جامعة جميرا
JUMEIRA UNIVERSITY

College of Computer Science

Bachelor of Science in Computer Science

Cybersecurity

AI-Embedded · Triple Certified · CAA Accredited · 100% Internship Guarantee

Defend the Digital World. Lead with Intelligence. Protect What Matters.

Programme Snapshot

120	4	CAA	AI	100%
Credit Hours	Years	Accredited	Embedded	Internship

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Programme Overview

The Bachelor of Science in Computer Science with a Concentration in Cybersecurity at Jumeira University is a rigorous, 120-credit-hour programme that prepares graduates to become the cyber defenders, digital forensics specialists, ethical hackers, and security architects that an increasingly threatened digital world demands. Fully accredited by the Commission for Academic Accreditation (CAA), the programme equips students with both the theoretical foundations and the applied technical competency to protect, investigate, and secure digital infrastructure across the UAE, GCC, and globally.

The programme bridges computer science fundamentals with advanced cybersecurity specialisation — spanning network security, cryptography, cloud security, digital forensics, ethical hacking, and cyber crime law. Students master the technical depth of a computer science degree while building the specialised security expertise that the UAE's most demanding employers require. AI is embedded throughout the learning journey — not as a separate module, but as the lens through which modern security challenges are understood, investigated, and solved.

Upon completion, graduates are positioned for careers as cybersecurity analysts, ethical hackers, digital forensics investigators, and security consultants — with preparation pathways aligned with globally recognised credentials including CompTIA Security+, CEH, ISC2 Certified in Cybersecurity, and more.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Programme Snapshot

Degree	**Bachelor of Science in Computer Science (BSc CS)**
Concentration	**Cybersecurity**
Duration	**4 Years | Full Time / Part Time**
Total Credit Hours	**120**
Accreditation	**Commission for Academic Accreditation (CAA)**
Location	**Latifa Bint Hamdan Street, Exit #24, Al-Khail Street, Dubai, UAE**
Teaching Language	**English**
Admissions	**Enrollment@ju.ac.ae | +971 52 806 3270**

Why Cybersecurity Matters

— The Profession of the Digital Age

Every 39 seconds, a cyberattack occurs somewhere in the world. The UAE and GCC are among the most targeted digital economies on earth. The professionals who stop those attacks are among the most sought-after in the global job market.

We live in a world where every organisation - from hospitals and banks to government agencies and critical infrastructure - depends on digital systems to function. The security of those systems is not a technical afterthought; it is a strategic imperative. The UAE's National Cybersecurity Strategy reflects this reality, positioning cybersecurity as a cornerstone of national resilience, economic stability, and digital sovereignty.

The global cybersecurity talent shortage is projected to reach 3.5 million unfilled positions. In the UAE alone, organisations across financial services, government, healthcare, and technology are competing for qualified cybersecurity professionals who can defend against sophisticated, AI-powered threats. The students who graduate from JU's BSc Cybersecurity programme in 2028 and beyond will enter a market where their skills are structurally in demand — not just locally, but globally.

Four Forces Driving Cybersecurity Demand in the UAE and GCC:

- AI-Powered Cyber Threats: Threat actors are now using AI to automate attacks, bypass traditional security controls, and launch sophisticated phishing, ransomware, and social engineering campaigns at unprecedented scale. Defending against AI-powered threats requires security professionals who understand how AI is being weaponised — and how to deploy it defensively.
- UAE Digital Economy Expansion: UAE's National AI Strategy 2031 and D33 economic agenda are accelerating digital transformation across government, banking, healthcare, and retail — dramatically expanding the attack surface that cybersecurity professionals must defend.
- Regulatory and Compliance Requirements: UAE Cybersecurity Law, NESA controls, ADGM regulations, and DIFC data protection standards are creating significant compliance obligations for organisations — requiring cybersecurity professionals with deep governance, risk, and compliance expertise.
- Cloud Adoption and Hybrid Infrastructure: Rapid migration to cloud environments across UAE organisations is creating complex new security challenges in identity management, data protection, cloud configuration, and Zero Trust architecture — all requiring graduates with current cloud security skills.

The UAE Cybersecurity Landscape

UAE & Regional Context	Significance for Graduates
UAE National Cybersecurity Strategy	Mandatory cybersecurity frameworks across all critical infrastructure sectors — creating structured demand for qualified professionals
Dubai Cyber Security Strategy	Dubai-specific security mandates covering government entities, smart city infrastructure, and digital services — sustained public sector hiring
UAE Cybersecurity Council	National coordination body mandating cyber incident reporting and response — creating demand for incident response professionals
GITEX Global — Dubai HQ	The world's largest tech event, hosted annually in Dubai — direct access to global cybersecurity industry networks and employers
FinTech & Banking Sector Growth	UAE's position as a global financial hub creates persistent demand for financial security, fraud prevention, and regulatory compliance specialists
Critical Infrastructure Protection	Government investment in securing energy, water, transport, and communications infrastructure - creating high-value public sector cybersecurity roles

Programme Objectives & Graduate Attributes

The BSc Computer Science (Cybersecurity) programme is designed to produce graduates who demonstrate technical excellence, professional responsibility, and practical readiness across six dimensions: cybersecurity expertise, AI-enabled security capability, professional ethics, global awareness, research capability, and innovation.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

