DEPARTMENT OF CYBER SECURITY
FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY
SULE LAMIDO UNIVERSITY KAFIN HAUSA

LIST OF COURSES FOR 2025/2026 ACADEMIC SESSION

CCMAS

LEVEL 100

FIRST SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
GST 111	Communication in English	2	C	30	0
COS 101	Introduction to Computer Science	3	C	30	45
MTH 101	Elementary Mathematics I	2	C	30	0
STA 111	Descriptive Statistics	3	C	45	0
PHY 101	General Physics I	2	C	30	0
PHY 107	General Practical Physics I	1	C	0	45
SLU-COS 121	Introduction to Application Packages	2	C	15	45
	Total	**15 Units**			

SECOND SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
GST 112	Nigeria People and Culture	2	C	30	0
COS 102	Introduction to Problem Solving	2	C	15	45
MTH 102	Elementary Mathematics II	2	C	30	0
PHY 102	General Physics II	2	C	30	30
PHY 108	General Practical Physics II	1	C	0	45
SLU-CYB 132	Fundamentals of Cybersecurity	2	C	15	45
SLU-STA 112	Probability I	2	C	30	0
SLU-COS 104	Introduction to File Processing	2	C	15	45
	Total	**15 Units**			

Summary: Level 100 Student should register a total of **30 credit unit** for this session; **15 Core credit** from first semester and **15 Core credit** from second semester.

LEVEL 200

FIRST SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
ENT 211	Entrepreneurship and Innovation	2	C	30	0
CYB 201	Introduction to Cyber Security and Strategy*	2	C	30	0
CYB 203	Cyber Crime Law & Countermeasures	2	C	30	0
SEN 201	Introduction to Software Engineering	2	C	15	45
COS 201	Computer Programming I	3	C	30	45
SLU-CYB 205	Fundamentals of Cyber Security II	2	C	30	0
SLU-COS 203	Discrete Structure	2	C	30	0
	Total	**15 Units**			

SECOND SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
GST 212	Philosophy, Logic and Human Existence	2	C	30	0
INS 204	Systems Analysis and Design	3	C	30	45
COS 202	Computer Programming II	3	C	30	45
CYB 299	SIWES I	3	C	0	135
SLU-IFT214	Fundamentals of Networking	3	C	30	45
SLU-CYB 208	Information Security Policy	2	C	30	0
	Total	**16 Units**			

Summary: Level 200 Student should register a total of **31 credit unit** for this session; **15 Core credit** from first semester and **16 Core credit** from second semester.

LEVEL 300

FIRST SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
GST 312	Peace and Conflict Resolution	2	C	30	0
CYB 301	Cryptographic Techniques, Algorithms and Application	2	C	15	45
CYB 305	Digital Forensics and Investigative	2	C	30	0

	Methods				
CSC 309	Artificial Intelligence	2	C	15	45
SLU-CYB 325	Enterprise and Perimeter Security	2	C	30	0
SLU-IFT337	LAN, Switching and Internetworking	3	C	30	45
SLU-CYB324	Information Security Engineering	2	C	15	30
	Total	**16 Units**			

SECOND SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
ENT 312	Venture Creation	2	C	30	0
CYB 302	Biometrics Security	2	C	30	0
CYB 304	Information and Big Data Security	2	C	30	0
CYB 322	Cybersecurity Innovation and New Technologies	2	C	30	0
CYB 399	SIWES II	3	C	0	135
CYB 303	Cybersecurity Risk Analysis, Challenges & Mitigation	2	C	30	0
SLU-IFT336	Routing Protocol Concepts	3	C	30	45
	Total	**15 units**			

Summary: Level 300 Student should register a total of **31 credit unit** for this session; **16 Core credit** from first semester and **15 Core credit** from second semester.

LEVEL 400

FIRST SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
COS 409	Research Methodology and Technical Report Writing	2	C	30	0
CYB 403	Cyber Threats Intelligence and Cyber Conflicts	2	C	30	0
CYB 407	Cloud Computing Security	2	C	30	0
CYB 497	Final Year Project I	3	C	0	135
SLU-CYB 407	Information Security Risk Analysis and Management	2	C	15	45
SLU-COS 401	Algorithms and Complexity Analysis	2	C	15	45
SLU-CYB409	Information Security Models	2	C	15	45
	Total	**15 units**			

SECOND SEMESTER

Course Code	Course Title	Credit Units	Course Status	LH	PH
CYB 402	Steganography Access methods and Data Hiding	2	C	15	45
CYB 404	Ethical Hacking and Reverse Engineering	2	C	15	45
CYB 406	Deep and Dark Webs Security	2	C	15	45
CYB 498	Project	3	C	0	135
CYB 408	System Vulnerability Assessment and Testing	2	C	15	45
SLU-CYB402	Database Management and Control System	2	C	15	30
SLU-IFT404	Applied Networks and Security	3	C	30	45
	Total	**15 units**			

Summary: Level 400 Student should register a total of **30 credit unit** for this session; **15 Core credit** from first semester and **15 Core credit** from second semester.

