Programme Specification for FdSc in Cyber Security

1.	**Awarding institution/body**	University of Worcester
2.	**Teaching institution**	Heart of Worcestershire College
3.	**Programme accredited by**	n/a
4.	**Final award**	FdSc
5.	**Programme title**	FdSc in Cyber Security
6.	**Pathways available and/or Linked Honours Degree progression route/s**	• BSc (Hons) in Computing • BSc (Hons) in Cyber Security (subject to approval and demand)
7.	**Mode and/or site of delivery**	Taught modules at Heart of Worcestershire College with some teaching to take place in the National Cyber Skills Centre in Malvern
8.	**Mode of attendance**	Full-time; part-time
9.	**UCAS Code**	
10.	**Subject Benchmark statement and/or professional body statement**	• eSkills Cyber Security Higher Apprenticeship Skills and Learning Framework (eSkills); • IISP Information Security Skills Framework, 2010 (IISP); • QAA Computing Benchmark Statement, 2007 (QAA); • QAA Foundation Degree Qualification Benchmark, 2010 (FDQB) • BCS IT Skills Framework (SFIAplus) (SFIA)
11.	**Date of Programme Specification preparation/ revision**	March 2014; August and October 2014 – amendment to regulations. Correction to module code COMP2370 and change to TCRF by AQU October 2016.

12. Educational aims of the programme

The FdSc in Cyber Security is a programme designed around the needs of individuals who are either currently working, or wish to start a career, in the cyber and information security sector, who:

- wish to develop or consolidate their professional skills;
- aspire to increase knowledge of change in the sector and so improve their career development prospects;
- have, or aspire to have, some management responsibilities;

- wish to complete a full University of Worcester undergraduate degree on completion of the FdSc.

The programme focuses on applied learning, and so allows students to develop an understanding of how cyber security fits into the wider world of business and commerce. In particular, the aims of the programme are to provide students with:

1. the theory and practice of cyber security, including an extensive appreciation of the importance of computer system and network infrastructure design, program code, webpage and database design to secure information (eSkills, QAA);
2. professional practical and technical skills in developing security solutions using a wide range of computer technology (eSkills, QAA);
3. an appreciation of the professional, psychological, social and ethical issues associated with computing and cyber security (eSkills, QAA);
4. the basis for further professional development, and encouragement to take responsibility for their own CPD and those for whom they are responsible (QAA);
5. the opportunity to build significant interpersonal and communication skills, particularly in relation to team working where the team members possess a wide range of skills (QAA);
6. progression opportunities to other programmes such as the existing University of Worcester BSc (Hons) in Computing and the proposed University of Worcester BSc (Hons) in Cyber Security programme.

13. Intended learning outcomes and learning, teaching and assessment methods

On successful completion of the course, students will be able to apply understanding and skills in a vocational and academic context. They will be able to demonstrate skills in the following four categories: (i) knowledge and understanding; (ii) cognitive abilities and skills related to intellectual tasks; (iii) practical skills related to the discipline of Cyber Security and (iv) transferable skills which may be learned within the context of Cyber Security, but may be deployed in other areas.

Knowledge and Understanding	**Examples of learning, teaching and assessment methods used**
On successful completion of the course, students will be able to: 1. appreciate the fundamental concepts of why information and cyber security is important to business and society, the role of legislation and standards, and the key social, legal and ethical issues encountered when securing access to data (eSkills, IISP); 2. recognise the threats and risk to information security and the measures needed to protect access to data and ensure business continuity (eSkills, IISP); 3. understand the fundamental concepts of computer hardware, software and data network design, how data is stored on a computer, network protocols and the range of techniques used to secure	• All modules contain varied approaches to learning, teaching and assessment designed to encourage students to progress as individuals within their capabilities, and to achieve a qualification; • Assessment is by a variety of means including essays, oral presentations, group work, practical work and research-driven tasks; • Tutor support is deployed to assist students’ progression towards achieving a broad but deep understanding of the field of Cyber Security, to motivate students and to provide different learning approaches; • Formal lectures, which encourage student interaction and discussion; interactive materials available on VLE;

and protect access to data stored on computers and transmitted via networks (eSkills, IISP, QAA); 4. appreciate the different views of the future and trends in technology, explaining what this might mean for business and commerce (eSKills, IISP).	• Practical workshops, which encourage students to apply their theoretical learning to a practical situation; • Electronic submission of coursework through the VLE and electronic feedback from the assessor for easier student access.

