrorism and terrorist tactics worldwide. Understanding Cyber threat intelligence - defining threats, Understanding risk, Cyber threat intelligence and its rule, Expectations of organisations and analysts, and indicators of compromise. Tactical threat intelligence. Role of a tactical threat intelligence analyst, expected skills and tradecraft. The Kill Chain and Intrusion Analysis. Indicator lifecycle. Introduction to operational threat intelligence - Role of an operational threat intelligence analyst, Need for information sharing and peers. Models and methods for managing intelligence, campaigns and threat actors. Introduction to strategic threat Intelligence - role of a strategic threat intelligence analyst. Threat modelling, Organisational change and security posturing. Event recording and incident sharing. Evolution of counterterrorism and cyber conflict.

CYB405: Ethical Hacking and Reverse Engineering (2 Units)

Introduction to ethical hacking, attacks, threats, hackers, measures and countermeasures. Overview of ethical hacker strategies. Focus on how perimeter defences work, how intruders escalate privileges and methods of security systems. Intrusion detection, policy creation, social engineering. Techniques and technologies for understanding the operation of malicious software and attacks. Threats and defence mechanisms. Attack phases. Secure network infrastructure. DDoS attacks, buffer overflows and virus creation. Network Infrastructure Attacks, Hacking Methodology, Developing ethical hacking plans. Footprinting and reconnaissance. Scanning Networks. Enumeration and system hacking. Malware threats. Sniffing. Social engineering. Physical security. Password vulnerabilities - cracking passwords. Denial of Service. Session hijacking. Hacking web servers. Hacking web applications. sql injection, hacking wireless networks. Hacking mobile platforms. Evading IDS, Firewalls, and Honeypots. Explores techniques and technologies for understanding the operation of malicious software and attacks. Techniques for detection, identification and prevention. Reverse engineering of code and network exploits as a method for understanding and development of countermeasures. Lab work: Practice the ethical hacker strategies and methods. Work on a sample perimeter defences and identify how intruders escalate privileges and methods of security systems. Practical exercises on the techniques and technologies of malicious software and attacks. Learn how to perform system hacking, mobile platform hacking, crack password, remove introduced vulnerabilities and evade IDs, firewalls, and honeypots. Apply reverse engineering of code and network exploits as a method for understanding and development of countermeasures. Utilise foot printing and reconnaissance, and scanning networks.

CYB499: Final Year Project I (3 Units)

An independent or group investigation of appropriate cybersecurity related problems carried out under the supervision of a lecturer. The student must submit a written proposal to the supervisor to review. The proposal should give a brief outline of the project with the statement of problem, aim, objectives, scope, significance, research gap, proposed research methodology, estimated schedule of completion, and resources needed. A formal written report is essential and an oral presentation may also be required. Topics from emerging trends such as applications in artificial intelligence, steganography, quantum computing, big data, cloud security, ethical hacking, cyber hunting, internet security, penetration testing, network intrusion and prevention, threat management, cybersecurity risk mitigation in the cloud, biometrics, digital image processing, Blockchain, quantum computing, edge computing, Internet of Things, 5G security, etc.

NOU-CYB-415: Disaster and incidence Risk Management (2 Units)

Fundamental Risk Concepts and terminology, Regulatory Requirements & Best Practices, Links between Risk, Incident & safety Culture in the work place, Key Risk Management Implementation issues, Practical Risk Assessment demonstration, Risk Control Options, Risk Prioritization and decision making, Risk Assessment strategies, Incident Investigation basics and terminology, Process of incident investigations, Interviewing and facts gathering techniques, Root Cause Analysis, Practical Incident Investigation Execution, Case Study on Incident Investigation, Incident Investigation Report writing & presentation, Practical integration of Risk Management and Incident

NOU-CYB-421: Digital Forensic Analysis (2 Units)

Capturing & Analyzing Data Packets. Going Wireless. Tracking an Intruder on the Network. Network Forensic tools: Visual Tracing tools, Traceroute tools, Monitoring Tools, Analysis Tools and Proprietary tools. Connecting the Dots – Event Logs, Proxies, Firewalls, and Routers. Smuggling Forbidden Protocols – Network Tunneling. Network Forensic Techniques: IP Trace back Technique, intrusion detection System, firewalls. Advanced network forensic Techniques: vulnerability Detection Techniques, Honeypots and Honeynets. Highly Efficient Techniques for Network Forensics: Bloom filter, Rabin Fingerprinting, Winnowing, Attribution System etc. Android Device Design & Security Overview. Extracting Data from Android Devices. Recovering & Analyzing Android Data. Android App Analysis, Malware & Reverse Engineering. Windows Phone Forensics. Parsing Third-Party Application Files. Virus & Malware Detection. Botnet Forensics Analysis

NOU-CYB-425: Current Trends in Cybersecurity (Seminar) (3 Units)