PLO	Outcome
PLO 1	Technical Proficiency and Problem Solving: Analyse and solve complex problems with appropriate knowledge and understanding of the concepts, principles, and theories in computing.
PLO 2	Design, Implementation, and Evaluation: Design, implement, and evaluate computing-based solutions to meet specific requirements, incorporating principles of sustainability and ethical considerations in the context of cybersecurity.
PLO 3	Effective Communication and Team Collaboration: Communicate effectively in various professional contexts and function as a responsible member or leader of diverse teams, promoting innovative and entrepreneurial solutions in computing projects
PLO 4	Ethics, Professional Responsibility, and Sustainability: Recognise professional responsibilities and make informed judgments in computing practice based on legal, ethical, and sustainability principles, ensuring data privacy and cybersecurity standards are upheld.
PLO 5	Lifelong Learning and Professional Development: Participate in continuous professional development and lifelong learning to keep pace with the rapidly evolving fields in computer science and cybersecurity.
PLO 6	Research, Innovation, and Entrepreneurship: Apply innovative solutions using advanced techniques in computer science to address real-world problems, demonstrate the ability to conduct research, and take individual initiative and enterprise.
PLO 7	Global, Societal, and Environmental Impact: Analyse the local and global environmental impact of computing on individuals, organisations, and society, emphasising the ethical implications, benefits, and its advancements.
PLO 8	AI Development: Develop and implement AI technologies, models and techniques across various domains encompassing the requirements, regulations and ethical practice locally and globally.
PLO 9	Data Analytics Implementation: Demonstrate proficiency in collecting, cleaning, managing, and analysing large datasets and making data-driven decisions in various business contexts.
PLO 10	Cybersecurity Analysis and Design: Illustrate expertise in identifying and analysing threats and risks, design and develop secure systems and networks by ensuring confidentiality, integrity, and authenticity.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Why Study Cybersecurity at Jumeira University?

01

AI-Embedded Cybersecurity Curriculum

Technology-Integrated from Day One

AI is not taught as a separate subject. It is embedded throughout the cybersecurity programme - from AI-powered threat detection in introductory modules to machine learning-based anomaly detection and adversarial AI analysis in advanced studies. Students graduate as cyber professionals who understand both sides of the AI security equation: how AI is being weaponised by attackers, and how it can be deployed defensively.

02

Triple-Certified Graduate Advantage

Degree + Certifications + Industry Projects

JU Cybersecurity graduates earn three categories of credential: the accredited BSc degree, preparation pathways aligned with industry certifications (CompTIA Security+, CEH, ISC2 CC), and verified real-world project experience. This Triple-Certified Graduate Advantage creates an employment profile that significantly outperforms a degree alone.

03

Guaranteed Internship Programme

Every Eligible Student. Real Cybersecurity Experience. Real UAE Employers.

Every eligible student receives an internship placement through JU's industry ecosystem. For cybersecurity students, this means placement in security operations centres, IT governance teams, digital forensics units, or cybersecurity consulting environments — gaining the workplace experience that transforms a qualified graduate into a career-ready professional.

04

Dedicated Cybersecurity Labs & Simulation Environments

Hands-On Security from Day One

Students practise in dedicated cybersecurity lab environments where they conduct ethical hacking exercises, digital forensics investigations, penetration testing, and incident response simulations. The programme's hands-on philosophy means graduates have applied their skills in controlled professional environments long before their first day at work.

05

Dubai Advantage — Cybersecurity Career Gateway

Studying in the UAE's Most Strategically Important Security Environment

Dubai is home to the UAE Cybersecurity Council, GITEX Global, regional headquarters of the world's leading cybersecurity firms, and some of the most sophisticated digital infrastructure on earth. JU students study cybersecurity where it matters most — in the city that is investing most aggressively in protecting its digital future.

جامعة جميرا
JUMEIRA UNIVERSITY

06

Industry-Aligned Curriculum with Global Career Relevance

NESA, UAE Cybersecurity Law, Cloud Security, Digital Forensics

The programme is built around the security frameworks, tools, and methodologies that UAE and global employers actually use — from cloud security architecture and network security management to digital forensics investigation and ethical hacking practice. Graduates arrive workplace-ready.

Future of AI-Powered Cybersecurity

How Artificial Intelligence Is Reshaping Cyber Defence and Attack

Cybersecurity is being transformed by artificial intelligence on both sides of the adversarial relationship. Attackers are deploying AI to automate vulnerability discovery, generate convincing phishing content, bypass biometric authentication, and create polymorphic malware that evades traditional detection. Defenders are deploying AI to detect anomalous behaviour, predict threat patterns, analyse vast security logs in real time, and automate incident response. The cybersecurity professional who does not understand AI — on both sides — is already working at a disadvantage.

How AI Is Being Used in Cyber Attacks

- AI-Generated Phishing & Social Engineering: Large language models are creating hyper-personalised phishing emails, deepfake voice calls, and synthetic identity fraud at a scale and quality that manual methods cannot match.
- Autonomous Vulnerability Scanning: AI-powered tools automatically identify and exploit security weaknesses across complex digital infrastructure faster than human-driven penetration testers.
- Polymorphic Malware: AI enables malware that continuously rewrites its own code to evade signature-based detection — requiring behavioural analysis and anomaly detection rather than traditional pattern matching.
- Adversarial AI Attacks: Attackers can manipulate AI-powered security systems by poisoning training data or crafting inputs that cause AI models to misclassify threats as benign.

How AI Is Being Used in Cyber Defence

- AI-Powered Threat Detection: Machine learning models analyse network traffic, user behaviour, and system logs to identify anomalies that indicate compromise — catching threats that rule-based systems miss.
- Security Information and Event Management (SIEM) Optimisation: AI dramatically reduces alert fatigue by intelligently correlating security events, prioritising genuine threats, and filtering false positives.
- Automated Incident Response: AI-driven security orchestration platforms can automatically isolate compromised systems, block malicious IPs, and initiate forensic data collection within seconds of threat detection.
- Predictive Threat Intelligence: AI models trained on global threat intelligence feeds can predict attack vectors, identify emerging threats, and recommend proactive security hardening before attacks occur.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Domain-Specific AI in Cybersecurity

What JU Students Learn

AI Application	Security Domain	Industry Relevance
AI-Powered Threat Hunting	SOC Operations	Automated detection of advanced persistent threats in enterprise environments
Machine Learning for Anomaly Detection	Network Security	Real-time identification of unusual traffic patterns and insider threats
Natural Language Processing for Phishing Detection	Email Security	AI-driven classification of phishing attempts and social engineering content
AI-Assisted Digital Forensics	Digital Forensics	Automated analysis of large evidence datasets, log files, and memory images
Predictive Vulnerability Management	Risk Management	AI-based prioritisation of vulnerabilities by exploitability and business impact
AI in Cryptographic Systems	Cryptography & Blockchain	Post-quantum cryptography and AI-enhanced encryption strength analysis
Generative AI for Red Team Exercises	Ethical Hacking	AI-augmented penetration testing and adversarial simulation
Behavioural Biometrics	Identity & Access Management	AI-driven continuous authentication using behavioural patterns

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Triple-Certified Graduate Advantage

Three Credentials. Maximum Employability.

