



ILAYS NATIONAL UNIVERSITY

JAAMACADDA UMMADDA ILAYS



Faculty of Computer Science



Department of Computer
Networking and Security



Bachelor of Computer
Networks and Security



Ilays University, Lasanod,
Northeastern State, Somalia



www.ilaysuniversity.edu.so



info@ilaysuniversity.edu.so



| ILAYS NATIONAL UNIVERSITY

Table of Contents

1. Department Overview	3
1.1 Vision.....	4
1.2 Mission	4
1.3 Core Values.....	5
1.4 The Department at a Glance.....	5
1.5 Academic Philosophy.....	5
1.6 Learning Environment and Facilities.....	6
2. Programme Objectives	8
2.1 Operational Objectives.....	8
2.2 Programme Educational Objectives	9
3. Curriculum Structure and Academic Progression.....	10
3.1 Design and Harmonization Principles.....	10
3.2 Course Type Key.....	11
3.3 Academic Progression Map.....	11
3.4 Contact-Hour Convention.....	11
3.5 Semester-by-Semester Curriculum.....	12
3.5.1 Foundation Year – Semester I	12
3.5.2 Foundation Year – Semester II	12
3.5.3 Year I – Semester I.....	13
3.5.4 Year I – Semester II	13
3.5.5 Year II – Semester I	14
3.5.6 Year II – Semester II.....	14
3.5.8 Year III – Semester II.....	15
3.5.9 Year IV – Semester I.....	16
3.5.10 Year IV – Semester II	16
4. Programme Learning Outcomes.....	18

4.1 Staged Attainment of Outcomes.....	19
5. Attributes of Graduates	20
6. Employability and Readiness of Graduates.....	21
6.1 Career Pathways	21
6.2 Sectors of Employment	22
6.3 Alignment with Professional Certification.....	22
6.4 Internship, Portfolio and Transition to Work	23
6.5 Postgraduate Study and Further Advancement.....	23
7. Teaching, Learning and Assessment.....	24
7.1 Modes of Delivery	24
7.2 Assessment Framework.....	25
7.3 Assessment Instruments	25
7.4 Feedback and Academic Integrity	26
7.5 Quality Assurance and Continuous Improvement.....	26
8. Research and Innovation	27
8.1 Priority Research Strands	27
8.2 The Research Pathway within the Curriculum	28
8.3 Innovation, Enterprise and Community Engagement	28
9. Strengths of the Curriculum.....	Error! Bookmark not defined.
10. Recommended Elective Pool.....	29
11. Graduation Requirements	29
12. Curriculum Approval Record.....	Error! Bookmark not defined.

1. Department Overview

The Department of Computer Networks and Security is the academic unit of Ilays National University responsible for the design, delivery, quality assurance and continuous development of the Bachelor of Computer Networks and Security. The department educates the engineers and specialists who build, operate, monitor and defend the network and systems infrastructure on which government services, financial institutions, telecommunications operators, humanitarian organizations, education providers and private enterprise now depend.

The department exists because connectivity and security have become inseparable. Every organization that connects a branch office, migrates a service to the cloud, opens a mobile money channel or publishes a public-facing portal simultaneously creates a network to be engineered and an attack surface to be defended. Historically these two responsibilities were taught, staffed and managed separately. The department rejects that separation. Its graduates are prepared as network professionals who think defensively by default and as security professionals who understand, at packet and protocol level, the infrastructure they are asked to protect.

The programme is deliberately built on a harmonised computing core shared with the Bachelor of Computer Science in Software Engineering. Approximately seventy-one per cent of bachelor-level credits are common to both programmes, covering programming, mathematics, computer systems, databases, networks, cybersecurity fundamentals, cloud computing, artificial intelligence, research methods, professional practice and the project and capstone sequence. The remaining twenty-nine per cent establishes the distinct professional identity of the networks and security graduate through routing and switching, server administration, network services, wireless systems, network automation, network security, penetration testing, security operations, digital forensics, enterprise network design and advanced network defence.

This structure is an academic decision before it is an administrative one. A shared core guarantees that a networks graduate is a genuine computing graduate, able to write code, reason about algorithms and data, work with databases and understand distributed and cloud systems, rather than a technician trained only in device configuration. It also permits common timetabling, shared laboratories, consistent assessment standards and a single quality benchmark across both programmes, while allowing each to specialise progressively and without duplication.

The curriculum is practice-weighted by design. Across the full pathway students accumulate 2,752 supervised practical hours against 1,920 lecture hours, a ratio of roughly 1.43 practical hours for every lecture hour. In the final year, practical engagement rises sharply as internship, capstone implementation and senior specialisation laboratories dominate the schedule. Students do not merely study routing protocols, directory

services, firewalls, intrusion detection, forensic acquisition or automation scripts; they configure, break, repair, measure, secure and document them under supervision.