Cognitive and Intellectual Skills	**Examples of learning, teaching and assessment methods used**
On successful completion of the course, students will be able to: 1. reason methodically and evaluate the strengths and weaknesses of such reasoning (QAA, IISP); 2. apply their knowledge and understanding in the design of secure systems (QAA); 3. recognise and analyse criteria and specifications appropriate to specific problems, and plan strategies for their solution (QAA); 4. analyse the extent to which a system meets the criteria defined for its current use and future development (QAA); 5. integrate theory and practice using appropriate techniques to communicate reasoning as well as synthesise and critically evaluate solutions to novel problems (QAA, IISP).	• Student activities including individual and group exercise, the use of guided worksheets and direct input into sessions; • Students are encouraged to engage in peer-support through both informal contacts (through the use of email for example) and formal discussion groups on the VLE; • Students and tutors are encouraged to make use of the VLE to incorporate collaborative learning; • It is the norm for modules to assess theory and practice in some combination; • Inclusion of peer assessment in formative feedback to encourage students to review each other's work before final submission.

Practical Skills Relevant to Employment	**Examples of learning, teaching and assessment methods used**
On successful completion of the course, students will be able to: 1. use a range of hardware and software tools to design, develop and test security solutions to protect access to information and data (eSkills, QAA); 2. evaluate systems in terms of general quality and possible trade-offs presented within the given problem (QAA); 3. demonstrate practical skills acquired without work carried out in labs, workshops or the workplace in individual and/or group work (eSkills, QAA);	• Use of computer applications is found in most modules – specific examples include the use of project management tools in the Security Project module, network simulation software in the network fundamentals and network security modules and software development software in the programming and coding modules; • Some modules will also provide basic preparation for professional vendor certification exams, such as Cisco ICND and CCNA Security; • Students are encouraged to gain practical skills in most modules, and by engaging in work placement throughout the programme.

4. set up, test and administer systems for effective use (eSkills); 5. research and investigate common attack techniques and make recommendations on how to defend against them (eSkills).	

Transferable Skills	**Examples of learning, teaching and assessment methods used**
On successful completion of the course, students will be able to: 1. use information retrieval skills, gathering and evaluating different types of information (QAA); 2. make effective use of ICT for project management, communication and collaboration; 3. demonstrate the ability to work independently and as part of a team (QAA); 4. demonstrate numeracy and literacy skills in presenting cases (QAA); 5. manage their own learning and development, including time management and organisational skills (QAA); 6. identify problems, develop and document solutions (QAA).	• Students have the opportunity to learn a variety of methods for online retrieval and research from Internet sources (in the Professional Development module) and are encouraged to incorporate this directly into assignments for all modules; • Several modules involve formal group work including assessment (for example the mandatory Computer Fundamentals module); • Management of individual learning is achieved through structured tutor support in learning activities, through meeting assignment deadlines and through the planning and production of the Security project; • Personal Development is introduced in the induction period, and developed through the mandatory Professional Development module; • The Induction process aims to introduce students to several aspects of learning and study - (i) Time Management related to assignment hand-in dates, (ii) The nature of learning, including concepts of multiple intelligences, levels of learning, experiential and collaborative learning approaches.

A matrix mapping the Programme Learning Outcomes developed and assessed by each Module is contained within the Course Handbook, in Appendix 1 (Module Mapping to Programme Outcomes).

In general, cognitive skills are acquired via lecture and practical laboratory exercises, directed private study, and debates and discussions in tutorials. These skills are assessed by assignments, work based evidence and practical laboratory reports. Level 4 consists of mostly tutor-led learning and Level 5 consists of both tutor-led and student-led learning. At each level, there is team-work in the laboratory, in tutorials, and in some assignment work. Independent learning is encouraged by the addition of support material available in digital form. ICT skills are embedded across the course.