The cybersecurity job market is one of the most credential-conscious in technology. Employers benchmark candidates against professional certifications — and candidates who arrive with verified academic credentials, industry certification preparation, and real-world project experience are hired faster, placed in better roles, and command higher starting salaries. JU's BSc Cybersecurity programme is designed to produce exactly this graduate profile.

01

Accredited Academic Degree

Bachelor of Science in Computer Science (Cybersecurity)

The CAA-accredited BSc degree demonstrates academic competence across computer science fundamentals, cybersecurity specialisation, AI applications, research methodology, and professional practice. It is the recognised academic credential that opens professional employment, postgraduate pathways, and higher-level certification registration requirements

02

Industry Certification Preparation Pathways

CompTIA, CEH, ISC2, Cisco, Microsoft, Google — aligned throughout the four-year journey

Students complete structured preparation pathways aligned with the cybersecurity industry's most valued certifications. These pathways are embedded in the curriculum's AI enhancement layer — ensuring students build the knowledge, tool experience, and practical capability that certification examinations require, and that employers verify.

03

Real-World Project Experience & AI-Enhanced Portfolio

Security Lab Projects · Digital Forensics Investigations · Ethical Hacking Assessments · SOC Simulations

Students build a portfolio of professional cybersecurity work across all four years — from network security assessments and cryptographic implementation projects to AI-powered threat detection systems and full-scope ethical hacking engagements. This project portfolio is the most compelling evidence of professional competency a graduate can present to an employer.

Industry Certifications Framework

Preparation Pathways Aligned with Leading Industry Credentials

Important Note

The following certifications represent preparation pathways aligned with leading industry credentials. JU provides structured academic and practical preparation that supports students in pursuing these certifications. Completion of individual certification examinations is the responsibility of each student. Preparation pathways are aligned with leading industry certifications

Cybersecurity Professional Certifications

Certification Option	Focus Area	Year / Stage	Employer Value
ISC2 Certified in Cybersecurity (CC)	Cybersecurity Foundations	Year 1–2	Internationally recognised entry-level credential - ideal first professional certification for cybersecurity students.
CompTIA Security+	Core Security Principles	Year 2	Vendor-neutral baseline security certification - widely required for security roles across UAE private and government sectors.
CompTIA CySA+	Security Analytics	Year 3	Validates threat detection and response capability using security analytics - highly valued in SOC analyst roles.
CompTIA PenTest+	Penetration Testing	Year 3–4	Confirms offensive security and penetration testing capability aligned with the Ethical Hacking concentration course.
EC-Council Certified Ethical Hacker (CEH)	Ethical Hacking	Year 4	One of the most globally recognised offensive security credentials - directly supported by CS 422 Ethical Hacking.
Microsoft Security Fundamentals (SC-900)	Cloud & Identity Security	Year 2–3	Validates foundational Microsoft security, compliance, and identity concepts across cloud environments.
Cisco CyberOps Associate	SOC Operations	Year 3	Prepares for security operations centre analyst roles with a focus on threat detection and monitoring workflows.
Google Cybersecurity Professional Certificate	Applied Security Practice	Year 2	Applied security credential covering Python for security, SIEM tools, and hands-on threat detection exercises.

جامعة جميرا
JUMEIRA UNIVERSITY

AI & Security Certifications

Certification Option	Focus Area	Year / Stage	Employer Value
AI Literacy Certificate Beginner	AI Foundations	**Year 1**	Awarded on completion of Tier 1 AI Literacy Programme — AI fundamentals, ethics, and responsible AI use.
AI Literacy Certificate - Intermediate	Applied AI in Security	**Year 2**	Awarded on completion of Tier 2 — AI tools in security disciplines, prompt engineering for security analysts.
AI Literacy Certificate - Advanced	AI Leadership in Security	**Years 3–4**	Awarded on completion of Tier 3 - AI model design, AI-driven security research, AI governance.
AI for Cybersecurity Certificate	AI-Powered Security Operations	**Year 3**	Validates ability to apply AI tools to threat detection, incident analysis, and security automation workflows.
Security Analytics with AI Certificate	Behavioural Analytics & SIEM	**Year 3**	Demonstrates proficiency in AI-enhanced SIEM optimisation and security log analysis.
Employer Readiness Certification	Full Career Preparation	**Year 4**	Awarded on completion of all employability requirements: internship, bootcamps, and career readiness modules.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Global Industry Projects & Cybersecurity Labs

Real Security Challenges. Real Skills. Professional Portfolio Before Graduation.

JU's BSc Cybersecurity programme embeds real-world security challenges throughout all four years. Students do not learn security theory and then wait to apply it — they practise in dedicated lab environments, work on industry-relevant simulation projects, and engage with real security challenges from their first semester. By graduation, every student has built a professional portfolio of security work that employers can evaluate.

Year 1

Security Foundations & AI Awareness Labs

- Network Security Fundamentals Lab: Hands-on exploration of network protocols, packet analysis using Wireshark, and identification of common network vulnerabilities.
- Introduction to Cybersecurity Tools Workshop: Guided exploration of industry-standard security tools including basic SIEM interfaces, vulnerability scanners, and security monitoring dashboards.
- AI in Cybersecurity Discovery Project: Identifying and critically evaluating three real-world examples of AI being used in cybersecurity — both offensively and defensively.
- Digital Hygiene & Security Awareness Assessment: Conducting a security awareness audit of a simulated organisational environment and presenting remediation recommendations.