The department also accepts a responsibility beyond its own students. Reliable and defensible digital infrastructure is a national development requirement, and a shortage of qualified network and security professionals is a strategic vulnerability. The department therefore positions itself as a contributor to national capacity: through graduates who can be trusted with critical systems, through applied research relevant to the local operating environment, through professional and community engagement, and through advocacy for lawful, ethical and accountable security practice.

1.1 Vision

VISION

To be a leading centre of excellence in computer networking and cybersecurity education in Somalia and the wider Horn of Africa, producing ethical, technically capable and industry-ready professionals who can design, operate and defend modern digital infrastructure.

1.2 Mission

MISSION

To provide comprehensive and practice-oriented education in networking and cybersecurity through strong computing foundations, intensive laboratory work, secure infrastructure design, ethical security practice, research, professional engagement and continuous alignment with evolving technologies and threats.

1.3 Core Values

Technical Excellence	Depth of knowledge and hands-on mastery of the systems, protocols and tools that carry national and organizational data.
Ethical Practice	Security capability exercised only within lawful, authorized and professionally accountable boundaries.
Practice Orientation	Learning anchored in laboratories, live equipment, simulation and real infrastructure rather than description alone.
Relevance	Continuous alignment of content with national digital priorities, employer demand, professional certification and the evolving threat landscape.
Inquiry and Innovation	A culture in which students investigate, measure, question and build rather than only consume technology.

1.4 The Department at a Glance

Academic unit	Department of Computer Networks and Security
Degree awarded	Bachelor of Computer Networks and Security
Programme model	1 Foundation Year + 4 Degree Years (10 semesters)
Credit structure	36 Foundation credits + 144 degree-stage credits = 180 credits
Shared core (degree stage)	102 credits, approximately 71 % of bachelor-level credits
Specialization (degree stage)	42 credits, approximately 29% of bachelor-level credits
Contact hours	1,920 lecture hours and 2,752 supervised practical hours
Semester length	16 teaching weeks
Mode of delivery	Full-time, on-campus, laboratory-intensive
Language of instruction	English

1.5 Academic Philosophy

The department's academic philosophy rests on five commitments that shape every course, laboratory and assessment in the programme.

- **Foundations before tools.** Products, vendors and platforms change; addressing, protocols, operating-system behaviour, cryptographic principles and system architecture endure. Students learn the underlying model first, then apply it on current platforms, so that competence transfers when the technology changes.
- **Build it, then break it, then defend it.** Offensive technique is taught only after students can construct and operate the systems in question, and always inside an authorised, contained laboratory environment. Understanding attack is a means of building defence, never an end in itself.
- **Security as a property of design.** Security is not a final-year add-on. It enters at Year I through networking fundamentals, is formalized in Year II through cybersecurity and internet security, and is then applied continuously through cryptography, network security, secure administration, monitoring and enterprise design.
- **Progressive independence.** Supervision is intentionally reduced across the pathway. Early laboratories are guided and prescriptive; Project I and Project II are team-based and semi-directed; the capstone requires students to define, justify, implement, evaluate and defend a substantial piece of work largely on their own initiative.
- **Professional accountability.** Technical work is assessed alongside documentation, reporting, ethical reasoning and legal awareness, because in professional practice an undocumented or unlawful intervention is a failed intervention regardless of its technical elegance.

1.6 Learning Environment and Facilities

Teaching is organised around laboratory environments that allow students to work on real and virtualised infrastructure. The programme's practical hours assume access to networking laboratories with routers, switches, structured cabling and wireless equipment; server and virtualisation environments supporting Linux and Windows Server administration; an isolated security laboratory in which vulnerability assessment, penetration testing, malware handling and forensic acquisition can be conducted without risk to production systems; and network simulation and emulation software that allows large topologies to be modelled where physical equipment is limited.

Laboratory design follows the principle of containment. Any exercise involving exploitation, traffic capture, credential attack or malicious code is confined to a segregated environment with no route to institutional or public networks, and is governed by written rules of engagement that students formally accept before participation. Students learn the discipline of authorized testing as an operational habit, not as a policy statement.

The department also maintains the software toolchain expected of the profession: protocol analyzers, configuration and automation frameworks, monitoring and log-management platforms, security information and event management tooling, forensic imaging and analysis utilities, and cloud platform access for virtualization and infrastructure automation. Where licensing or hardware constraints apply, open-source and community-edition equivalents are used so that no student is excluded from the practical component of any course.