Students are expected to write a seminar paper on any new and recent technologies/topics for mitigating against attacks in the industry/society

NOU-CYB-489: Cyber Warfare and Defense (2 Units)

Definitions of cyber warfare and defense. The basic building blocks of cyber warfare. The difference between information warfare and cyberwarfare. Cyber warfare and the elements that makes it attractive. Understanding the threats in cyberspace. The Internet architecture. Three major information infrastructures. The challenges of situational awareness. Cyber vulnerabilities and how cyber-attacks are enabled. Common categories and methods of cyber-attack. Classes of cyber-attack. Software which enables exploitation of vulnerabilities. Digital evidence. Cyber weapons. Ambiguities and problems of cyberwar. Cyber deterrence. Tools for physical attack and defense

CYB402: Steganography-Access Methods and Data Hiding (2 Units)

History of secret writing. An overview of steganography. Introduction to steganography - Definition of steganography. Why is steganography important? Steganography vs. Encryption. Uses of steganography. Problem of steganography. Steganography applications and methods. Steganography types and methods - text steganography, images steganography, video and audio steganography. Steganography techniques. Survey of different steganography techniques for encrypting the data. Information hiding: steganography and steganalysis. Data hiding methods, techniques and access methods. Requirements for data hiding. Steganography and Business - the basics of embedding, different aspects in informationhiding systems. Steganographic algorithm. Security of a steganographic algorithm. Steganography detection, finding images, and verifying hidden content. Research and practical experimentation of data hiding tools. Research on investigation techniques and the latest countermeasures. Lab work: Practice secret writing using different methods and tools. Learn how to use steganography methods and techniques for encrypting the data. Master data hiding methods, techniques and access methods using case study exercises. Write samples steganography algorithm and secure the algorithm. Detect elements of steganography, finding images, and verifying hidden content in a given text, image, audio and video samples.

CYB404: Cloud Computing Security (2 Units)

Introduction to cloud computing, cloud computing vendors, cloud computing threats, cloud reference model. Cloud-enabling technologies. Services, Service-Oriented Architectures. Cloud service models. Cloud deployment models. Introduction to data centres: servers, data storage, networking and virtualisation. Data centre networking. Introduction to server virtualisation software: VMware VSphere. Virtual machine management: configuration, placement and resource allocation. Power efficiency in virtual data centres. Fault tolerance in virtual data centres. The cloud cube model and security for cloud computing. Security in the cloud. Cloud threats, threat mitigation and security risks. Real world issues with cloud computing. Cloud security alliance. National Institute of Standards and Technology, Information Assurance Framework. Cloud audit. Cloud management audit/assurance programme, Cloud business continuity planning. Building a cloud. Architectural best practices: Designing for the cloud. Economics of the cloud. Cloud strategy. Cloud standards and the future. Security of the cloud.

CYB406: Deep and Dark Web Security (2 Units)

Dark web, deep web, clear net. Tor Onion, Silk Road. How to get on the dark web. Users of dark and deep web. Invisible Web Search Engines. Privacy and anonymity as core values of the darknet. Decentralisation on the dark web. Accessing the Deep web and the Dark web through the TOR browser. Web security. Cryptocurrencies. Overview on Dark Web and Deep Web. The Hidden side/area of the web. Deep/Dark Web Anonymity, TOR, Hidden services, TAILS, Web Security, Cryptocurrencies. Crypto Trading and Cryptomining. Cryptocurrencies, Anonymity & Security. How to install a VPN, and adequate browsers like Chrome, Opera, or Firefox with tracking technologies. How Does the Dark Web Work? Reasons for Accessing the Dark Web. Security issues of Dark and Deep web. How to use the Tor over VPN method - Session logs storage. Encryption of traffic. Protection against malicious Tor exit nodes. How to use Tor over VPN - bypass blocked Tor nodes, ISP visibility in accessing onion content, susceptible to end-to-end timing attacks. Tor alternatives such as I2P, Matrix.org, Orbot, Globus Secure Browser, Comodo Ice Dragon and FreeNet. Cons and Pros of Tor. Use of virtual machine software. Navigating the Dark Web. The Hidden Wiki as Wikipedia's evil twin. Search engines such as DuckDuckGo, Torch, the triple-W Virtual Library, Uncensored Hidden Wiki, and ParaZite. Commercial services. Email clients. Darknet version of social media and instant messaging - Zuckerberg's Facebook, BlackBook, Torbook, Campfire, MadIRC Chat Server. Safety on the dark web. Inside the dark and deep web. The Best Sites and Services on the Dark Web. Deep web radio. Benefits of Deep and Dark web. Cyber Threats and Dangers on the Deep/DarkWeb. How to fight hackers underground. Dark web and Deep web monitoring. Lab work: Install your VPN. Practice how to access the Deep web and the Dark web with enhanced security. Investigate advanced and famous websites located on the Deep and Dark Web. Practically learn how to anonymously access the darknet and TOR hidden services (onion services), and how to enter the dark web while staying safe. Try to visit the best sites and buy an educational resource.