Year 2

Applied Security & Threat Analysis Projects

- Network Vulnerability Assessment Project: Using automated scanning tools and manual techniques to identify and document vulnerabilities in a simulated network environment.
- Cryptographic Implementation Lab: Implementing and testing symmetric and asymmetric encryption algorithms — and analysing their strengths and weaknesses against common attack vectors.
- Database Security Audit: Conducting a security review of a simulated relational database environment, identifying injection vulnerabilities and proposing hardening measures.
- AI-Powered Malware Detection Lab: Using machine learning tools to train a basic malware classifier on sample datasets — understanding AI-based detection limitations and capabilities.

Year 3

Advanced Security Operations & Forensics Projects

- Security Operations Centre (SOC) Simulation: A full simulation of an SOC analyst role — monitoring alerts, triaging incidents, using SIEM tools, and producing incident reports for a simulated security event.
- Cloud Security Architecture Assessment: Auditing a simulated cloud environment for misconfigurations, identity and access management weaknesses, and data protection gaps.
- Digital Forensics Investigation: A structured forensic investigation of a simulated cybercrime scenario — evidence collection, chain of custody documentation, forensic analysis, and expert report preparation.
- Penetration Testing Project: Conducting a structured ethical hacking assessment of a simulated target environment — reconnaissance, exploitation, post-exploitation, and professional pentest report.
- AI-Assisted Threat Hunting Lab: Using AI-powered security analytics tools to hunt for indicators of compromise across simulated network traffic and log data.

Year 4

Capstone, Research & Industry Projects

- CS Project (CG 499): A supervised final-year research and implementation project in the student's cybersecurity specialisation area, with compulsory AI integration and structured reflective practice. Projects are assessed by both academic faculty and industry practitioners.
- Global Cybersecurity Consulting Challenge: A capstone simulation in which student teams develop and present a comprehensive security strategy and risk assessment for a real or simulated organisation.
- CS Internship (CG 490): Minimum 12-week placement in a UAE cybersecurity environment — security operations, digital forensics, GRC, or security consulting — applying academic skills in a live professional context.
- Industry Security Symposium: Students present their CS Project findings and security research to an audience of industry professionals and academic assessors.

Future Skills Bootcamps

- Security Tools Fundamentals Bootcamp (Year 1–2): Introduction to Kali Linux, Wireshark, Nmap, and basic SIEM tool navigation.
- Advanced Penetration Testing & Ethical Hacking Bootcamp (Year 3): Hands-on offensive security practice aligned with CompTIA PenTest+ and CEH preparation.
- Cloud Security & Zero Trust Architecture Bootcamp (Year 3): Applied cloud security configuration, identity management, and Zero Trust implementation exercises.
- Career Accelerator Bootcamp: Portfolio, Interview & Professional Presence (Year 4): Cybersecurity CV development, technical interview preparation, certification roadmap planning, and employer engagement.

جامعة جميرا
JUMEIRA UNIVERSITY

Guaranteed Internship Pathway

100% GUARANTEED INTERNSHIP

Every eligible student is provided with internship opportunities through JU's industry ecosystem, ensuring practical cybersecurity workplace exposure prior to graduation.

The CS Internship (CG 490) is a formal 3-credit-hour programme requirement completed after 90 credit hours. Cybersecurity internships provide irreplaceable professional value — the ability to demonstrate that skills learned in academic and lab environments translate to real organisational security contexts.

Benefit	What It Delivers for Cybersecurity Students
SOC & Security Operations Exposure	Understanding how security operations centres function in real organisations — monitoring, triage, escalation, and incident response in live threat environments.
Professional Security Tools Experience	Working with enterprise-grade security platforms, SIEM systems, and vulnerability management tools that laboratory environments cannot fully replicate.
Industry Mentoring & Professional Network	Direct relationships with cybersecurity professionals, SOC leads, forensics specialists, and GRC managers who can become career references and future employers.
Regulatory & Compliance Context	Understanding how UAE cybersecurity regulations, NESA controls, and international frameworks operate in real organisational settings — invaluable for GRC and compliance career pathways.
Employability Documentation	Verified, employer-confirmed professional experience — increasingly decisive in competitive UAE and GCC cybersecurity hiring where practical experience is a primary differentiator.
Career Conversion Pathway	Many students convert internships into direct graduate employment offers, dramatically accelerating the transition from student to qualified security professional.

Cybersecurity Internship Environments

- Security Operations Centres (SOC)
- Government Cybersecurity Agencies
- Financial Services Security Teams
- Digital Forensics Units
- Cloud Security Teams
- Cybersecurity Consulting Firms
- GRC & Compliance Departments
- Telecom & Technology Security
- Critical Infrastructure Protection

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Career Opportunities

Where This Degree Takes You in the UAE, GCC, and Globally

Graduates of JU's BSc Computer Science (Cybersecurity) programme are prepared for a wide and growing spectrum of professional roles across the UAE, GCC, and international markets. Cybersecurity professionals are among the most sought-after in global technology hiring — and graduates who combine academic rigour with practical lab experience, AI literacy, and professional certifications are at a decisive advantage.

	Career Role	Sector	AI-Enhanced Dimension
01	Cybersecurity Analyst	Banking, Government, Technology, Telecom	AI-powered threat monitoring, behavioural analytics, automated alert triage.
02	SOC Analyst	Security Operations Centres, MSPs	AI-enhanced SIEM analysis, machine learning-driven threat prioritisation.
03	Cyber Threat Intelligence Analyst	Government, Defence, Finance	AI-driven threat feed analysis, predictive attack pattern modelling.
04	Incident Response Specialist	Enterprise, Consulting, Government	AI-assisted forensic analysis, automated containment and recovery workflows.
05	Ethical Hacker / Penetration Tester	Consulting, Bug Bounty, Enterprise	AI-augmented reconnaissance, automated exploitation frameworks, AI-generated reports.
06	Digital Forensics Investigator	Law Enforcement, Corporate, Legal	AI-powered evidence analysis, automated artifact extraction from large datasets.
07	Cloud Security Specialist	Technology, Banking, Healthcare	AI-driven cloud misconfiguration detection, automated cloud compliance monitorin
08	Security Consultant	Big Four, Boutique Advisory, Technology	AI-enhanced risk assessment frameworks, intelligent security architecture design.
09	Cyber Risk Analyst	Insurance, Finance, GRC Functions	AI-powered risk scoring models, predictive vulnerability prioritisation.
10	Information Security Officer	Any Sector	AI-supported governance frameworks, automated policy compliance monitoring.