Modules at all levels emphasise the skills of communication, organisation and presentation, and these are supported by workshops on electronic information retrieval and reinforced within the Professional Development module and tutorial sessions. Students have opportunities to participate in either group or individual presentations. A matrix mapping the transferable skills supported in each module is contained within the Course Handbook, in Appendix 7 (Module Mapping to Transferable Skills).

All students on the course are assigned a Personal Tutor, who guides the student's completion of their Personal Development Plan and offers general support and guidance. (NB - the guidance and support is formally timetabled. Preparation of a Personal Development Plan is a feature in COMP2372 which runs throughout the duration of the entire programme and is timetabled with tutorial and classroom based sessions; and the progress file generated in that module provides the framework for subsequent tutorial discussion and action). Throughout the programme the designated tutor will offer students individual and plenary sessions, covering both academic and pastoral areas. In this way the team seek to avoid a 'problem-driven' approach to personal tutorship in which support is triggered only by a student identifying and communicating a 'problem' to the tutor. The team therefore recognise that the nature of this foundation degree requires close, personalised and continuous monitoring and exchange. Remote web-based tutorial support will be a key element for all students across all attendance modes.

The content of the course is firmly centred on the workplace, either in terms of continued employment through the programme or participation in work placements at regular intervals throughout the course. Therefore, it is expected that students subsequently draw upon and share their practical experience in the classroom. Successful completion of some assessment pieces will require research and activity to take place in the classroom and the workplace and the co-operation of the employer, or another appropriate individual at work will also be required. A 'Work Based Learning' handbook is to be circulated to all students and employers in which their suggested responsibilities are clearly set out.

14. Assessment Strategy

The assessment strategies are designed to enable students to demonstrate their achievement of the course aims and outcomes. As such they are intended to develop and assess the knowledge and skills relevant to practitioners in the cyber security industry. A mapping of assessment methods against modules appears in the Course Handbook, in Appendix 2 (Assessment Methods and Weightings).

Assessments on the programme are, where possible, work-based or work-related. Students are encouraged to use examples from work placements where possible. Where assessments cannot utilise work-based content, a case study/simulation approach is used.

Therefore, as with the Learning and Teaching strategy, outlined above, the assessment strategy has been designed to provide students with a variety of challenges appropriate for undergraduate level work and appropriate to the IT and cyber security context of the qualification. Assessment is constructed in such a way that a student's knowledge and understanding of each module studied during the course is assessed.

The Foundation Degree is aimed at giving students the practical skills they need in order to gain employment in the cyber security industry. As such, the focus of assessments is on the student demonstrating a practical ability. Consequently the majority of modules are assessed by report, practical skills-based exercise and oral presentations as these reflect the skills most needed by employers. For Level 4 modules, oral presentations may be to a smaller audience to allow a student to gain in confidence at presenting, before being expected to present to a much larger group during Level 5.

Formative assessment on the programme works in three ways. Firstly because undertaking any assessment is in itself a learning experience, feedback on any item of assessment is therefore diagnostic, positive and formative for future work and is intended to guide and motivate the student towards higher levels of achievement. Assessment has therefore been devised to ensure that feedback on performance is given at a time and in a way that is useful to the student as he/she prepares for the next assessment. Individual feedback is supplemented by group debriefings. Exemplar materials are also provided on the VLE and students are encouraged to evaluate these materials. Secondly, learning outcomes are achieved through assessments that recognise the benefits to the student of formative assessment – students submit written responses to tasks that allow them to assess their knowledge and understanding of a topic, receive feedback on presentation rehearsals; do mock practical assessments, undertake reflective accounts of their learning. Thirdly the teaching and learning strategy recognises the need to develop transferable skills. In-class case studies are used to develop skills in analysis and synthesis by transferring learning from one context and applying it to another.

Students are required to complete much assessed work on an individual basis. However, at this level, students are also actively encouraged to discuss their understanding of models, concepts and theories, and more importantly their application to a given scenario, with other members of their teaching group. This allows students to share ideas and experiences, test their understanding, and more critically, evaluate the models under discussion. In this way students learn from each other, develop relationships from the workplace that will help them through the rest of their studies and engage in the 'lived experience' of managing peers.