BMAS

LEVEL 100

FIRST SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSC 131	Introduction to Computer Science	Core	3
MTH 121	Elementary Set Theory and Algebra	Core	2
MTH 113	Trigonometry	Core	1
STA 121	Descriptive Statistics	Core	2
PHY 131	Mechanics, Thermal Physics & Waves	Core	3
PHY 117	Basic Experimental Physics I	Core	1
BIO/CHM		Elective	2
GSP 121	Communication in English	Core	2
		Total	**16 Units**

SECOND SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 132	Fundamentals of Cyber Security I	Core	2
CSC 132	Introduction to Problem Solving	Core	3
MTH 132	Differential Calculus and Applications	Core	3
PHY 132	Electricity, Magnetism and Modern Physics	Core	3
PHY 118	Basic Experimental Physics II	Core	1
STA 122	Probability I	Core	2

GSP 122	Information & Communication Technology	Core	2
GSP 124	Use of Library and study skills	Core	2
		Total	**19 Units**

LEVEL 200

FIRST SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 221	Fundamentals of Cyber Security II	Core	2
CSS 225	Introduction to Digital Forensics	Core	2
SWE 231	Introduction to Software Engineering	Core	3
CSC 231	Computer Programming I	Core	3
CSC 239	Operating Systems I	Core	3
MTH 231	Mathematical Method I	Core	3
MTH 233	Linear Algebra I	Core	3
GSP 221	Introduction to Entrepreneurship	Core	2
GSP 223	Peace and Conflict Resolution	Core	2
GSP 121	Communication in English I	Core	2 (D.E ONLY)
		Total	**22 Units (D.E =24)**

SECOND SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 222	System and Network Administration	Core	2
CSS 224	Information Security Engineering	Core	2
IFT 232	Fundamentals of Networking	Core	3
CSC 232	Computer Programming II	Core	3
CSC 232	Information Security Policy	Core	3
CSC 236	Fundamentals of Data Structures	Core	3

CSC 238	Discrete Structures	Core	3
GSP 224	Communication in English II	Core	2
GSP 228	Nigerian People and Culture	Core	2
GSP 224	Use of Library and Study Skills	Core	2 (D.E ONLY)
		Total	**23 Units (D.E =25)**

LEVEL 300

FIRST SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 323	Biometrics Security	Core	2
CSS 327	Cryptographic Techniques	Core	2
CSS 325	Enterprise and Perimeter Security	Core	2
CSS 329	Information Security Engineering	Core	2
CSS 331	Systems Security	Core	2
CSC 330	Algorithms and Complexity Analysis	Core	3
CSC 333	Computer Architecture and Organization I	Core	3
CSC 335	Systems Analysis and Design	Core	3
GSP 321	Entrepreneurship Studies	Core	2
		Total	**21 Units**

SECOND SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 360	SIWES	Core	6
		Total	**6 Units**

LEVEL 400

FIRST SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 411	Cyber Law	Core	1
CSS 421	Software Defined Networks	Core	2
CSS 423	Forensic Analysis	Core	2
CSS 425	Cloud Computing Security	Core	2
CSS 427	Information Disaster Recovery	Core	2
CSS 429	Cyber Security in Business and Industry	Core	2
CSC 431	Artificial Intelligence	Core	3
CSC 411	Research Methods in Computing	Core	1
		Total	**16**

SECOND SEMESTER

Course Code	Course Title	Course Status	Credit Units
CSS 422	Database Management and Control System	Core	2
CSS 424	VoIP and Multimedia Security	Core	2
CSS 426	Fault Tolerant Computing	Core	2
CSS 432	System Vulnerability Assessment and Testing	Core	3
CSS 468	Project	Core	6
		Total	**15**

DESCRIPTION OF COURSE CONTENT

CCMAS

LEVEL 100 Courses

SLU-CYB 132: Fundamentals of Cybersecurity

Learning Outcomes: At the end of this course, students should be able to;
Explain the basic concepts of cyber security;
2. Explain the concept fault tolerant methodologies for implementing security;
3. Understand security policies and best current practices;
4. Test system security and incident response;
5. Have the introductory knowledge of risk management, access control cryptography as well as disaster recovery;
6. Identify software application vulnerabilities

Course content
Provides an overview of the introductory topics in cyber security. Topics include basic concepts 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, access control, basic cryptography and software application vulnerabilities.