2. Programme Objectives

The programme objectives describe what the department sets out to achieve through the curriculum. They are stated at two levels: operational objectives that guide course design and delivery, and programme educational objectives that describe the professional standing expected of graduates three to five years after graduation.

2.1 Operational Objectives

- Develop strong foundations in programming, mathematics, computer systems, databases, networking and cybersecurity that support lifelong technical growth.
- Develop competence in routing, switching, network services, server administration and enterprise network design.
- Prepare students to configure, monitor, troubleshoot and secure wired, wireless, virtualized and cloud-based networks.
- Develop skills in network automation, security operations, vulnerability assessment, penetration testing and digital forensics.
- Develop understanding of cryptography, incident response, cyber law, privacy and professional security practice.
- Build research, project-management, teamwork, communication and entrepreneurship capabilities.
- Prepare graduates for professional roles in networking, cybersecurity, cloud infrastructure and security operations, and for postgraduate study.
- Instill the habit of authorized, documented and accountable practice in every technical intervention.

2.2 Programme Educational Objectives

Programme educational objectives express the intended achievement of graduates in the early years of professional practice.

Ref.	Objective	Statement
PEO 1	Professional competence	Graduates practice successfully as network, systems or security professionals, designing, deploying, operating and troubleshooting reliable infrastructure in organisational settings.
PEO 2	Security leadership	Graduates assume responsibility for the protection of organisational information assets through monitoring, assessment, hardening, incident response and defensible architecture.
PEO 3	Technical adaptability	Graduates absorb new platforms, protocols, threats and tools independently, sustaining relevance as the technology and threat landscape changes.
PEO 4	Ethical and legal integrity	Graduates apply professional codes, cyber law, privacy principles and authorisation discipline consistently, including under commercial or institutional pressure.
PEO 5	Communication and teamwork	Graduates work effectively in multidisciplinary teams and communicate technical findings and recommendations clearly to both specialist and non-specialist audiences.
PEO 6	Advancement and contribution	Graduates progress into senior technical roles, postgraduate study, professional certification, entrepreneurship or teaching, and contribute to national digital capacity.

3. Curriculum Structure and Academic Progression

The curriculum is delivered over ten semesters: two Foundation Year semesters of 36 credits and eight degree-stage semesters of 144 credits, giving a total pathway of 180 credits. Degree-stage semesters carry a stable load of 18 credits, which supports predictable timetabling, consistent workload and reliable progression.

3.1 Design and Harmonization Principles

- **Common-core design.** Courses marked “Shared Core” use the same code, title, credit value, lecture hours and practical hours in both degree programmes. Students may therefore attend the same class and laboratory sections for those courses, under a single syllabus and assessment framework.
- **Progressive specialization.** The Foundation Year is fully shared. Year I contains one specialisation course per semester. From Year II onward each programme normally contains two specialisation courses per semester, while the remaining courses continue to be shared.
- **Prerequisite logic.** Programming and mathematics precede algorithms; computer architecture precedes operating systems; networking fundamentals precede routing and security; cybersecurity fundamentals precede cryptography and penetration testing; research methods and project courses precede the capstone.
- **Shared-degree balance.** The degree stage contains 102 shared credits and 42 specialisation credits. Approximately 71% of bachelor-level credits are common to both programmes, while 29% establish the professional identity of each specialisation.

- **Vertical integration.** Each specialisation strand is developed across multiple semesters rather than delivered in a single course, so that routing, security, administration and automation each mature through repeated and deepening exposure.
- **Project spine.** Project I, Project II, the internship and the two-semester capstone form a continuous line of increasingly independent applied work running through the second half of the programme.

3.2 Course Type Key

Shared Core	Identical code, title, credit value, lecture hours and practical hours in both the Computer Networks and Security programme and the Computer Science in Software Engineering programme. Timetabled jointly.
CNS Specialization	Delivered only to Computer Networks and Security students, with discipline-specific laboratories, projects and assessment tasks. Timetabled separately.

3.3 Academic Progression Map

Stage	Focus of the stage
Foundation	Academic, mathematical and computing readiness
Year I	Programming and systems foundations with networking fundamentals
Year II	Linux and Python, routing, server administration, cybersecurity and network services
Year III	Cryptography, network security, wireless, automation and penetration testing
Year IV	AI and cloud, security operations, forensics, enterprise design, advanced network security, internship and capstone

3.4 Contact-Hour Convention

LH and PH denote total contact and supervised hours across a full sixteen-week semester. Theory courses normally use 48 lecture hours for a 3-credit course; mixed courses combine lecture and laboratory contact; practical programming, networking and security courses carry expanded laboratory hours. Project, internship and capstone hours represent supervised practical and project engagement rather than ordinary classroom meetings.