Assessment items are scheduled so that they can be completed on an ongoing basis throughout the year. Detailed assessment briefs are given to students at the start of a module and are published to the VLE (Moodle). Students are encouraged to access and submit all assessments electronically. Staff then download and edit the submitted document and re-upload the edited document to Moodle; there is a feature on Moodle to allow this to happen anonymously.

Full attendance will normally be expected. It is the nature of the programme however that work commitments may over-ride attendance on occasions. If students cannot attend a class for unavoidable reasons, they should inform the module tutor of their non-attendance in advance so that alternative arrangements for the delivery of material, or additional support tutorials can be organised. In every circumstance students are expected to meet agreed submission deadlines and will be expected to make full use of the VLE to assure timely submission of work. In cases of non / late submission UW procedures will apply.

In marking assessed work, Internal Verification and Moderation form part of the quality assurance procedure. Assessed work will be subject to University of Worcester Business School procedures. The University of Worcester designated Link Tutor is also given full access to these materials and asked to comment formally through UoW channels and also informally on an ongoing basis. Where there is some doubt as to the authorship of an assessment, the programme will follow the University of Worcester published policy for investigating plagiarism.

In line with the University of Worcester Assessment Policy, assessments for the individual modules have been designed to enable students to demonstrate that they have successfully met the learning outcomes. Each module outline thus specifies an assessment strategy outlining the nature of the summative assessment exercises it employs and the respective weighting of each assessment item in its overall assessment loading. If students fail to achieve a learning outcome University of Worcester procedures as to resits apply. The course complies with the University's anonymous marking requirements as articulated in the UW Assessment Policy.

A grid showing assessment methods and weightings mapped to modules at each level, together with an assessment calendar of submission dates is included in the Course Handbook, in Appendix 3 (Assessment Calendar)

15. Programme and requirements

Students who complete the programme and accumulate 240 credits are eligible for the award of FdSc in Cyber Security. These students may either progress to the final year of the University of Worcester's BSc (Hons) in Computing or the proposed BSc (Hons) in Cyber Security programmes (the latter being subject to final University approval and sufficient demand).

There are two general attendance modes available. Students can study full-time (two taught days per week with independent learning outside this time) or part-time (one taught day per week with some independent learning outside scheduled classes). For full-time students the nine modules that make up the Foundation Degree are completed within the standard university two-year calendar. Part-time students are generally expected to complete within three years. The Course Handbook contains a full calendar (Appendix 3) and module sequence (Appendix 8).

Students studying full-time would sit the four Level 4 modules during Year 1, concurrently, followed by the three mandatory Level 5 modules and optional Level 5 modules totalling a further 45 credits during Year 2. Module COMP2372 requires full-time students to undertake a minimum of four two-week placements (two each year), with the course calendar being designed to give four opportunities each year for this to happen. These placements may be with the same employer, or may be with different employers, depending on individual circumstance. More details on work placements can be found in the Work Based Learning Handbooks (Student and Employer editions).

Students studying part-time would sit the four Level 4 modules over two years (two being sat each year) – it is normally expected that modules COMP1371 and COMP1373 would be studied in year 1, with COMP1372 and COMP1374 coming in the second year. They would then complete the core module COMP2373 plus optional Level 5 modules totalling a further 45 credits in Year 3. Modules COMP2370 and COMP2372 would be completed through a combination of independent study and work-based study; and would be formally assessed in their third year.

The Award Map is included at the end of the document here.

The Level 5 option modules will only run subject to demand in any given year. It is generally expected that students will study the mandatory modules, and then pick a major specialism (either Protecting Web Applications or Network Security), topping up their required credits with one of the 15 credit modules.

16. QAA and Professional Academic Standards and Quality

This foundation degree is written in line with a number of standards, namely QAA Foundation Degree Qualification Benchmark, 2010, QAA Computing Benchmark Statement, 2007, eSkills UK's Cyber Security Higher Apprenticeship Framework and IISP Information Security Skills Framework.