LEVEL 200 Courses

CYB 201: Introduction to Cybersecurity and Strategy (2 Units C: LH 30)
Learning Outcomes
At the end of this course, students should be able to:
1. explain cybersecurity concepts, its methods, elements, and terminologies of cybersecurity, security, threat, attack, defence, and operations;
2. describe common cyber-attacks and threats, cybersecurity issues, challenges and proffered solutions, and build an enhanced view of main actors of cyberspace and cyber operations;
3. apply the techniques for identifying, detecting, and defending against cybersecurity threats, attacks and protecting information assets;
4. explain the impact of cybersecurity on civil and military institutions, privacy, business and government applications;
5. identify the methods and motives of cybersecurity incident perpetrators, and the countermeasures employed by organisations and agencies to prevent and detect those incidences and software application vulnerabilities; and
6. state the ethical obligations of security professionals, evaluate cybersecurity and national security strategies to the typologies of cyber-attacks that require policy tools and domestic response, and define the cybersecurity requirements and strategies evolving in the face of big risk.

Course Contents
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.

CYB 203: Cybercrime, Law and Countermeasures (2 Units C: LH 30)

Learning Outcomes

At the end of this course, students should be able to:

1. discuss cybercrimes, including computer crimes, internet fraud, e-commerce, and threats to the national infrastructure;
2. review the policies, legal issues, investigative techniques and strategies, implications for investigation and enforcement on a global scale;
3. analyse the cyber law of Nigeria and some other countries with the penalties attached to each of the cyber laws;
4. describe cyber law application at the international and national levels with examples from Africa, European, North American, South American and Asian countries;
5. compare the cyber law framework and countermeasures in Nigeria with other countries; and
6. state the challenges and opportunities for enforcement of cyber law in Nigeria.

Course Contents

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.

CYB 299: SIWES I (3 Units C: PH 135)

Learning Outcomes

At the end of this training, students should be able to:

1. assess their knowledge of cybersecurity, its application, preventive measures and defence of the cyber environment;
2. explain how a typical cybersecurity unit/department of an organisation operates;

3. describe the various assignments carried out and the skills acquired during the SIWES period; and
4. submit a comprehensive report on the knowledge acquired and the experience gained during the exercise.

Course Contents
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.

SLU-CYB 205: Fundamentals of Cyber Security II (2 Units C: LH 30)
Learning Objectives
Upon successful completion of the course, the students will have:
1. reasonable understanding of the fundamentals of the cyber security domain and related issues
2. practical knowledge of various tools, processes and methods to ensure security of systems through a minimum of two hands-on assignments involving attack and protection in a virtual environment
3. an understanding of the inter-disciplinary nature of cyber security domain
4. adequate level of cross-disciplinary knowledge of design, implementation, evaluation and testing of secure protocols, systems or applications
5. basic knowledge to be able to build bug-free systems, dependable during malice or error
6. foundational skills for developing expertise in one or more sub-domains of cyber-security
7. foundational skills and knowledge of impact of security on economics, legal, business, warfare and social domains
8. effective communication skills through an in-class project along with a presentation and project report

Course Content
Introduction, Psychology, Usability, Thinking like a Hacker, CIA Triad, Security Terminologies, Security Protocols, Security Policies and Management, Multilevel and multilateral Policies, Security Mechanisms, Security Design Principles, Threat Analysis and Risk Assessment, Securing a System, Cryptography, Basic Techniques, Digital Signatures, Cryptanalysis, Software Security, Low-level attacks, Code Review and Testing, Defenses, Fall-Break, Student Project Idea Discussion, Network Security, Vulnerabilities, Attacks, Defenses, Internet and Smartphone Security, Anonymous vs Secure Browsing, Information Economics, Economics of Security, Physical Protection, Biometrics, Banking Security, Cyber Forensics, Cyber Warfare, Surveillance and Privacy, Incident Response and Mitigation, Business Continuity, Legal issues and Ethics.