3.5 Semester-by-Semester Curriculum

The tables below list every course in the pathway with its code, type, credit value, lecture hours (LH) and practical hours (PH). Each page presents one stage of the programme.

3.5.1 Foundation Year – Semester I.

No.	Code	Course Title	Type	Cr.	LH	PH
1	FE000	Freshman English	Shared Core	3	48	0
2	PC001	Pre-Calculus	Shared Core	3	48	0
3	SH002	Somali History and Culture I	Shared Core	2	32	0
4	CT003	Critical Thinking	Shared Core	2	32	0
5	CF004	Computer Fundamentals	Shared Core	3	32	32
6	CA005	Computer Applications / Digital Literacy	Shared Core	3	16	64
SEMESTER TOTAL				16	208	96

3.5.2 Foundation Year – Semester II

No.	Code	Course Title	Type	Cr.	LH	PH
1	AE007	Academic English I	Shared Core	3	48	0
2	CL008	Calculus	Shared Core	3	48	0
3	IS009	Islamic Studies	Shared Core	2	32	0
4	IP010	Introduction to Programming & Computing	Shared Core	4	32	64
5	WD011	Web Development Fundamentals	Shared Core	3	32	32
6	SH012	Somali History and Culture II	Shared Core	2	32	0
7	CM013	Computer Hardware Fundamentals & Maintenance	Shared Core	3	16	64
SEMESTER TOTAL				20	240	160

3.5.3 Year I – Semester I

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC101	Academic English II & Technical Communication	Shared Core	3	48	0
2	CSC102	Programming Fundamentals	Shared Core	3	32	64
3	CSC103	Discrete Mathematics	Shared Core	3	48	0
4	CSC104	Probability and Statistics	Shared Core	3	48	0
5	CSC105	Computer Organization & Architecture	Shared Core	3	32	32
6	CNS106	Networking Fundamentals I	CNS Specialization	3	32	64
SEMESTER TOTAL				18	240	160

3.5.4 Year I – Semester II

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC107	Object-Oriented Programming	Shared Core	3	32	64
2	CSC108	Data Structures & Algorithms	Shared Core	3	32	32
3	CSC109	Operating Systems	Shared Core	3	32	32
4	CSC110	Database Systems I	Shared Core	3	32	32
5	CSC111	Computer Networks I	Shared Core	3	32	32
6	CNS112	Networking Fundamentals II	CNS Specialization	3	32	64
SEMESTER TOTAL				18	192	256

3.5.5 Year II – Semester I

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC201	Python Programming	Shared Core	3	32	64
2	CSC202	Systems Programming & Linux	Shared Core	3	32	64
3	CSC203	Fundamentals of Cybersecurity	Shared Core	3	32	32
4	CSC204	Internet & Web Security Fundamentals	Shared Core	3	32	32
5	CNS205	Routing & Switching I	CNS Specialization	3	32	64
6	CNS206	Windows Server Administration	CNS Specialization	3	32	64
SEMESTER TOTAL				18	192	320

3.5.6 Year II – Semester II

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC207	Design & Analysis of Algorithms	Shared Core	3	48	32
2	CSC208	Cloud & Distributed Computing Fundamentals	Shared Core	3	32	32
3	CSC209	Computing Ethics & Professional Practice	Shared Core	2	32	0
4	CSC210	Project I – Computing Project	Shared Core	4	0	96
5	CNS211	Routing & Switching II	CNS Specialization	3	32	64
6	CNS212	Network Services & Infrastructure	CNS Specialization	3	32	64
SEMESTER TOTAL				18	176	288

3.5.7 Year III – Semester I

Research, cryptography, data and mathematics are common; advanced specialization begins in two courses.

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC301	Applied Cryptography	Shared Core	3	48	32
2	CSC302	Research Methods in Computing	Shared Core	3	32	32
3	CSC303	Data Analysis	Shared Core	3	32	64
4	CSC304	Linear Algebra for Computing	Shared Core	3	48	0
5	CNS305	Network Security	CNS Specialization	3	32	64
6	CNS306	Wireless & Mobile Networks	CNS Specialization	3	32	64
SEMESTER TOTAL				18	224	256

3.5.8 Year III – Semester II

Distributed systems, IoT, project management and the integrated project are common; two specialization courses deepen professional capability.

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC307	Distributed Systems	Shared Core	3	32	32
2	CSC308	Internet of Things	Shared Core	3	32	64
3	CSC309	ICT Project Management & Entrepreneurship	Shared Core	3	32	32
4	CSC310	Project II – Integrated Computing Project	Shared Core	3	0	96
5	CNS311	Network Programming & Automation	CNS Specialization	3	32	64
6	CNS312	Ethical Hacking & Penetration Testing	CNS Specialization	3	32	64
SEMESTER TOTAL				18	160	352

3.5.9 Year IV – Semester I

Advanced shared technologies and capstone preparation are combined with two senior specialisation courses.