10	Security Auditor	Audit Firms, Government, Banking	AI-assisted audit trail analysis, automated compliance gap reporting
11	Governance & Compliance Specialist	Finance, Government, Healthcare	AI-driven regulatory mapping, automated compliance reporting tools.
12	Cybersecurity Engineer	Technology, Telecom, Critical Infrastructure	AI-enhanced secure system design, automated security testing pipelines.
13	AI Security Specialist	Technology, Banking, Defence	Specialist in AI model security, adversarial attack mitigation, and secure AI deployment.
14	Blockchain Security Analyst	FinTech, Cryptocurrency, DeFi	AI-powered smart contract vulnerability analysis, blockchain forensics.

Graduate Salaries & Market Demand

The Financial Case for a Cybersecurity Career

Cybersecurity is consistently one of the highest-paying entry-level technology disciplines in the UAE and GCC. The combination of talent scarcity and critical importance means that qualified cybersecurity graduates command salaries that outpace most other technology disciplines — and the AI skills premium amplifies this advantage further.

Graduate Starting Salaries — UAE & GCC Cybersecurity Market

AED 10,000–16,000/month	Average Graduate Entry Salary	Cybersecurity roles, Dubai / UAE
AED 18,000–32,000/month	Mid-Career Security Professional	3–5 years experience, UAE
AED 40,000–80,000+/month	CISO / Head of Security / Director	8+ years, GCC market

Salary Benchmarks by Role — Entry Level

Role	UAE Entry Salary (AED/month)	With AI & Cert Premium
Cybersecurity Analyst	AED 9,000–14,000	AED 12,000–18,000
SOC Analyst (Tier 1/2)	AED 9,000–14,000	AED 11,000–17,000
Incident Response Specialist	AED 10,000–16,000	AED 13,000–20,000
Digital Forensics Investigator	AED 10,000–15,000	AED 13,000–19,000
Penetration Tester / Ethical Hacker	AED 12,000–18,000	AED 15,000–24,000
Cloud Security Specialist	AED 12,000–18,000	AED 15,000–24,000
Cyber Risk / GRC Analyst	AED 9,000–14,000	AED 11,000–18,000
AI Security Specialist (Emerging)	AED 15,000–22,000	AED 18,000–30,000

The AI & Certification Premium in Cybersecurity

Cybersecurity professionals with verified AI literacy and industry certifications (CompTIA Security+, CEH, cloud security credentials) consistently command salaries 20–40% above uncertified peers at entry level in the UAE market. JU's triple-certified graduate model is directly translatable to financial advantage from the first day of employment.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Career Progression Pathway

Tier 1

ENTRY LEVEL

- Cybersecurity Analyst · SOC Analyst · Digital Forensics Investigator · Security Support Engineer
- GRC & Compliance Analyst · Junior Penetration Tester · Security Awareness Coordinator

Tier 2

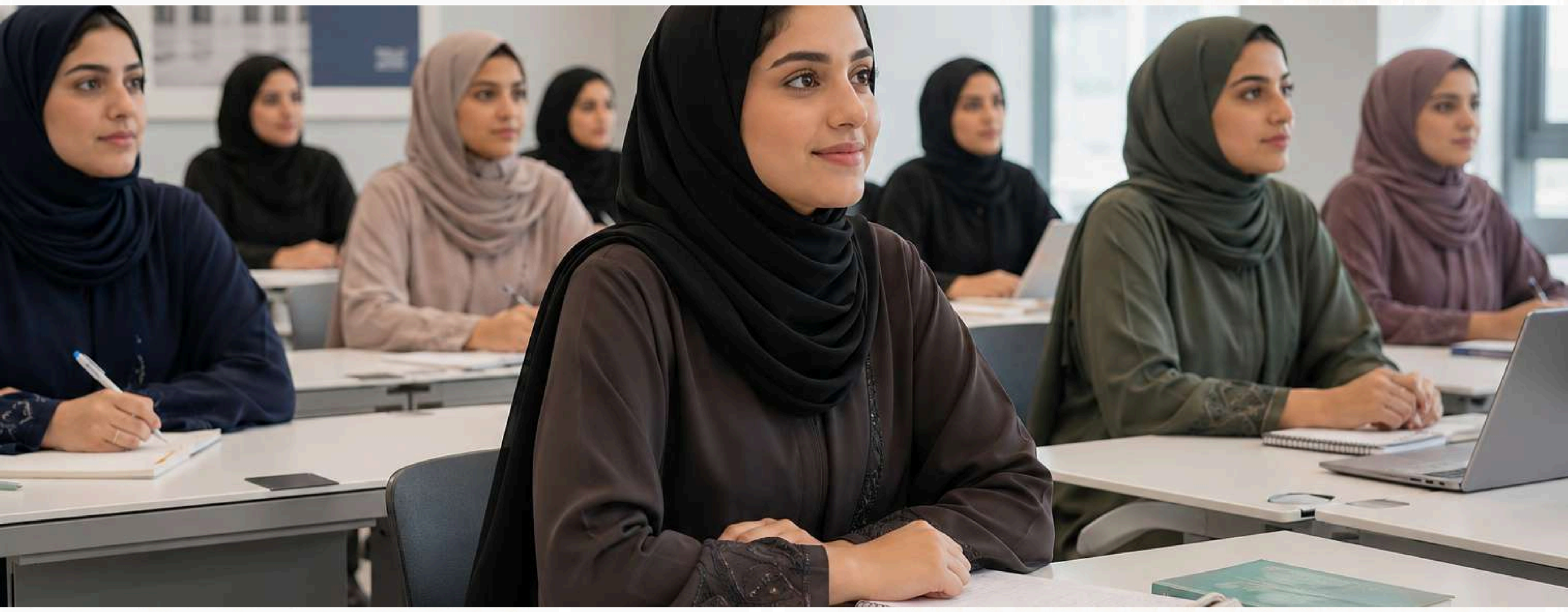
MID LEVEL

- Senior Security Analyst · SOC Lead · Penetration Tester · Cloud Security Engineer
- Threat Intelligence Analyst · Incident Response Manager · Security Consultant