SLU-CYB 206: Information Security Engineering (2 Units: LH 20, P 30)
Learning outcomes:
At the end of this course, students should be able to;
1. understand System and management view of information security,
2. understand the Requirements for information security,
3. understand the Basic policies on information security and methodologies.
4. understand the Information-security risk management,

5. understand the Laws related to information security and management of operational systems.

Course content
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.

SLU-CYB 208: Information Security Policy (2 Units C: LH 30)
Learning outcomes:
1. explain the objectives of information security
2. explain the importance and application of each of confidentiality, integrity, authentication and availability
3. understand various cryptographic algorithms. Understand the basic categories of threats to computers and networks
4. describe public-key cryptosystem.
5. describe the enhancements made to IPv4 by IPSec
6. understand Intrusions and intrusion detection
7. discuss the fundamental ideas of public-key cryptography.
8. generate and distribute a PGP key pair and use the PGP package to send an encrypted e mail message.
9. discuss Web security and Firewalls

Course Content
Attacks on Computers and Computer Security, Cryptography: Concepts and Techniques, Symmetric key Ciphers, Message Authentication Algorithms and Hash Functions, Authentication Applications, E-Mail Security, IP Security. Web Security, Intruders, Virus and Firewalls:

BMAS

CSS 221: Fundamentals of Cyber Security II (2 Units: LH 20, P 30)

Operating system protection mechanisms, intrusion detection systems, 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, homeland cybersecurity policy, and government regulation of information technology

CSS 222: System and Network Administration (2 Units: LH 20, P 30)

This course focuses on the tasks and issues involved in the administration of distributed computing networks. Topics include user access and privileges, DHCP, DNS, remote access, file and print, update and patch management, security and network management service.

Authentication, Authorization, and Accounting systems are covered with emphasis on using cross-platform authentication. Network services including firewalls, DNS, mail, and web services, SANs, WAN administration, and network management tools. Topics will be covered from a practical, business-oriented, cost/benefit perspective and best practice implementation techniques. Hands-on experience will include representative technology from each of these areas.

CSS 225: Introduction to Digital Forensics (2 Units: LH 20, P 30)

This course will examine digital forensic as it relates to both civil and criminal investigations. The course content includes best practices in securing, processing, acquiring, examining and reporting on digital evidence. Students will be exposed to current technologies and methods as well as leading edge techniques with practical based projects and research opportunities.

LEVEL 300

CSS 323: Biometrics Security (2 Units: LH 20, P 30)

Introduction to Biometrics, Brief introduction of digital image processing and Matlab in biometric image/signal processing, Introduction to Biometric Algorithms and Systems with emphasis on any two of the following: Face, Fingerprint, Iris, Speech & speaker. Multimodal biometrics, Privacy issues and other aspects of biometrics, Applications of biometrics & future trends. The course also addresses such challenging issues as security strength, recognition rates and privacy, as well as alternatives of passwords and smart cards.

CSS 325: Enterprise and Perimeter Security (2 Units: LH 20, P 30)

Students will examine network-based attacks, whether originating from the Internet or the local LAN, and learn about ways to protect, detect, and defend the enterprise network from such attacks. Perimeter security (Firewalls, IDS, IPS, VPN, proxy servers) enterprise security policies, as well as securing devices on large-scale distributed networks. Students will participate in hands-on experiments and demonstrate their understanding of subject matter via writing and presentations.

CSS 327: Cryptographic Techniques (2 Units: LH 20, P 30)

Explores symmetric and asymmetric cryptography, key management, and encryption algorithms such as DES, AES, RSA, and PGP. Discusses PKI, SSL, and VPN including how to use protocols, hashing, digital signatures, and certificates and certificate authorities. Covers policies, procedures, and methods for the proper use of cryptography in secure systems.

CSS 329: Information Security Engineering (2 Units: LH 20, P 30)

System and management view of information security, Requirements for information security, System-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 system-engineering process, Laws related to information and management of operational systems.

CSS 331: Systems Security (3 Units: LH 45, P 45)

Security Principles, Account Security, File System Security, Assessing Risk, Risk Analysis, and Encryption. The student's basic network and operating system skills will be expanded to include planning, implementation, and auditing of a system's security package. Secure design and secure coding principles, practices, and methods including least privilege, threat modeling, and static analysis. Covers common vulnerabilities such as buffer overruns, integer overflows, injection attacks, cross-site scripting, and weak error handling.

CSS 360: Industrial Training (6 Units)

Student's Industrial work experience of 6 months' duration. Students' reports will be presented in a seminar.