In line with the QAA Foundation Degree Qualification, Benchmark, the Foundation Degree is at Level 5 of the Framework for Higher Education Qualifications in England, Wales and Northern Ireland (FHEQ) and as such is recognised as an award that would be generally equivalent to Level 5 within the Qualifications and Curriculum Framework (QCF), and aims to support students to:

- Develop an understanding of the well-established principles of cyber security and the way in which these have developed;
- Develop analytical techniques and problem-solving skills that can be applied in many types of employment;
- Effectively communicate information, arguments and analysis in a variety of forms to specialist and non-specialist audiences, and deploy key techniques effectively;
- Develop the qualities needed for employment including the exercise of personal responsibility and decision-making.

Work based learning forms an integral part of this foundation degree (as specified by the QAA Foundation Degree Qualification Benchmark, *paragraphs 20 and 23*). The Professional Development module assesses the student's skills in the workplace, although work placements occur throughout the programme. The work based element of the programme allows for students to be either employed for the entire (or part of the) duration of the programme in a directly relevant role to cyber security, or to undertake regular work placements through the programme. In line with the FDQB Benchmark, employers taking on either employed students or placement students would be expected to be involved in the formative assessment of the student's progress in the work place (*Paragraph 25*).

The programme aims and learning outcomes are also written to map to the eSkills UK Cyber Security Higher Apprenticeship *(as suggested by the QAA Foundation Degree Qualification Benchmark, para 16*) and the IISP Information Security Skills Frameworks, and to take account of the QAA Computing Benchmark Statements. A mapping of the programme outcomes to these can be found in the Course Handbook, in Appendix 5 (Module Mapping to eSkills Cyber Security Framework), Appendix 6 (Module Mapping to IISP Framework) and Appendix 4 (Module Mapping to QAA Computer Benchmark Statements).

17. Support for students

The following support services are in place at HOW to provide support for students on the programme:

- an induction programme including inputs from HOW Student Services as well as course staff;
- course handbook and module outlines;
- support from HOW Study Centre staff during induction and subsequently at St Andrew's Study Centre;
- representation on Course Team Committee to address course-wide issues and offer feedback (from students on all modes);
- an assigned personal tutor to provide academic and pastoral support as required;
- a work-place nominated manager to provide work-based support for work placements;
- access to Moodle (HOW VLE) and ProMonitor (HOW online gradebook);
- HOW Equal Opportunities Unit implements codes of practice in relation to disability, racial and other forms of discrimination;
- HOW Student Services provide advice and support for students who have mental health difficulties, dyslexia, sensory or physical impairments and other difficulties;
- Student and academic support, representation and social networking via the Student's Union.

18. Admissions

Admissions Policy

Both the University (UoW) and the College (HOW) aim to be accessible. They are committed to widening participation and encouraging diversity in the student population. Worcester Business

School (at UoW) and the Department of Computing (at HOW) work closely with central services including the Admissions Office, the Equal Opportunities Centre and the International Centre to support students from a variety of different backgrounds. We actively encourage and welcome people from the widest range of economic and cultural backgrounds and value the contribution of mature learners*.*

Entry requirements

The general admissions requirement of this programme are:

- The University's standard minimum entry requirements apply: 4 GCSEs (Grade C or above) plus a minimum of 2 and maximum of 3½ A Levels or equivalent Level 3 qualifications. . See UW Admissions Policy for other acceptable qualifications. The current UCAS Tariff requirements for entry to the course are published in the HOW prospectus.

- The programme welcomes applications from learners who feel they may benefit, from outside the UCAS tariff, and actively encourages and welcomes people from the widest range of economic and cultural backgrounds, in work or directly from full-time study. In particular the programme values the contribution of mature learners.

Recognition of Prior Learning

Details of acceptable level 3 qualifications, policy in relation to mature students or applicants with few or no formal qualifications can be found in the prospectus or on the University webpages. Information on eligibility for recognition of prior learning for the purposes of entry or advanced standing is also available from the University webpages or from the Registry Admissions Office (01905 855111).

Admissions procedures

The University encourages applicants to attend visit days and also a selection interview is normally required.

Full-time applicants apply through UCAS:
Part-time applicants apply directly to Heart of Worcestershire College (HOW).

Admissions/selection criteria

The selection interview will comprise: a site visit of the relevant HOW facilities (where appropriate); an online knowledge and skills aptitude test; an informational talk by a member of the course teaching team and a formal interview with the Course Admissions Tutor, or member of the course teaching team.

