

Advanced Diploma in Cybersecurity

NQF Level 7 | 120 Credits | Advanced Diploma

Value Proposition: Specialised. Practical. Industry-aligned.

The Advanced Diploma in Cybersecurity equips you with the specialised skills to identify, analyse and counter modern cybersecurity threats across software, networks, systems and organisational environments. The qualification is an engaging, high-quality learning experience that builds practical capability and opens clear pathways into further postgraduate study.

Qualification Overview

The Advanced Diploma in Cybersecurity builds on your previous IT studies and equips you with the specialised skills needed to identify, analyse and respond to cybersecurity threats across software, networks, systems and organisational environments. Designed for those who want to deepen their capability in a fast-growing field, the programme develops both technical and organisational cybersecurity competence and allows you to specialise in either Secure Electronic Communication Networks or Secure Software Development. Delivered fully online through scheduled live sessions, the programme offers consistent academic quality, practical learning, and direct access to expert lecturers to prepare you for workplace contribution and further study.

Delivered fully online through scheduled, live late-afternoon sessions, the programme provides structured, real-time engagement with expert lecturers across campuses and international locations. This model ensures consistent academic quality, practical learning and direct access to specialist knowledge - preparing you for workplace contribution and further postgraduate study.

Programme Structure and Components

The qualification comprises 120 credits, structured across a combination of core modules and a specialist stream.

- **Core modules (75 credits):** All students complete a common set of compulsory core modules that provide foundational cybersecurity knowledge and skills.
- **Specialist stream (45 credits):** Students select one specialist stream. All modules within the chosen stream are compulsory



Core Modules

- **Principles of Project Research 581 (PRP581)** — 15 Credits
- **Introduction to Cyber Security 581 (ICB581)** — 10 Credits
- **Ethics in Cyber Security 581 (ECB581)** — 20 Credits (Prerequisites: PRP581 & ICB581)
- **Secure Project 581 (SPP581)** — 30 Credits (Prerequisites: PRP581 & ICB581)

Specialist Streams

Stream 1: Secure Electronic Communication Networks Stream

(Prerequisites: PRP581 and ICB581)

- **Network Development and Management 581 (NDM581)** — 15 credits
- **Secure Networking 581 (SCM581)** — 15 credits
- **Cloud Security 581 (CSC581)** — 15 credit

Stream 2: Secure Software Development Stream

(Prerequisites: PRP581 and ICB581)

- **Architectural Principles of Secure Software 581 (APS581)** — 15 credits
- **Secure Software Strategy and Practices 581 (SSP581)** — 15 credits
- **Data Security 581 (DSC581)** — 15 credits

Applied and Research-Oriented Learning

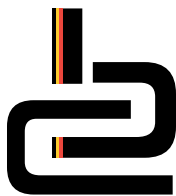
The Advanced Diploma in Cybersecurity builds focused, practical capability through applied learning, real-world projects and industry-aligned practice, offering specialisation in secure networking or secure software development while developing analytical and problem-solving skills and providing a clear pathway into postgraduate study.

Key Features

- A structured, applied learning approach combining theory with practical cybersecurity implementation.
- Strong alignment with current and emerging cybersecurity practices and technologies.
- Opportunity to engage with real-world cybersecurity challenges through applied projects and case-based learning.
- Development of analytical, technical and problem-solving capability in software and network security environments.
- Specialisation through dedicated streams in secure networking or secure software development.
- A clear progression pathway into postgraduate study in cybersecurity and related ICT fields.

Integrated Approach to Applied Learning and Industry Engagement

The programme blends applied inquiry, technical development and industry engagement to ensure practical, relevant learning, with students using real or simulated environments, current cybersecurity tools and frameworks, and completing an applied project often linked to workplace contexts and supported by hands-on laboratory experimentation.



Key elements include:

- Practical application within real or simulated cybersecurity environments.
- Alignment with current industry practices, tools and frameworks.
- Development of analytical thinking and solution-focused problem-solving.
- Applied projects aligned to workplace or organisational contexts.
- Opportunities to address real cybersecurity risks, vulnerabilities or system requirements.
- Hands-on experimentation, simulation and testing in the cybersecurity laboratory.

