

# SECTION 3: PROGRAMME DESIGN and PHILOSOPHY

## How Will My Knowledge, Understanding & Skills Develop?

This Section provides information about the nature of the learning students can expect to engage with on this programme and the pedagogic considerations underpinning these. Please write this section in the first person, addressing your (prospective) students.

| Part A: Enhancement Framework |
| --- |
| Learning and Teaching Methods |
| The programme has been designed to meet the required criteria for certification by the NCSC. Teaching and Learning ApproachTeaching and learning will take place in both the workplace and the institution. There are two parallel major strands of learning in the apprenticeship degree. One is for knowledge, mainly achieved in the institution, and the other is for competence, mainly achieved in the workplace. However, the programme design has to cross reference and link the two in order to take advantage of progress in each. The approach taken is to include practical activities in the knowledge sessions that match a planned sequence of competencies in the workplace. In the standard each knowledge component has a complementary competence component. As the criteria are covered in the knowledge modules, then classroom practical activities will show the apprentices how knowledge is applied. They can then take this understanding into the workplace and apply it, thereby building a sequence of evidence which demonstrates the required competence. As an example, networking (a year 1 module) has a knowledge component of network foundations, connections, internetworking, protocols, standards, performance, security and server virtualisation. The complementary competency component requires the apprentice to design, build, configure, optimise, test and troubleshoot simple and complex networks. In the module there will be a lecture on the fundamental building blocks, followed by a practical on interconnecting the devices to form a simple network. An assessment component could require the apprentice to map and report on the network in use at their workplace. In subsequent years the apprentice would be expected to design and build the complex network in the workplace. This would then tie into the year 2 module on the Embedded Systems Security where the apprentice would have to apply networking knowledge along with threat and risk knowledge from year 1 to research and analyse the impact of embedded systems on a network. The progression is of an increasing command of the specialised skills along with growing self-reliance and accountability. Throughout the programme various teaching methods will be used: Lectures to impart core knowledge Experiential learning in practical sessions Reflective learning in reports Group work and group discussions about workplace experience and practice Case studies from the apprentices’ workplaces Development of a portfolio of evidence of competence Student presentations The focus throughout will be on enquiry-based learning, where apprentices are set real world tasks. Employers will be required to establish development plans for the apprentices that match the required competencies. Apprentices will be visited once a month by an assessor to review, advise, support and provide feedback on the body of evidence. This will ensure satisfactory progress. In End Point Assessment module, the apprentice will apply the total range of acquired knowledge, competencies, skills and behaviours to complete between six and eight real work projects or pieces of work. This portfolio, along with the completion of all prior modules will enable the apprentice to enter and complete the end point assessment.Content progression and coherenceThe essential learning progression is as follows:Year 1: Establish a clear, detailed understanding of the components of IT systems and the cyber threats to themYear 2: Develop the responses to the threats and the underlying techniques employedYear 3: Use the knowledge and skills gained to complete a significant project using professional practice and processesEnd of year 3: Complete workplace projects and build a portfolio of evidence for use in the EPA interviewThe complexity of the assessment tasks at each level reflects these very broad foci. for example, in year one tasks are well-contained, individual examples relevant to the topics covered, in year two tasks are synthesised across topic areas, in year three students tackled more complicated, open-ended tasks.This is described in much more detail in a document available on CMT under the "Document" tab.Scholarly and enquiry basedApprentices will be required to research academic sources for contemporary knowledge on the topics in the modules. They will then take this into the workplace and investigate how it applies to their employer’s particular practice. Areas of special interest will be where the experience and knowledge gained in the block release sessions can be applied to practical problem solving. Inclusive and internationalIndividual employers will set the selection criteria for the apprentices (subject to UWE entry requirement) and normal discrimination legislation will apply. The apprenticeship will appeal to students completing level 3 qualifications and mature applicants who wish to retrain.The apprenticeship funding will allow applicants, who may not wish to incur debt, to achieve a higher qualification.As the apprentices are employed in the cybersecurity industry there are many opportunities for them to bring their experiences into the block release sessions. This will enrich the learning and encourage discussion and debate. It is unlikely that there will be international applicants for this apprenticeship as the apprentices will have to be employed relatively locally and have a general work visa (tier 2) or other right to employment in the UKGraduate attribute enablingThe apprenticeship standard has fifteen specific learning outcomes covering professional, interpersonal, business skills and behaviours. These will be developed and evidenced as part of their development in employment. They are also assessed in year 2 and 3 modules.Many of the employers in cybersecurity have national and international customers and apprentices will have exposure to these. |
| Assessment Strategy (c. 400 words) |
| As described above, throughout this programme students are assessed through a series of real world, employment-related tasks.Assessments will require apprentices to use their own organisations as examples and case studies for discussion and reflection.They will be able to: apply the methods and techniques that they have learned to review, consolidate, extend and apply their knowledge and understanding, and to initiate and carry out projects, both in the third year and at work for their EPA portfolio. critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete), to make judgements, and to frame appropriate questions to achieve a solution - or identify a range of solutions - to problems in the workplace. communicate information, ideas, problems and solutions to both specialist and non-specialist audiencesSkills attitudes and behaviours will be developed and demonstrated in the workplace and also incorporated in the knowledge sessions. Assessment strategies will require apprentices to showcase their achievement of these. |
| Student Support and Special Features of the Programme |
| Students on this programme will have access to the full support facilities at both Gloucestershire College and UWE. Both institutions provide a student support service to help students make the most of their study time. Student services are able to answer questions about the courses, the facilities and to signpost to other specialist support for health and well-being. Student services also offer financial advice and provide access to financial assistance. In addition to general student services, Gloucestershire College provides training co-ordinators who support the student in the workplace . Naturally, members of the academic team are available during published office hours and during teaching time to provide direct support with specific academic issues. A UWE link tutor is also available to liaise between the University, College and employer to ensure that the students have an integrated educational experience. In addition to all of this, an assessor from Gloucestershire College will visit the students once a month at their workplace. The purpose of this visit is to review the student’s academic and workplace competency progress, offer support and provide feedback on achievements so far.  Students on this programme have a unique opportunity to pursue an integrated degree at the end of which they will have both a higher education qualification and three years of cutting edge cyber security work experience. Where appropriate, teaching and learning will take place in block-release mode in Gloucestershire College’s brand new cyber rooms as well as within the workplace. Students will have access to specialist facilities both at Gloucester College and UWE. These include an isolation room in which they can explore and experiment with malware, other suspect software and specialist, industry-standard software. They will be taught by expert staff from both Gloucestershire College and UWE. |

