



Diploma in Cybersecurity (DCY500)

**FACT
SHEET**

Welcome to CIAFS

Diploma in Cybersecurity

The Diploma in Cybersecurity is CIAFS's flagship cybersecurity credential, designed for serious security professionals targeting senior specialist and management roles. The 18-course curriculum extends beyond core security into the adjacent disciplines that define modern cybersecurity work: cyber threat intelligence, cybersecurity risk management, IoT security, secure software development, and the application of artificial intelligence and data science to security problems.

Students complete substantial project work in threat intelligence, secure software engineering, cyber risk assessment, and AI-applied-to-cyber, building a portfolio that demonstrates senior-level capability to employers. The curriculum reflects the convergence of security with software engineering and data science that defines the next generation of cyber roles.



Modules

* Prescribed textbooks, must be obtained by students at their own cost prior to the commencement of their studies

Module Codes	Description	Credits	Semester
DCY501	Cybersecurity Risk Management	3	1
DCY502	Cyber Threat Intelligence	3	1
DCY503	Cloud Computing	3	1
DCY504	Wireless Communications for IoT	3	2
DCY505	IoT Security	3	2
DCY506	IoT Networks and Protocols	3	2
DCY507	Cybersecurity and AI-Based Software Development	3	3
DCY508	Secure Software Development	3	3
DCY509	Software Requirements and Specifications	3	3
DCY510	Database Systems in Software Engineering	3	4
DCY511	Software Metrics and Models	3	4
DCY512	Data Ethics and Privacy	3	4
DCY513	Predictive Analytics	3	5
DCY514	Time Series Analysis	3	5
DCY515	AI Ethics and Policy	3	5
DCY516	Reinforcement Learning	3	6
DCY517	Computer Vision	3	6
DCY518	Knowledge Representation and Reasoning	3	6



Assessment

- Continuous assessment (assignments, projects, and quizzes)
- Summative assessment (tests and examinations)
- No practical or workplace-based component

Outcomes

Upon completion of the qualification, graduates will be able to:

- Lead enterprise cybersecurity risk assessment programs and produce executive-level risk reports.
- Operate a cyber threat intelligence capability including collection, analysis, and dissemination.
- Design and audit secure software development lifecycles for high-stakes applications.
- Architect IoT security solutions across embedded devices, wireless networks, and cloud platforms.
- Apply machine learning, predictive analytics, and computer vision techniques to cybersecurity problems.
- Develop and apply ethical, privacy, and regulatory frameworks to cybersecurity decision-making.

Admission Requirements

- US High School Diploma, GED, or international equivalent (NQF Level 4 or higher)
- Recognition of Prior Learning (RPL) in line with CIAFS institutional policy
- English language proficiency: IELTS 5.5, TOEFL iBT 60, or equivalent for non-native English speakers
- Mature applicants (21+) with relevant work experience welcomed via portfolio review

Purpose of the Qualification

To provide students with:

- Deliver senior specialist competence across the converging disciplines that define modern cybersecurity.
- Build the AI-and-data-applied-to-security skill set that distinguishes next-generation security professionals.
- Prepare graduates for CISSP, CISM, and CCSP certifications alongside the academic credential.
- Open a direct articulation path into bachelor's degree completion programs in cybersecurity.



Articulation Options

Graduates can articulate horizontally or vertically into:

- Bachelor of Science in Cybersecurity (final-year completion)
- Bachelor of Science in Information Assurance
- Bachelor of Science in Computer Science with security concentration

Career Opportunities

Diploma in Cybersecurity

Graduates may pursue roles such as:

- Cybersecurity Manager
- Cyber Threat Intelligence Analyst
- Secure Software Engineer
- IoT Security Specialist
- Cyber Risk Analyst