LEVEL 400

CSS 411: Cyber Law (1 Unit: LH 1, P 0)

This course provides an overview of the legal doctrines and principles that apply to the operation and development of computer technology and the Internet. Topics include: issues related to jurisdiction, constitutional issues of free speech, property rights, e-business, and current developments in legislation and case law.

CSS 421: Software Defined Networks (2 Units: LH 20, P 30)

History, Motivation and Concept of SDN, SDN Architecture, SDN Application, Controller, Datapath, Control to Data-Plane Interface (CDPI), SDN Northbound Interfaces (NBI), Deployment Models, Application areas of SDN, Security Using SDN Paradigm.

CSS 422: Database Management and Control System (2 Units: LH 20, P 30)

Introduction: Security issues faced by enterprise, installing a typical database product, Security architecture, Operating system security principles, Administration of users, Profiles, password policies, privileges and roles, Database application security models, Database auditing models, Application data auditing, Practices of database auditing.

CSS 424: VoIP and Multimedia Security (2 Units: LH 20, P 30)

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.

CSS 425: Cloud Computing Security (2 Units: LH 20, P 30)

Introduction to cloud computing, cloud computing vendors cloud Computing threats, Cloud Reference Model. Introduction to data centers: servers, data storage, networking and virtualization. Data center networking, Introduction to server virtualization software: VMware VSphere. Virtual machine management: configuration, placement and resource allocation. Power efficiency in virtual data centers. Fault tolerance in virtual data centers., The Cloud Cube Model and Security for Cloud Computing. Security in the Cloud, Cloud Threats, Threat Mitigation, Cloud 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 Program, Cloud Business Continuity Planning.

CSS 426: Fault Tolerant Computing (2 Units: LH 20, P 30)

Introduction and overview of fault tolerant schemes; fault and error modelling; test generation and fault simulation; concepts in fault-tolerance; reliability/availability modelling; system level diagnosis; low level fault-tolerance – coding techniques (basic principles, parity bit codes, hamming codes, error detection and retransmission codes, burst error correction codes, Reed-Solomon codes, etc.); high-level fault tolerant techniques in systems: rollback, check pointing, reconfiguration; software fault-tolerance; fault tolerant routing; integrated hardware/software fault-tolerance; redundancy, spares and repairs – apportionment, system versus component redundancy, parallel redundancy, RAID system reliability, N-modular redundancy; software reliability and recovery techniques, network system reliability, reliability optimization.

CSS 427: Information Disaster Recovery (2 Units: LH 20, P 30)

Disaster Recovery Philosophy, Principles and Planning, Contingency Plan Components, Agency Response Procedures and Continuity of Operations, Planning Processes, Continuity and Recovery Function, Steps of Disaster Recovery Planning, Role of IT and Network Management in Disaster Recovery, Developing the Disaster Recovery, Executive Support, DRP Leadership, Cross Department Subcommittee, Department Level Teams, Relationship between IT and Network Staff with Departments, Planning Team Skill Inventory, DRP Team Training, DRP Awareness Campaign, Standards and Regulatory Bodies, Assessing Organizational Risk, Documenting Business Processes, Business Process Inventory, Identifying Threats and Vulnerabilities, Measuring and Quantifying Threats, Risk Reports, Prioritizing systems and Functions for Recovery, Classifying Systems, Determination of Backup Requirements.

CSS 429: Cyber Security in Business and Industry (2 Units: LH 20, P 30)

A study of the application and integration of cybersecurity principles, frameworks, standards, and best practices to the management, governance, and policy development processes for businesses. Discussion covers the organization, management, and governance of cybersecurity for enterprise IT in business settings; risk and risk management practices; and development and implementation of industry-wide cybersecurity initiatives and programs.

CSS 432: System Vulnerability Assessment and Testing (3 Units: LH 45, P 45)

This course focuses on testing methods and techniques to effectively identify and mitigate risks to the security of a company's infrastructure. Topics include penetration testing methodologies, test planning and scheduling, information gathering, password cracking penetration testing and security analysis, social engineering penetration testing and security analysis, internal and external penetration testing and security analysis, router penetration testing and security analysis and reporting and documentation. Operating system fingerprinting, remote network mapping, software and operational vulnerabilities, attack surface analysis, fuzz testing, patch management, and security auditing.

CSS 460: Project **(6 Units: PH 270)**

Students should embark on a project under the supervision of a member of staff.

If you have any questions or need further information, please do not hesitate to reach out.

Yours faithfully,

Dr. Idris Ahmed
Ag. H.O.D, Cyber Security