The Course Admissions Tutor will gather evidence from the application (including the reference), the aptitude test and the formal interview and make a decision about the offer of a place based on the results.

Where an applicant has met (or is predicted to meet) the entry requirements, and has satisfied the Course Admissions Tutor that they are at the appropriate stage in their development to benefit from the programme, then an offer will be made.

See also Section 22 of the Programme Specification for information regarding the admissions arrangements for progression to the linked Honours Degree(s)/Top-Up Degree(s).

19. Methods for evaluating and improving the quality and standards of teaching and learning

University of Worcester and Heart of Worcestershire College policies on the evaluation and improvement of teaching and learning apply to this qualification. Mechanisms for review and evaluation of teaching, learning, assessment, the curriculum and outcome standards, include:

- module feedback at the mid-point (of a 30 credit module) and at the end (of every) module (completed online using Moodle);
- the annual Course Evaluation Report is completed by the course manager;
- QAA Reviews;
- peer teaching observation;
- External Examiners' reports
- academic staff annual appraisal (based on peer teaching observation);
- feedback from workplace managers;
- Link Tutor reports;
- questionnaires to employers.

Mechanisms for gaining student feedback on the quality of teaching and their learning experience include:

- module feedback at the end of the module (completed online using Moodle);
- student representatives meet with the course team at course team committee meetings;
- student meetings with personal tutor;
- on-line tutorial support systems;
- participation in the external National Students Survey.

20. Regulation of assessment

The course operates under the University's Taught Courses Regulatory Framework

Requirements to pass modules

- Modules are assessed using a variety of assessment activities which are detailed in module specifications.
- The minimum pass mark is D- for each module.
- Students are required to submit all items of assessment in order to pass a module, and in some modules, a pass mark in each item of assessment may be required.
- Full details of the assessment requirements for a module, including the assessment criteria, are published in the module outline.

Submission of assessment items

- Students who submit course work late but within 5 days of the due date will have work marked, but the grade will be capped at D- unless an application for mitigating circumstances is accepted.
- Students who submit work later than 5 days but within 14 days of the due date will not have work marked unless they have submitted a valid claim of mitigating circumstances.
- For full details of submission regulations see Taught Courses Regulatory Framework.

Retrieval of failure

- Students are entitled to resit failed assessment items for any module that is awarded a fail grade, unless the failure was due to non-attendance.
- Reassessment items that are passed are graded at D-.

- If a student is unsuccessful in the reassessment, they have the right to retake the module (or, in some circumstances, take an alternative module).

Requirements for Progression

- Students at Level 4 may be permitted to progress to Level 5 when they have passed at least 90 credits at Level 4.
- A student who fails 90 credits or more due to non-submission will be required to withdraw from the University.
- Students who pass less than 90 credits but have submitted all items of assessment will be required to retake modules.

Requirements for Awards

Award	**Requirement**
Certificate of Higher Education in Cyber Security (CertHE)	120 credits at Level 4 or higher
Foundation Degree in Cyber Security (FdSc)	120 credits at Level 4 and 120 credits at Level 5

These awards are not classified.

21. Indicators of quality and standards

The University underwent a QAA Institutional Audit in March 2011. The audit confirmed that confidence can be placed in the soundness of the institution’s current and likely future management of the academic standards of its awards and the quality of the learning opportunities available to students. The audit team highlighted several aspects of good practice, including the student academic representative (StARs) initiative, the proactive approach which supports the student experience for disabled students, the comprehensiveness of the student online environment (SOLE), the wide range of opportunities afforded to students to enhance their employability, the institution’s commitment to enhancement, and the inclusive approach to working with its collaborative partners.

Heart of Worcestershire College underwent a QAA / IQER Institutional Review of its HE provision in January 2012. In expressing confidence in the College’s performance, the following aspects of good practice were recognised:

- the thorough and robust monitoring and action planning arrangements assure standards
- and the quality of learning experiences within the higher education provision of the College
- the provision of an integrated system of support addresses the needs of all higher
- education students
- the many opportunities provided by employers enable students to acquire and demonstrate
- work-related skills and enhance their employability
- there are multiple opportunities for students to provide feedback and the College has
- developed innovative ways to facilitate feedback for the benefit of all students (IQER, 2012).