CYB498: Final Year Project II (3 Units)

This is a continuation of CYB 497. This includes the research methodology, analysis of data using statistical tools, performance evaluation, standard documentation of the project, referencing style, programming of the prototype/simulation model, plagiarism and grammarly check, and PowerPoint presentation skill. The formal written report made up of chapters four and five approved by the supervisor will be submitted to the Department for final grading. An oral presentation is required.

NOU-CYB-414: Network Threats and Risk Assessment (2 Units)

Introduction to the Theories of Risk Management, The Art of Managing Risks, Threat Assessment and Its Input to Risk Assessment, Threat Assessment Method, Operating System Vulnerabilities and Application Vulnerabilities. Public Domain and Commercial Off-the-Shelf Software, Connectivity and Dependence, Policies, Procedures, Plans, and Processes of Risk Management and Integrated Risk Management.

NOU-CYB-422: Mobile Network Security (2 Units)

Introduction to Mobile Security. Building Blocks – Basic security and cryptographic techniques. Security of GSM Networks. Security of UMTS Networks, LTE Security. WiFi and Bluetooth Security. SIM/UICC Security. Mobile Malware and App Security. Android Security Model. IOS Security Model. Security Model of the Windows Phone. SMS/MMS Security. Mobile Geolocation and Mobile Web Security. Security of Mobile VoIP Communications. Emerging Trends in Mobile Security. Network monitoring using Burp & proxy Configuration. SSL verification methods. Interception with SSL pinning. Certificate – Manual obtaining and generating. Bypass Trust Managers. Analysis methodologies-Static analysis Dynamic analysis, MODSF installation, Security review & Resources. Drozer Server, Sessions, Interacting with services.

NOU-CYB-424: Steganography and Steganalysis using AI (2 Units)

Introduction Methods for Hiding Information: students hiding in Text, Hiding in Disk Space, Hiding in Network Packets, Hiding in Software and Circuitry, Hiding in Audio and Images. Attacks against Hidden Information: Distortion and Removal, Countermeasures Against Attacks; XPLORING STEGANOGRAPHY: Digital Images, Hiding Information in Images, Hiding Data in the Noise, Watermarking Techniques, Issues in Information Hiding, Level of Visibility: Perceptible or Imperceptible, Robustness vs. Payload. Spatial or transform domain, File Format Dependence, Image Modeling, Examples of Digital Image Steganography Software: StegoDos, White Noise Storm, S-Tools, Comments on Other Software, Summary of Tools, Comments on Steganography: Steganalysis: Attacks Against Hidden Data: Detection: Seeing the Unseen.

Techniques for Detecting Hidden Information, Examples of Detecting Signatures in Stego-Images, S-Tools, Mandelsteg, Hide and Seek, Hide4PGP, EzStego, Stego On-line, lsteg-.lpeg, Distortion: Disabling Steganography and Watermarking, Techniques for Distorting Embedded Data, Examples of Distorting Embedded Information, Application of Steganalysis: Forensic Investigation; Comments on Steganalysis. Countermeasures to Attacks: Countermeasures to Distortion, Stronger Watermarks, Recognition Based on Image Characteristics, "Fingerprinting" Images, Affine Transformations and Invariants Using Fingerprints for Recognition, Recovering Watermarks from Distorted Images, Recovery using Image Fingerprints, Refinement using Normal Flow, Examples of Recovering Watermarks from Images, Comments on Countermeasures

NOU-CYB-426: E-Business Security (2 Units)

Introduction: Ecommerce on the Internet, Web Technology, Basic web security model, Web attacks (e.g., SQL injection, XSS, CSRF) and defenses, Session management and user authentication, Certificates and PKI, HTTPS: Design and pitfalls, Cryptography Basics, Privacy and Security, Using SSL/TLS and Proper Password Storage, Secure Development Methodologies (Coding Issues), Web Server Security, Database Security Principles, Securing Web Applications, Biometrics and Digital Identification, Digital Payments, Legacy payment systems, EMV(Europay, mastercard and visa) protocol, Attacks on EMV, Securing CNP transactions and PCI compliance, Cryptocurrency transaction (Tokenization), Policy issues including legal and ethical issues

NATIONAL OPEN UNIVERSITY OF NIGERIA

SENATE

Programme Title. B.Sc Cybersecurity

School/Institute/Centre: Faculty of Computing

Comments made by Senate by Dean of Faculty on Programme

Signature of Dean

Comments of Chairman of Senate

Signature of Chairman of Senate

Signature of Registrar - Secretary to Senate