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC401	Artificial Intelligence & Machine Learning	Shared Core	3	32	64
2	CSC402	Cloud Computing, Virtualization & Infrastructure Automation	Shared Core	3	32	64
3	CSC403	Cyber Law, Ethics & Digital Privacy	Shared Core	3	48	0
4	CSC404	Capstone Project I – Proposal & Design	Shared Core	3	16	64
5	CNS405	Security Operations & SIEM	CNS Specialization	3	32	64
6	CNS406	Digital Forensics & Incident Response	CNS Specialization	3	32	64
SEMESTER TOTAL				18	192	320

3.5.10 Year IV – Semester II

Internship, capstone implementation and professional portfolio are common; two final specialisation courses complete the professional track.

No.	Code	Course Title	Type	Cr.	LH	PH
1	CSC407	Internship / Professional Practice	Shared Core	4	0	192
2	CSC408	Capstone Project II – Implementation & Defense	Shared Core	6	16	192
3	CSC409	Capstone Seminar & Professional Portfolio	Shared Core	2	16	32
4	CNS410	Enterprise Network Design & Management	CNS Specialization	3	32	64
5	CNS411	Advanced Network Security	CNS Specialization	3	32	64
SEMESTER TOTAL				18	96	544

3.6 Credit and Contact-Hour Summary

Stage / Semester	Credits	LH	PH	Status
Foundation – Semester I	16	208	96	Shared
Foundation – Semester II	20	240	160	Shared
Year I – Semester I	18	240	160	Degree
Year I – Semester II	18	192	256	Degree
Year II – Semester I	18	192	320	Degree
Year II – Semester II	18	176	288	Degree
Year III – Semester I	18	224	256	Degree
Year III – Semester II	18	160	352	Degree
Year IV – Semester I	18	192	320	Degree
Year IV – Semester II	18	96	544	Degree
FOUNDATION TOTAL	36	448	256	
DEGREE TOTAL	144	1,472	2,496	
OVERALL PATHWAY	180	1,920	2,752	

Practical hours exceed lecture hours across the pathway by a ratio of approximately 1.43 to 1, and the practical proportion rises sharply in the final year as internship, capstone implementation and senior specialisation laboratories dominate the schedule.

4. Programme Learning Outcomes

Graduates are expected to demonstrate the following outcomes on completion. Each is assessed through identified course-level tasks and mapped to the objectives in Section 2.

Ref.	On completion, graduates will be able to:	Supports
PLO 1	Design, configure, operate and troubleshoot scalable computer networks and network services.	PEO 1, 3
PLO 2	Administer Linux and Windows systems and integrate them securely into organisational infrastructure.	PEO 1, 2
PLO 3	Apply routing, switching, wireless, network automation and enterprise network design principles to meet defined organisational requirements.	PEO 1, 3
PLO 4	Assess vulnerabilities and implement appropriate network and system security controls.	PEO 2, 4
PLO 5	Use security monitoring, SIEM, incident-response and digital-forensics methods in authorised environments.	PEO 2, 4
PLO 6	Apply cryptography, access control, secure protocols and defensive architecture appropriately.	PEO 2
PLO 7	Write, adapt and reason about programs, and apply computing, mathematical and data-analysis foundations to networking and security problems.	PEO 1, 3, 6
PLO 8	Work effectively in teams and communicate technical findings, reports and recommendations professionally.	PEO 5
PLO 9	Apply professional, ethical, legal and privacy principles to technical decisions and to the conduct of security work.	PEO 4
PLO 10	Plan, conduct, document and defend a substantial networking or security investigation or project, and sustain independent learning thereafter.	PEO 3, 6

4.1 Staged Attainment of Outcomes

Outcomes are not attained in a single course. The level of achievement expected at the end of each stage is set out below.

Stage	Level of attainment	Expected demonstration
Foundation	Awareness and readiness	Students demonstrate academic literacy, mathematical readiness, digital fluency, introductory programming and hardware competence.
Year I	Comprehension and basic application	Students program with confidence, reason about computer organization and operating systems, and configure fundamental network components.
Year II	Applied competence	Students administer servers, configure routed and switched networks, deploy core network services and apply cybersecurity fundamentals in guided settings.
Year III	Analysis and integration	Students secure networks, deploy wireless infrastructure, automate configuration, conduct authorised testing and evaluate designs against requirements.
Year IV	Synthesis, evaluation and independence	Students design enterprise infrastructure, operate security monitoring and response, conduct forensic investigation, and deliver and defend an independent capstone.

