

Higher Certificate in Cybersecurity (HCCY500)

**FACT
SHEET**

Welcome to CIAFS

Higher Certificate in Cybersecurity

The Higher Certificate in Cybersecurity opens the door to one of the fastest-growing and best-paid technology disciplines in the United States and globally. Through six foundational courses, students develop the technical literacy and security mindset employers need from entry-level security professionals, with a strong grounding in the computer science fundamentals that underpin all cyber work.

Designed for career changers, IT support staff seeking to specialize, military veterans entering civilian technology careers, and recent graduates, this qualification covers cybersecurity principles, cybersecurity frameworks, operating systems, computer networks, the discrete mathematics that underpins cryptography and algorithms, and the data structures used in defensive and offensive security tooling.

Graduates are positioned for Security Operations Center analyst roles, junior security engineer positions, and IT security support.



Modules



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

Module Codes	Description	Credits	Semester
HCCY501	Cybersecurity Principles	3	1
HCCY502	Cybersecurity Fundamentals and Frameworks	3	1
HCCY503	Operating Systems	3	1
HCCY504	Computer Networks	3	2
HCCY505	Discrete Mathematics for Computer Science	3	2
HCCY506	Data Structures and Algorithms	3	2



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:

- Explain core cybersecurity concepts including confidentiality, integrity, availability, and the threat landscape.
- Apply industry frameworks including NIST CSF, ISO 27001, and the CIS Critical Security Controls to organizational contexts.
- Analyze operating system internals to identify and mitigate common security vulnerabilities.
- Reason about network protocols, network design, and common network-layer attacks and defenses.
- Apply discrete mathematics and algorithmic thinking to security problems and cryptographic foundations.
- Communicate security findings, risks, and recommendations clearly to non-technical stakeholders.

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:

- Provide the technical foundations and security mindset employers expect from entry-level cyber professionals.
- Align with the NICE Cybersecurity Workforce Framework so graduates can speak the language employers use.
- Prepare students to pursue CompTIA Security+, the gateway industry certification, in parallel with study.
- Open progression to the Advanced Certificate in Cybersecurity for offensive and defensive specialization.



Articulation Options

Graduates can articulate horizontally or vertically into:

- Advanced Higher Certificate in Cybersecurity
- Certificate in Computer Science (cross-track entry)
- Associate degree programs in Cybersecurity or Information Assurance

Career Opportunities

Higher Certificate in Cybersecurity

Graduates may pursue roles such as:

- Security Operations Center (SOC) Analyst Tier 1
- Junior Cybersecurity Analyst
- IT Security Support Specialist
- Junior Security Engineer
- Information Security Assistant