Tier 3

SENIOR LEADER

- Head of Cybersecurity · Chief Information Security Officer (CISO) · Security Director
- VP Security · AI Security Strategist · Digital Transformation Security Lead



جامعة جميرا
JUMEIRA UNIVERSITY

Graduate Employability Advantage

What Makes JU Cybersecurity Graduates Different

A JU BSc Cybersecurity graduate does not enter the job market as merely an academically qualified candidate. They enter as a verified, lab-tested security professional — with documented project experience, AI-validated credentials, certification preparation, internship-backed professional exposure, and a portfolio of cybersecurity work that employers can evaluate directly.

Competency	How JU Develops It	Employer Relevance
Ethical Hacking & Penetration Testing	CS 422 Ethical Hacking, penetration testing lab projects, PenTest+ preparation	Offensive security capability — one of the highest-demand and highest-compensated skill sets in UAE cybersecurity recruitment.
Digital Forensics	CS 421 Digital Forensics, forensic investigation simulations, evidence handling practice	Forensic investigative capability valued by law enforcement, legal teams, and corporate incident response units.
Cloud Security	CS 311 Cloud Security & Privacy, cloud security architecture projects, Microsoft SC-900 preparation	Cloud security is the fastest-growing specialisation in UAE cybersecurity hiring as organisations accelerate cloud migration.
Cryptography & Blockchain	CS 312 Cryptography, CG 409 Blockchain Technologies, cryptographic implementation labs	Deep cryptographic knowledge underpins all security systems — and blockchain security is an emerging high-demand specialisation.
Network Security	CG 301 Information Security, CG 204 Computer Networks, network vulnerability assessment projects	Network security fundamentals are the foundational requirement for every cybersecurity role in every sector.
AI-Powered Security Operations	Three-tier AI Literacy, AI-enhanced SIEM labs, AI threat detection projects	Growing baseline requirement in SOC and security operations roles as organisations deploy AI-powered security platforms.
Cyber Law & Governance	CS 420 Cyber Crime and Law, GRC simulation projects, UAE cybersecurity regulatory context	Legal and regulatory expertise is critical for governance, risk, and compliance roles — and increasingly required in senior security positions.
Research & Project Management	CG 400 Research Methodology, CG 410 Software Project Management, capstone project	Research rigour and project management capability that elevates a security professional from technical contributor to strategic leader.

جامعة جميرا
JUMEIRA UNIVERSITY

Complete Approved Curriculum Structure

120 Credit Hours — Reproduced Exactly as Approved by CAA

Academic Integrity Notice

The following curriculum structure is reproduced exactly as approved by the Commission for Academic Accreditation (CAA). No course names, credit hours, sequences, or prerequisites have been modified. This is the official approved academic structure of the BSc Computer Science (Cybersecurity) programme.

University Requirements (24 Credit Hours)

Core Courses — 18 Credit Hours

Code	Course Title	CH	Requisites
GE 101 / GE 115	Arabic Language Communication 1 or Basic Arabic Language 1	**3**	None
GE 103	English Language Communication 1	**3**	Score 5 in IELTS or equivalent
GE 104	English Language Communication 2	**3**	Score 5 in IELTS or equivalent
GE 125	Fundamentals of Entrepreneurship & Innovation	**3**	Score 5 in IELTS or equivalent
GE 142 / GE 144	UAE Society / مجتمع الإمارات	**3**	Score 5 in IELTS or equivalent /None
GE 142 / GE 144	Islamic Thought / الثقافة الإسلامية	**3**	Score 5 in IELTS or equivalent /None
	Total	**18**	Credit Hours

Elective Courses — 6 Credit Hours

Code	Course Title	CH	Requisites
GE 102 / GE 116	Arabic Language Communication 2 or Basic Arabic Language 2	**3**	None
GE 114	Principles of Research Skills	**3**	Score 5 in IELTS or equivalent
GE 123 / GE 107	Personal Management / الإدارة الذاتية	**3**	Score 5 in IELTS or equivalent / None
GE 131	Critical Thinking	**3**	Score 5 in IELTS or equivalent
GE 145 / GE 140	Islamic Civilization / الحضارة الإسلامية	**3**	Score 5 in IELTS or equivalent /None
GE 148	UAE Economy and Labour Market	**3**	Score 5 in IELTS or equivalent
GE 132	Introduction to Programming	**3**	None
GE 133	Linear Algebra	**3**	None
	Total	**6**	Credit Hours

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

College Requirements — 54 Credit Hours

Core Courses — 45 Credit Hours

Code	Course Title	CH	Requisites
MA 110	Probability and Statistics	**3**	None
CG 200	Digital Logic Design	**3**	None
MA 201	Calculus	**3**	GE 133
MA 202	Discrete Mathematics	**3**	MA 201
CG 203	Fundamentals of Computer Hardware	**3**	CG 200
CG 204	Fundamentals of Computer Networks	**3**	None
CG 205	Fundamentals of Relational Database Management Systems	**3**	GE 132
CG 300	Advanced / Object Oriented Programming	**3**	CG 207
CG 206	Database Administration	**3**	CG 205
CG 207	Introduction to Software Engineering	**3**	CG 205
CG 301	Introduction to Information Security	**3**	CG 204
CG 208	Web Engineering	**3**	GE 132
CG 400	Research Methodology & Project Planning	**3**	CG 207
CG 490	CS Internship	**3**	90 Credits
CG 499	CS Project	**3**	96 Credits
	Total	**9**	Credit Hours