5. Attributes of Graduates

Beyond examinable outcomes, the department cultivates a recognizable professional character. The following attributes describe the graduate the programme is designed to produce, and are developed cumulatively through laboratory practice, project work, supervision, internship and the ethical framing applied throughout the curriculum.

Technically grounded	Competent across the full stack a network professional must command: cabling and hardware, addressing and routing, operating systems, services, wireless, virtualization, cloud and security tooling.
Defensively minded	Trained to ask how a system fails, how it is attacked and how it is monitored before declaring it complete.
Ethically anchored	Committed to authorization, proportionality, confidentiality and lawful conduct, and able to refuse or escalate improper technical requests.
Analytically rigorous	Able to diagnose from evidence — logs, captures, configurations and metrics — rather than from assumption or trial and error.
Articulate	Able to produce professional documentation, incident reports, network designs and assessment findings, and to brief technical and non-technical audiences.
Collaborative	Experienced in team-based project delivery, peer review, task division and shared accountability for outcomes.
Independent and self-renewing	Habituated to learning new platforms and threats without formal instruction, supported by research methods training and capstone experience.
Enterprising	Equipped through project management and entrepreneurship training to identify service opportunities and establish or grow technology ventures.
Contextually aware	Able to design realistic solutions for local constraints of bandwidth, power, budget, supply chain and skills availability, without lowering security standards.
Professionally responsible	Accustomed to documenting work, respecting change control, protecting evidence integrity and accepting accountability for technical decisions.

6. Employability and Readiness of Graduates

Employability is treated as a design requirement of the curriculum rather than an outcome left to chance. Three mechanisms carry it: a practical hour load that produces demonstrable configuration and diagnostics

6.1 Career Pathways

Role	Core capability required	Principal enabling courses
Network Engineer / Network Administrator	Routing, switching, network services, enterprise design	CNS106, CNS112, CNS205, CNS211, CNS212, CNS410
Systems / Server Administrator	Windows and Linux administration, directory and virtualisation services	CSC202, CNS206, CSC402
Cybersecurity Analyst	Threat detection, monitoring, log analysis, alert triage	CSC203, CNS305, CNS405
Security Operations Centre (SOC) Analyst	SIEM operation, incident detection and escalation	CNS405, CNS406, CNS411
Penetration Tester / Vulnerability Analyst	Authorised testing, exploitation, reporting and remediation advice	CNS312, CNS305, CSC204
Digital Forensics / Incident Response Specialist	Evidence acquisition, analysis, containment and recovery	CNS406, CSC403
Cloud Infrastructure / DevOps Engineer	Virtualisation, cloud deployment, infrastructure automation	CSC208, CSC402, CNS311
Network Automation Engineer	Scripted configuration, orchestration, programmable networks	CSC201, CNS311
Wireless / Telecommunications Engineer	Wireless design, mobile networks, site survey and optimization	CNS306, CNS410
IT Support / Field Engineer (entry route)	Hardware, operating systems, connectivity and user support	CM013, CSC109, CSC111
ICT Consultant / Technology Entrepreneur	Advisory, design, implementation and managed services	CSC309, CSC407, CSC408

6.2 Sectors of Employment

- Telecommunications and internet service providers
- Banking, mobile money and financial services
- Government ministries, agencies and regulatory bodies
- Humanitarian, United Nations and non-governmental organizations
- Health services and hospital information systems
- Higher education and research institutions
- Energy, transport, ports and other critical infrastructure operators
- Managed service providers, systems integrators and ICT consultancies
- Independent practice, contracting and technology entrepreneurship

6.3 Alignment with Professional Certification

Course content is structured so that students preparing for widely recognized industry credentials are covering familiar ground rather than starting again. The department does not award these credentials and does not guarantee examination success; the mapping below indicates where curriculum content substantially supports certification preparation.

Certification domain	Supporting courses	Typical credential family
Networking associate level	CNS106, CNS112, CNS205, CNS211, CSC111	Vendor associate-level routing and switching credentials
Vendor-neutral networking	CSC111, CNS212, CNS306	General network technician and infrastructure credentials
Vendor-neutral security	CSC203, CSC204, CNS305	Foundational security practitioner credentials
Systems administration	CSC202, CNS206	Linux and Windows Server administration credentials
Ethical hacking/ offensive security	CNS312, CNS411	Penetration testing and offensive security credentials

Security operations and analysis	CNS405, CNS406	SOC analyst, incident handling and forensics credentials
Cloud infrastructure	CSC208, CSC402	Cloud associate and cloud security credentials

6.4 Internship, Portfolio and Transition to Work

The 4-credit Internship / Professional Practice course carries 192 supervised hours in an approved organization and is a graduation requirement. Students are assessed on workplace supervisor evaluation, a maintained logbook and a reflective report, and the placement is used deliberately as a recruitment channel: employers assess a candidate over a full semester rather than in a single interview.