Staff development at Heart of Worcestershire College is actively encouraged and supported with teaching staff undertaking regular development in both aspects of teaching and learning and in their subject specific areas. Continuing professional staff development is central to the success of the programmes and comprises opportunities such as: in-house and external activities, formal professional qualifications, work experience/external visits, team meetings or cross-college groups for awareness raising, specific skill training and sharing and dissemination of information, mentoring/ coaching/deputising, undertaking projects and representing the department/section in the wider community.

The Foundation Degree in Cyber Security is a new qualification, and as such, previous indicators do not exist. The course will be delivered within the Higher Education Computing team, and the following indicators apply to existing HE Computing qualifications offered at HOW:

- NSS Scores for 2013-14:
    - Quality of Teaching is good: 94% of students agreed;
    - Quality of assessment & feedback is good: 87% of students agreed;
    - Quality of academic support is good: 98% of students agreed;
    - Organisation and management of the course is good: 87% of students agreed;
    - Learning resources are good: 93% of students agreed;
    - The course helped personal development: 100% of students agreed;
    - Overall satisfaction of the course: 95%.

- Students leaving the HND course in 2013:
    - in related employment: 55%;
    - progressed to further study: 25%.

- External Examiner Report in June 2013
    - very positive, with no actions for the following academic year. Report stated that "*There is a high degree of programme co-ordination that ensures that students are well supported throughout their learning experience."*

22. Graduate destinations, employability and links with employers

Graduate destinations

The foundation degree has been developed in conjunction with local employers from the cyber security industry. It also has the backing of the Worcestershire Local Enterprise Partnership (WLEP). The local Cyber Security Consortium have stated their intent to work with the course team to provide work placement opportunities for students on the course and career paths and job opportunities post-graduation.

Progression to Linked Honours Degree(s)/Top-Up Degree(s)

Students who complete the programme and accumulate 240 credits are eligible for the award of FdSc in Cyber Security. These students may either progress to the final year of the University of Worcester's BSc (Hons) in Computing or the proposed BSc (Hons) in Cyber Security programmes (the latter being subject to final University approval and sufficient demand). Students progressing to the top-up degree programme will receive advice from the BSc (Hons) Admissions Tutor on module choices, Integrated Project preparation and a bespoke induction/academic development programme on entry to the top-up degree.

Student employability

This foundation degree is underpinned by employability skills. The Professional Development module requires students to create a career development plan, and to undertake activities and studies to work towards stated goals. Students are encouraged to undertake placements in a variety of different sectors within the IT and security industries to widen their portfolio of skills and experience. Transferable skills are taught within the Professional Development module, but reinforced throughout every module (students will be expected to work collaboratively on group work, deliver presentations to peers, assessors and employers throughout). The use of guest speakers and visiting lecturers from within the industry will further reinforce links with industry and the skills required to enter the world of work.

Some teaching will be located in the state-of-the-art and nationally-acclaimed Malvern Hills Science Park ‘Dirty Lab’, which will allow students access to dedicated, specialist facilities to test their work for the hacking and defence modules, and a further purpose-built training facility funded by Worcestershire County Council at the Malvern Hills Science Park (where many of the Cyber Security cluster companies are based). This will reinforce the links with industry and local employers.

The HOW Employability Skills Framework underpins the delivery of all modules. Examples of employability skills in action are:

- Managing Self - organising workloads, time management and attendance, responding to external stimuli and modifying actions accordingly, meeting assignment deadlines, being open to feedback on skills and development.

- Working with Others - working in teams to deliver results, managing others in group activities, reflecting on own team working practice.

- Problem Solving & Decision Making - case studies, critical incident analysis, debates, completion of a work-based management project or dissertation.

- Communication & Literacy Skills - writing reports, presenting orally in groups and individually, debates on ethical issues, negotiating and persuading others in class discussions and in writing.

- IT & Information Literacy - using software to present your work (eg word processing, spreadsheets and presentation software), using online resources for research

- Critical Thinking Skills - developing, evaluating and justifying original arguments. Evaluating published research and referencing the work of others.

