

Cyber Security Technical Professional

About the programme:

The Cyber Security Technical Professional Integrated Degree Apprenticeship at De Montfort University (DMU) provides the technical skills and knowledge to ensure that learners can become competent and independent cyber security professionals. Individuals will be able to operate within business, technology or engineering functions across a range of sectors including critical national infrastructure such as energy, transport, water, and finance.

Integrating on-the-job practical training with academic learning provides graduates with an increased understanding of their organisation's unique business needs.

Apprentices will develop skills which will enable them to lead teams that research, analyse, model and assess cyber risks, and design, develop, justify, manage and operate secure solutions, detecting and responding to incidents.

This programme is aligned to the Level 6 Cyber Security Technical Professional (Integrated Degree) apprenticeship standard, and is allocated Funding Band 27 (£24,000) by the Education and Skills Funding Agency. Note that the price of the course is currently £27,000 so an employer contribution may be required.

Who is this apprenticeship suitable for?

Typical job roles include: Cyber Risk Manager, Cyber Risk Analyst, Cyber Research Analyst, Cyber Incident Manager, Cyber Security Engineer and Cyber Security Design Engineer.

What are the entry requirements?

All applicants need to be employed by an organisation in a role that provides them with the experience and exposure to a range of relevant business areas. This will ensure that apprentices can complete all elements as required by the apprenticeship standard.

Each applicant will be individually assessed on their eligibility, qualifications and work experience.

What level qualification will be achieved?

BSc (Hons) Cyber Security Technical Professional Degree.

What is the duration of the apprenticeship?

The programme duration is 3.5 years.

What modules will be studied?

Core skills

Technical competencies: foundations of cyber security and its significance, concepts, threats, vulnerabilities and assurance, risk modeling, analysis and assessment strategies, cyber incident response tools and techniques, secure software development, malware analysis, and understanding of the applicable laws, regulations, standards and ethics.

Indicative Content

This programme has been developed to provide learners with the skills and knowledge necessary to operate as cyber security professionals. It starts by providing a solid baseline of computer systems before introducing more complex elements of cyber security, directly informed by research from DMU. Topics covered include but are not limited to:

Computer Law and Ethics	Computer Programming	Operating Systems and Architecture	Database design and Implementation
Cyber Threat Intelligence and Incident Response	Penetration Testing	Embedded Systems	Linux Security
Web application Penetration Testing	Industrial Control System Security	Emerging Topics in Cyber Security	Final Year Project

What is the delivery model?

Learners will be taught in blocks of one week at a time, each block comprising four days of teaching followed by one day of revision. There will also be pre and post block support.

Block mode teaching allows the potential for greater use of new pedagogic practices and presents the opportunity to truly immerse the apprentices within a scenario.

How is the apprenticeship assessed?

The apprentices will undertake a range of assessments at the end of their academic modules. Apprentices must also create a portfolio which will capture the knowledge and skills developed through the programme and in the workplace. They will complete a work-based project in their final year which will bring together their accumulated knowledge. The portfolio and project will contribute towards the apprentice's End Point Assessment for the apprenticeship standard.

Discover, Develop, Deliver.