The Capstone Seminar and Professional Portfolio course consolidates evidence accumulated across the programmed: configuration artefacts, laboratory reports, security assessments, network designs, automation scripts, project documentation and the capstone thesis. Graduates therefore enter the labor market with a demonstrable body of work rather than a transcript alone.

6.5 Postgraduate Study and Further Advancement

The shared computing core, the mathematics sequence, Research Methods in Computing and the two-semester capstone together satisfy the normal entry expectations for master's-level study in computer networks, cybersecurity, information security management, cloud computing and related fields. Graduates intending an academic route are encouraged to develop their capstone toward publishable form during the final year.

7. Teaching, Learning and Assessment

Teaching in the department is organized around the principle that networking and security competence is demonstrated, not recited. Delivery therefore combines conceptual instruction with sustained supervised practice, and assessment is weighted toward evidence of what a student can actually configure, diagnose, secure and document.

7.1 Modes of Delivery

Lectures and structured seminars	Establish conceptual models, protocol behaviour, standards and theory, supported by worked examples and guided problem solving.
Supervised laboratories	The core of the programme. Students configure, test, break and repair real or virtualized infrastructure against defined objectives and verification criteria.
Simulation and emulation	Network simulation software extends laboratory reach, allowing large or multi-site topologies to be built where physical equipment is limited.
Case-based analysis	Real incidents, breaches, outages and design failures are examined to develop diagnostic reasoning and professional judgement.
Team projects	Project I, Project II and the capstone require division of work, integration, peer review and joint accountability for a delivered system.
Industry engagement	Internship, guest practitioners, site visits and employer-informed briefs connect academic work to operational reality.
Independent research	Research Methods and the capstone develop literature review, methodology design, data collection, analysis and academic writing.
Structured self-study	Documentation reading, vendor material, laboratory repetition and certification preparation build the habit of self-directed technical learning.

7.2 Assessment Framework

The indicative weightings below apply within the university's general assessment regulations. Precise distributions are specified in each course syllabus.

Course category	Continuous assessment components	Wt.	Final assessment	Wt.
Theory-dominant courses	Continuous assessment, assignments presentations and mid term exam	60%	Written final examination	40%
Mixed lecture / laboratory courses	Laboratory work, practical tests, assignments and continuous assessment	60%	Written and practical final examination	40%
Laboratory-intensive courses	Configuration tasks, laboratory reports, practical tests and portfolio	60%	Practical and written final examination	40%
Project courses (Project I and II)	Milestone deliverables, supervision reports, teamwork and documentation	70%	Demonstration and oral defence	30%
Internship / Professional Practice	Workplace supervisor evaluation, logbook and reflective report	60%	Institutional presentation and assessment	40%
Capstone Project	Proposal, design, implementation milestones and written thesis	60%	Public demonstration and oral defence	40%

7.3 Assessment Instruments

- Practical configuration and troubleshooting tasks assessed against verifiable outcomes rather than description
- Laboratory reports requiring evidence, methodology, results and interpretation
- Timed diagnostic exercises in which a broken topology or compromised system must be restored
- Security assessment reports written to professional structure, including findings, risk rating and remediation advice
- Design assignments producing addressing schemes, topology diagrams, security architecture and justification
- Scripts, automation artefacts and code reviewed for correctness, readability and safety
- Written examinations testing conceptual understanding, protocol reasoning and analytical judgement
- Oral defence and demonstration for project and capstone work
- Professional portfolios evidencing accumulated practical competence across the programme

7.4 Feedback and Academic Integrity

Laboratory and project work receives formative feedback within a defined turnaround so that correction can occur while the material is still active. Project and capstone supervision is structured around scheduled milestones rather than a single end-of-semester submission.

Academic integrity is enforced with particular firmness in this discipline. Submitted configurations, scripts and reports must be the student's own work, testing activity must be authorised and contained, and the misuse of security tooling against systems for which authorisation has not been granted is treated as a serious disciplinary matter in addition to any legal consequence. Students formally accept the departmental rules of engagement before undertaking any offensive or forensic laboratory exercise.