Industry Engagement

The programme is supported by structured engagement with industry to ensure continued relevance and alignment with evolving cybersecurity demands.

This may include:

- Exposure to real-world case studies and scenarios
- Engagement with industry practices, standards and tools
- Participation in masterclasses, guest sessions, or roundtable discussions with industry practitioners

This integrated approach reflects Belgium Campus iTiversity's focus on quality, applied learning and meaningful industry engagement, ensuring that graduates are prepared to contribute effectively within cybersecurity environments.

Cybersecurity Laboratory Environment

Students benefit from a dedicated cybersecurity laboratory that provides practical, hands-on learning through real-world threat simulation, experimentation and applied skills development. This environment ensures strong alignment with industry expectations and prepares students for practical application in professional cybersecurity settings.

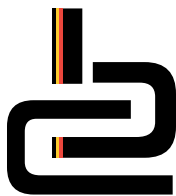
The lab enables:

- Simulation of real-world cyber threats and attack scenarios.
- Practical testing of security tools, frameworks and techniques.
- Safe environments for experimentation, analysis and response.
- Development of applied skills in both network and software security contexts.

What Makes This Programme Different

The programme is designed to deliver focused, relevant and applied cybersecurity capability through the following distinguishing features:

- **Specialised stream options:** Students deepen their expertise through either the Secure Electronic Communication Networks stream or the Secure Software Development stream.
- **Applied cybersecurity focus:** Learning is oriented toward identifying, articulating and countering complex cybersecurity attacks in real organisational environments.
- **Balanced technical and organisational capability:** The programme addresses software, networks, cloud, risk, ethics and human factors as part of a modern cybersecurity skill set.



- **Preparation for further study:** The qualification develops the research foundation needed for articulation into postgraduate diploma or honours study in cybersecurity and related ICT fields.
- **Industry-aligned design:** The programme reflects current cybersecurity demands and prepares graduates to contribute effectively from early in their careers.

What You Will Develop

Through this programme, graduates will develop the knowledge, skills and professional capability required to operate effectively within cybersecurity environments and contribute to organisational resilience. Graduates will develop:

- The ability to collect, interpret and manage cybersecurity-related information across organisational contexts.
- Knowledge literacy in evaluating threats, risks and countermeasures.
- Analytical and problem-solving capability in software and network security environments.
- The ability to communicate cybersecurity concepts and recommendations effectively to different stakeholders.
- Ethical and professional judgement in cybersecurity practice.
- Responsibility and accountability in implementing and supporting security measures.

Who Should Apply and Career Outcomes

This qualification is suited to learners who have completed prior study in information technology and want to specialise in cybersecurity. It is especially relevant for those seeking to enter or strengthen their position in technical and applied cybersecurity roles.

On completion, graduates are equipped to contribute across a range of cybersecurity functions and may pursue roles such as:

- **Cybersecurity Analyst.**
- **Network Security Analyst.**
- **Security Software Developer.**
- **IT Security Specialist.**
- **Cybersecurity Technician.**
- **Risk and Compliance Support Practitioner**

Further Study Opportunities

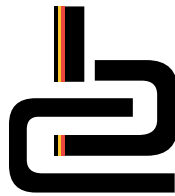
On completion of this qualification, graduates may articulate into a Postgraduate Diploma in Cybersecurity Risk Management or related ICT qualifications, subject to admission requirements. This forms part of a structured pathway toward advanced specialisation and postgraduate study as offered by Belgium Campus iTiversity.

Why Study This Qualification

This programme is designed to build focused, in-demand capability in cybersecurity while supporting both immediate employability and future progression.

Key reasons to consider this qualification include:

- Develop specialised skills in a high-demand and evolving field.
- Build expertise in either secure networking or secure software development.
- Strengthen both technical capability and applied problem-solving skills.



- Develop a foundation for further postgraduate study.
- Prepare for roles that support organisational resilience and digital security.
- Gain a qualification aligned to industry needs and national skills priorities.

Admission Requirements

To be considered for admission into the Advanced Diploma in Cybersecurity, applicants must hold a relevant NQF Level 6 qualification in the field of Information Technology.