At the end of the award, students are also presented with a transcript stating the modules completed and the grades achieved. This enables prospective employers to see clearly the subjects that have been studied and the level of attainment by the student. This transcript may be provided as a supplement to employment applications or CVs, as well as a focus for discussions at interview to demonstrate student employability.

Award Map – Full Time Route

Course Title: Foundation Degree in Cyber Security (Full Time)	

Level 4					
Code	**Title**	**Credits**	**Mandatory or Option**	**Pre-requisites**	**Exclusions**
COMP1371	Computing & Networking Fundamentals	30	M	-	-
COMP1372	Software Development & Data Vulnerabilities	30	M	-	-
COMP1373	Foundations of Cyber Security & Information Assurance	30	M	-	-
COMP1374	Web, HCI & Emerging Technologies	30	M	-	-

Requirements at Level 4

Students must take 120 credits in total, taken from the four modules listed above.

Level 5					
Code	**Title**	**Credits**	**Mandatory or Option**	**Pre-requisites**	**Exclusions**
COMP2370	Security Based Project	30	M	-	
COMP2372	Professional Development & Practice	30	M	-	
COMP2373	Cyber Hacking & Counter Hacking	15	M	COMP1373	
COMP2374	Cryptography Techniques and Applications	15	O	COMP1373	
COMP2375	Network Implementation and Systems Security	30	O	COMP1371, COMP1373	COMP2376
COMP2376	Protecting Web Applications	30	O	COMP1372, COMP1374	COMP2375
COMP2377	Cyber Security Standards	15	O	COMP1373	

COMP2378	Implementing Information Security Management Systems	15	O	COMP1373	

Requirements at Level 5

Students must take 120 credits in total, taken from the eight modules listed above, which must include COMP2370, COMP2372, COMP2373 plus a further 45 credits. Level 5 modules would be subject to demand in any given year (demand will be decided by the HOW resource and costing procedures for any given year; generally a minimum of six students will be required for any one module to be viable).

Award Map – Part Time Route

Course Title: Foundation Degree in Cyber Security (Part Time)	

Year 1 - Level 4					
Code	**Title**	**Credits**	**Mandatory or Option**	**Pre-requisites**	**Exclusions**
COMP1371	Computing & Networking Fundamentals	30	M	-	-
COMP1373	Foundations of Cyber Security & Information Assurance	30	M	-	-

Year 2 - Level 4					
Code	**Title**	**Credits**	**Mandatory or Option**	**Pre-requisites**	**Exclusions**
COMP1372	Software Development & Data Vulnerabilities	30	M	-	-
COMP1374	Web, HCI & Emerging Technologies	30	M	-	-

Requirements at Level 4

Students must take 120 credits in total, taken from the four modules listed above, normally taken over two years.

Year 3 - Level 5					
Code	**Title**	**Credits**	**Mandatory or Option**	**Pre-requisites**	**Exclusions**
COMP2370	Security Based Project	30	M	-	
COMP2372	Professional Development & Practice	30	M	-	
COMP2373	Cyber Hacking & Counter Hacking	15	M	COMP1373	
COMP2374	Cryptography Techniques and Applications	15	O	COMP1373	
COMP2375	Network Implementation and Systems Security	30	O	COMP1371, COMP1373	COMP2376
COMP2376	Protecting Web Applications	30	O	COMP1372, COMP1374	COMP2375
COMP2377	Cyber Security Standards	15	O	COMP1373	
COMP2378	Implementing Information Security Management Systems	15	O	COMP1373	

Requirements at Level 5

Students must take 120 credits in total, taken from the eight modules listed above, which must include COMP2370, COMP2372 (these modules to be submitted based upon work based experience, supported by tutorials during Years 2 and 3), COMP2373 plus a further 45 credits. Level 5 modules would be subject to demand in any given year (demand will be decided by the HOW resource and costing procedures for any given year; generally a minimum of six students will be required for any one module to be viable).

Please note: *This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided. More detailed information on the learning outcomes, content and teaching, learning and assessment methods of each module can be found in the module outlines and the course handbook. The accuracy of the information contained in this document is reviewed by the University and may be checked by the* ***Quality Assurance Agency for Higher Education****.*