|  |
| --- |
| Part B: Assessment Map |
| |  |  |  |  | | --- | --- | --- | --- | | Module number: Short name | Brief outline of assessment type(s) to create a map of assessments across the programme and where relevant indicate using (T) if they require timetabling and invigilation by CETTS. | Assessment weighting % | UWE Week | |  |  |  |  | | Year 1 |  |  |  | |  |  |  |  | | UFCFFU-30-1 Cyber Threats 2020-21 |  |  |  | | UFCFDU-30-1 Networking 2020-21 |  |  |  | | UFCFCU-30-1 Operating Systems and Architecture 2020-21 |  |  |  | | UFCFEU-30-1 Programming 2020-21 |  |  |  | | Year 2 |  |  |  | |  |  |  |  | | UFCFGU-30-2 Cryptography 2021-22 |  |  |  | | UFCFJU-30-2 Embedded Systems Security 2021-22 |  |  |  | | UFCFKU-30-2 Information management and security 2021-22 |  |  |  | | UFCFHU-30-2 Operating Systems Security and Defensive Programming 2021-22 |  |  |  | | Year 3 |  |  |  | |  |  |  |  | | UFCFNU-20-3 Cyber Security Incident Management and Professionalism 2022-23 |  |  |  | | UFCFBU-10-3 End Point Assessment (Cyber Security) 2022-23 |  |  |  | | UFCFPU-30-3 Project and Dissertation 2022-23 |  |  |  | | UFCFMU-30-3 Risk and Information Management 2022-23 |  |  |  | | UFCFLU-30-3 Security Assurance 2022-23 |  |  |  | |