7.5 Quality Assurance and Continuous Improvement

Course files and moderation	Every course maintains a file containing the syllabus, delivery record, assessment instruments, marking schemes and samples of graded work, subject to internal moderation.
Outcome mapping	Assessment tasks are mapped to programme learning outcomes so that attainment can be evidenced at course and programme level rather than inferred.
Student feedback	End-of-course evaluation and periodic focus discussions inform teaching adjustment, laboratory provision and resource planning.
Employer and alumni input	Internship supervisor reports, employer consultation and alumni tracking are used to test the continuing relevance of course content.
Periodic curriculum review	The curriculum is reviewed on a defined cycle, with interim revision permitted where technological or threat developments require earlier action.
Shared-course alignment	Courses marked Shared Core are jointly monitored with the sister programme to ensure identical syllabi, standards and assessment expectations.

8. Research and Innovation

Research in the department is applied in orientation. Its purpose is to improve the reliability, security and affordability of digital infrastructure in the operating environment in which its graduates will actually work, characterised by constrained bandwidth, intermittent power, limited redundancy, tight budgets and scarce specialist staffing. Problems of this kind are under-represented in the international literature, which makes local investigation both academically legitimate and practically valuable.

8.1 Priority Research Strands

Network performance and resilience	Measurement, optimisation and fault tolerance of networks operating under constrained bandwidth, unstable power and limited redundancy.
Applied cybersecurity for developing infrastructure	Threat profiling, control selection and cost-effective defence for organisations with limited security budgets and staffing.
Security operations and threat detection	Log analytics, detection engineering, alert quality and practical SIEM deployment in small and medium operational environments.
Digital forensics and incident response	Evidence handling, acquisition methodology and investigative practice consistent with local legal requirements.
Wireless, mobile and last-mile connectivity	Coverage, capacity and security of wireless deployments serving underserved and rural communities.
IoT and operational technology security	Protection of connected devices and control systems in health, energy, water and transport contexts.
Cloud, virtualization and infrastructure automation	Secure migration, configuration-as-code, orchestration and cloud security posture management.
Applied artificial intelligence for defense	Anomaly detection, traffic classification and triage support, together with the limitations and risks of such methods.
Cyber law, policy and digital privacy	Regulatory readiness, data protection practice, institutional policy design and professional accountability.

8.2 The Research Pathway within the Curriculum

Research capability is built cumulatively rather than assumed. The following courses form a continuous research and project pathway.

Course	Stage	Contribution to research capability
CSC302 – Research Methods in Computing	Year III, Semester I	Literature review, research questions, methodology, ethics, data collection, analysis and academic writing.
CSC210 – Project I	Year II, Semester II	First supervised team project; scoping, planning, implementation and documentation of a bounded computing problem.
CSC310 – Project II	Year III, Semester II	Integrated project of greater technical scope, requiring combination of multiple subject areas.
CSC404 – Capstone Project I	Year IV, Semester I	Independent problem definition, literature grounding, requirements, design and formal proposal defence.
CSC408 – Capstone Project II	Year IV, Semester II	Full implementation, evaluation, written thesis and public oral defence before an academic panel.
CSC409 – Capstone Seminar & Portfolio	Year IV, Semester II	Dissemination, peer critique and consolidation of evidence of professional competence.

8.3 Innovation, Enterprise and Community Engagement

Innovation activity in the department is organized around three channels. The first is the project and capstone sequence itself, which is used as a pipeline for prototypes addressing genuine institutional or community problems rather than artificial exercises. Supervisors are encouraged to source briefs from partner organizations so that student work has an identified beneficiary from the outset.

The second is a set of applied activities that sit alongside the formal curriculum: security and networking interest groups, capture-the-flag and troubleshooting competitions, certification study circles, hackathons and open laboratory time. These build depth and peer learning without additional credit load, and are often where the strongest students first distinguish themselves.

9. Recommended Elective Pool

Electives extend the specialization into areas determined by staff expertise, laboratory capacity, industry demand and emerging technologies. Each elective carries 3 credits and uses the approved LH and PH pattern for its delivery mode.

Secure Systems Administration & Hardening	Cybersecurity Governance, Risk & Compliance
Cloud & DevSecOps Security	Malware Analysis & Cyber Threat Intelligence
Business Continuity & Disaster Recovery	Internet of Things & OT Security
Advanced Digital Forensics	Cyber Threat Hunting
Advanced Network Automation	Wireless Network Security

The elective list is reviewed each academic year. Electives may be added, retired or rotated without structural amendment of the core curriculum, which allows the programme to respond quickly to new threats and technologies.

11. Graduation Requirements

- Successfully complete the 36-credit Foundation Year where applicable.
- Successfully complete all 144 bachelor-level credits, including the required shared-core and specialisation courses.
- Successfully complete the Internship / Professional Practice requirement.
- Successfully complete and defend the Capstone Project.
- Meet the university's minimum cumulative academic standing and all other institutional graduation requirements.