College Elective Courses — 9 Credit Hours (Choose 3)

Code	Course Title	CH	Requisites
CG 401	Scientific Programming	**3**	CG 300
CG 302	Applied Regression Analysis	**3**	MA 110
CG 402	Advanced Data Mining	**3**	CG 205
CG 403	Time Series Analysis	**3**	MA 110
CG 404	Data Visualization	**3**	CG 209
CG 405	Advanced Web Engineering	**3**	CG 208
CG 406	Information Audit and Assurance	**3**	CG 206
CG 407	Risk Management	**3**	CG 305
CG 408	Network Administration	**3**	CG 204
	Total	**09**	Credit Hours

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Programme Requirements — 42 Credit Hours

Core Courses — 33 Credit Hours

Code	Course Title	CH	Requisites
CG 209	Algorithms and Data Structure	**3**	GE 132
CG 303	Operating Systems	**3**	CG 203
CG 409	Block Chain Technologies	**3**	CG 209
CG 304	IoT Concepts and Architecture	**3**	CG 203, CG 204
CG 410	Software Project Management	**3**	CG 207
Concentration	Concentration Courses	**3**	See below
	Total	**33**	Credit Hours

Programme Elective Courses — 9 Credit Hours (Choose 3)

Code	Course Title	CH	Requisites
CG 411	Network Security & Management	**3**	CG 301
CG 412	Programming with Python	**3**	CG 300
CG 413	Software Requirement Specification	**3**	CG 207
CG 305	Mobile & Cloud Computing	**3**	CG 204, CG 303
CG 306	Software Development Process	**3**	CG 207
Concentration	Concentration Courses	**3**	See below
	Total	**9**	Credit Hours

Concentration Courses — 18 Credit Hours

Cybersecurity Core Courses — 18 Credit Hours

Code	Course Title	CH	Requisites
CS 212	Introduction to Cyber Security	**3**	None
CS 311	Cloud Security and Privacy	**3**	CG 301
CS 312	Cryptography	**3**	CG 301
CS 420	Cyber Crime and Law	**3**	CS 311
CS 421	Digital Forensics	**3**	CS 312
CS 422	Ethical Hacking	**3**	CG 301
	Total	**18**	Credit Hours

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Programme Credit Hour Summary

University Requirements: 24 Credit Hours
College Requirements: 54 Credit Hours
Programme Requirements: 42 Credit Hours
Concentration Courses (Cybersecurity): 18 Credit Hours
TOTAL PROGRAMME CREDITS: **120 Credit Hours | Duration: 4 Years | Full Time / Part Time | CAA Accredited**

AI Enhancement Layer — Year-by-Year Map

How This Section Works

The AI Enhancement Layer describes all AI certifications, security labs, industry projects, bootcamps, and career readiness activities that complement the approved curriculum. These activities do not modify or replace any formal academic component — they are the value-added layer through which students build their Triple-Certified Graduate Advantage.

YEAR 1 — Foundations

AI & Security Tools

- Kali Linux basics and security tool landscape awareness
- Network traffic analysis with Wireshark fundamentals
- Basic vulnerability scanner introduction (Nmap, OpenVAS)
- AI in cybersecurity: tools and applications overview

Certifications Aligned

- ISC2 Certified in Cybersecurity (CC) — Preparation Pathway begins
- AI Literacy Certificate — Tier 1 Beginner (AI fundamentals, ethics, responsible use)
- CompTIA IT Fundamentals (ITF+) awareness pathway

Lab Projects & Industry Challenges

- UAE Cybersecurity Landscape Project: Mapping current threats and UAE regulatory frameworks
- Network Security Fundamentals Lab: Protocol analysis and vulnerability identification
- AI in Cybersecurity Discovery Project: Evaluating real-world AI-powered security tools
- Digital Hygiene Audit: Security assessment of a simulated organisational environment

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

YEAR 2 Development

AI & Security Tools

- Wireshark advanced packet analysis for threat detection
- Cryptographic tool implementation (OpenSSL, symmetric/asymmetric encryption)
- Database vulnerability scanning and SQL injection detection
- Introduction to SIEM tool interfaces (Splunk, IBM QRadar awareness)
- AI-powered malware classification using basic ML frameworks

Certifications Aligned

- CompTIA Security+ Preparation Pathway (aligned with CG 301 Information Security)
- AI Literacy Certificate — Tier 2 Intermediate (AI in security disciplines, prompt engineering for analysts)
- Google Cybersecurity Professional Certificate preparation pathway
- Microsoft Security Fundamentals (SC-900) preparation pathway

Lab Projects & Industry Challenges

- Network Vulnerability Assessment Project: Identifying and documenting vulnerabilities in a simulated network
- Cryptographic Implementation Lab: Building and testing encryption solutions
- Database Security Audit: SQL injection testing and hardening recommendations
- AI-Powered Malware Detection Lab: Training a basic ML classifier on malware sample datasets

YEAR 3 Specialisation

AI & Security Tools

- Metasploit Framework for penetration testing exercises
- Digital forensics tools: Autopsy, FTK Imager, Volatility for memory analysis
- Cloud security configuration: AWS/Azure security settings and misconfiguration detection
- SIEM platform analysis: Alert correlation, threat hunting, and incident triage
- AI-assisted threat hunting using behavioural analytics platforms

Certifications Aligned

- CompTIA CySA+ Preparation Pathway (security analytics and threat detection)
- CompTIA PenTest+ Preparation Pathway (aligned with CS 422 Ethical Hacking)
- Cisco CyberOps Associate Preparation Pathway
- AI for Cybersecurity Certificate preparation
- Cloud Security Fundamentals Certificate