This includes:

- A 360-credit Diploma, or
- A 240-credit Diploma together with completed work-integrated learning, or a combination of work-integrated learning and coursework equivalent to 120 credits, or
- A Bachelor's degree in the Information Technology field

Examples of relevant qualifications include:

- **Diploma in Computer Networking**
- **Diploma in Information Technology**
- **Diploma in Information and Communications Technology in Communication Networks**
- **Diploma in Information Technology in Network Management**

Admission is subject to alignment between the applicant's prior learning and the technical requirements of the programme.

Recognition of Prior Learning (RPL)

Belgium Campus iTversity recognises that applicants may have acquired relevant knowledge and skills through formal, informal, or work-based learning. In line with the policy framework of the South African Qualifications Authority (SAQA) and quality assurance requirements of the Council on Higher Education (CHE), Recognition of Prior Learning (RPL) may be applied in the following ways:

RPL for Access (Admission Equivalence)

Applicants who do not meet the formal NQF Level 6 entry requirements may be considered for admission based on demonstrated equivalence. This process evaluates whether the applicant's prior learning, professional experience and competencies are comparable to the expected outcomes of a relevant NQF Level 6 qualification in Information Technology.

Applicants will be required to submit a portfolio of evidence, which may include:

- Academic records and prior learning achievements
- Relevant professional or workplace experience
- Evidence of technical capability in IT or cybersecurity-related areas
- A motivation outlining readiness for further study

Admission through RPL for access is granted only where sufficient evidence demonstrates the applicant's ability to succeed in a specialised, applied learning environment.

RPL for Credit (Advanced Standing)

In line with SAQA and institutional guidelines, a maximum of 50% of the total credits for the qualification may be awarded through RPL, where applicable and academically justifiable.

RPL for credit may be considered where prior learning demonstrates clear alignment and content overlap with specific modules within the programme. This is typically limited to structured modules where equivalence in learning outcomes can be demonstrated.

Given the integrated and applied nature of the qualification:

- Credit recognition is evaluated on a module-by-module basis
- Exemptions are granted only where there is sufficient evidence of depth and relevance
- The Secure Project module must be completed in full to meet the qualification's exit level outcomes

Assessment Process

All RPL applications are subject to a structured academic review process, which includes:

- Formal evaluation of the submitted portfolio of evidence
- Assessment of alignment with programme learning outcomes and academic standards
- Review and approval by the relevant institutional academic structures

Admission through RPL is limited in accordance with institutional policy.

Application Process

Applications are submitted through the Belgium Campus iTiversity online application portal. Applicants are required to submit standard admission documentation, together with additional supporting information to assess academic readiness and alignment with the programme.

Stream Selection

As part of the application process, applicants are required to indicate their preferred specialist stream. This supports planning and cohort formation. Final stream allocation is confirmed based on enrolment patterns and cohort viability, while taking student preference into consideration.

Note: The availability of each specialist stream is subject to a minimum cohort size (typically 10 students) to ensure a high-quality learning experience. Where necessary, stream offerings will be confirmed based on demand and students may be guided toward the stream with sufficient enrolment.

Standard Documentation

Applicants must submit:

- A certified copy of identification documentation
- A certified copy of full academic records

Standard Documentation

To support admission decisions, applicants may be required to provide:

- A brief motivation outlining their interest in cybersecurity and readiness for further study
- Evidence of relevant technical knowledge, skills, or work experience (where applicable)
- For applicants applying through Recognition of Prior Learning (RPL), a portfolio of evidence will be required in line with the RPL process.

Selection Considerations

Admission is based on:

- Academic eligibility and prior qualifications
- Alignment between the applicant's background and the technical requirements of the programme
- Demonstrated readiness to engage with specialised cybersecurity content
- Where applicable, RPL applications are evaluated through a structured academic process in line with institutional policy.

Programme Enquiries

For further information or academic enquiries regarding the Advanced Diploma in Cybersecurity, please contact:

Mr Francois Smit

Head of Department: Networking & Cybersecurity

Belgium Campus iTiversity

smit.f@belgiumcampus.ac.za