Lab Projects & Industry Challenges

- Security Operations Centre (SOC) Simulation: Full incident monitoring, triage, and response exercise
- Cloud Security Architecture Assessment: Auditing a simulated cloud environment for security gaps
- Digital Forensics Investigation: End-to-end forensic investigation of a simulated cyber crime
- Penetration Testing Project: Structured ethical hacking engagement with professional pentest report
- AI-Assisted Threat Hunting Lab: Hunting for indicators of compromise using AI-powered analytics tools

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

YEAR 4
Leadership

AI & Security Tools

- Advanced persistent threat (APT) simulation and analysis
- Blockchain forensics and smart contract vulnerability analysis
- AI adversarial attack simulation and detection exercises
- Zero Trust architecture design and implementation exercises
- CEH-aligned comprehensive ethical hacking methodology application

Certifications Aligned

- EC-Council Certified Ethical Hacker (CEH) Preparation Programme
- AI Literacy Certificate — Tier 3 Advanced (AI model design, AI-driven security research, AI governance)
- Decision Intelligence & Responsible AI Certificate
- Employer Readiness Certification (internship + bootcamps + career readiness)

Lab Projects & Industry Challenges

- CS Project (CG 499): Supervised final-year research with compulsory AI integration and Gibbs Reflective Framework
- Global Cybersecurity Consulting Challenge: Develop and present a comprehensive security strategy for a real or simulated organisation
- CS Internship (CG 490): 12-week cybersecurity workplace placement in a UAE-based organisation
- Industry Security Symposium: Present CS Project findings to industry professionals and academic assessors
- Career Accelerator Bootcamp: Portfolio development, technical interview preparation, certification roadmap planning

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Graduate Success Pathway & Long-Term Career Sustainability

A Career in Cybersecurity That Grows as Threats Grow

Cybersecurity is one of the most career-resilient degree pathways available in technology education. Unlike disciplines where demand fluctuates with market cycles, cybersecurity demand is driven by the continuous expansion of digital infrastructure and the relentless evolution of cyber threats. As long as there is digital technology — which is to say, indefinitely — there will be critical demand for the professionals who protect it.

Why Cybersecurity Careers Are Structurally Secure

- Structural Talent Shortage: The global cybersecurity workforce gap is expected to remain above 3 million unfilled positions for the foreseeable future — ensuring demand significantly outpaces supply for the career lifetimes of current students.
- AI Creates More Security Work, Not Less: Every AI system introduced into an organisation creates new security requirements — protecting training data, securing AI model inference pipelines, governing AI outputs, and defending against AI-powered attacks. AI growth is a catalyst for security employment, not a threat to it.
- Regulatory Expansion: UAE cybersecurity regulation, EU NIS2 Directive, Saudi PDPL, and international frameworks are mandating higher security standards across more organisations — creating sustained compliance-driven demand for qualified professionals.
- Cross-Sector and Cross-Geographic Mobility: A qualified cybersecurity professional can work across healthcare, finance, government, technology, and consulting — and across the UAE, GCC, UK, Singapore, and beyond. Few career paths offer equivalent flexibility.

Graduate Value Proposition

A Jumeira University BSc Computer Science (Cybersecurity) graduate enters the workforce with:

1. A fully accredited BSc degree in Computer Science — CAA-accredited, Jumeira University Dubai
2. Preparation pathways aligned with industry certifications: ISC2 CC, CompTIA Security+, CompTIA CySA+, CEH, Cisco CyberOps
3. Three-tier AI Literacy Certification (Beginner, Intermediate, Advanced)
4. Verified security lab project experience across all four years of study
5. Guaranteed internship experience in a UAE-based cybersecurity environment — documented and employer-verified
6. An Employer Readiness Certification confirming full career preparation
7. A starting salary benchmark of AED 10,000–16,000/month and a 10-year earnings potential of AED 3M–6M+

This is not just a degree. It is a comprehensive cybersecurity career launch platform.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Testimonials

Aisha Al Marri

BSc in Cybersecurity

Studying Cybersecurity at Jumeira University has helped me understand how digital systems are protected in the real world. Through practical labs, security simulations, and industry-focused learning, I gained the confidence to analyse threats, secure networks, and build strong problem-solving skills for my future career in cybersecurity.

Salama Al Dhaheri

BSc in Cybersecurity

The Cybersecurity programme gave me more than technical knowledge. It helped me develop critical thinking, ethical hacking skills, and a strong understanding of data protection. The supportive faculty and hands-on learning environment made every module engaging and relevant to today's digital world.

Maryam Al Suwaidi,

BSc in Cybersecurity

What I appreciate most about Jumeira University is how the Cybersecurity programme connects classroom learning with real-world security challenges. From network defence to risk management, every course strengthened my understanding of cyber threats and inspired me to build a career that protects people, organisations, and digital systems.

جـــامعة جـــميرا
JUMEIRA UNIVERSITY

Ready to Become the Next Generation Cybersecurity Leader?

The digital world needs defenders. The UAE needs cybersecurity leaders. Your career protecting what matters most begins at Jumeira University.

- **AI-Embedded Learning**
- **Triple Certified Degree**
- **CIPD-Aligned Curriculum**
- **100% Guaranteed Internship**
- **Real-Time Global Project Experience**
- **Industry Certifications**
- **Dubai-Based Education**
- **Global Career Prospects**

In four years, you could be the analyst who stops a ransomware attack before it encrypts a hospital's patient records.
The ethical hacker who finds the vulnerability before the attacker does. The CISO who builds the security strategy that protects an entire organisation.

That career begins at Jumeira University.

Apply Now

Website:
www.ju.ac.ae

E-mail:
enrollment@ju.ac.ae

General Inquiries:
+971 4 515 4555

Landline
+971 (0) 515 4561
+971 (0) 515 4558
Admission Inquiries:
+971 52 806 3270
+971 52 806 3723

Scan to Apply

Scan to Apply

Scan to Connect

The Professions University: Where Your Future Takes Flight