THE UNIVERSITY *of* EDINBURGH
informatics

Board of Studies

Course Proposal Template

PROPOSED COURSE TITLE: Work-based Professional Practice in Cyber Security

PROPOSER(S): Tony Venus

DATE: 3rd February 2019

SUMMARY

This template contains the following sections, which should be prepared roughly in the order in which they appear (to avoid spending too much time on preparation of proposals that are unlikely to be approved):

1. Case for Support

– To be supplied by the proposer and shown to the BoS Academic Secretary prior to preparation of an in-depth course description

1a. Overall contribution to teaching portfolio

1b. Target audience and expected demand

1c. Relation to existing curriculum

1d. Resources

2. Course descriptor

- This is the official course documentation that will be published if the course is approved, ITO and the BoS Academic Secretary can assist in its preparation

3. Course materials

- These should be prepared once the Board meeting at which the proposal will be discussed has been specified

3a. Sample exam question

3b. Sample coursework specification

3c. Sample tutorial/lab sheet question

3d. Any other relevant materials

4. Course management

- This information can be compiled in parallel to the elicitation of comments for section 5.

4a. Course information and publicity

4b. Feedback

4c. Management of teaching delivery

5. Comments

- To be collected by the proposer in good time before the actual BoS meeting and included as received

5a. Year Organiser Comments

5b. Degree Programme Co-Ordinators

5c. BoS Academic Secretary

[Guidance in square brackets below each item. Please also refer to the guidance for new course proposals at http://www.inf.ed.ac.uk/student-services/committees/board-of-studies/course-proposal-guidelines. Examples of previous course proposal submissions are available on the past meetings page http://web.inf.ed.ac.uk/infweb/admin/committees/bos/meetings-directory.]

SECTION 1 – CASE FOR SUPPORT

[This section should summarise why the new course is needed, how it fits with the existing course portfolio, the curricula of our Degree Programmes, and delivery of teaching for the different years it would affect.]

1a. Overall contribution to teaching portfolio

[Explain what motivates the course proposal, e.g. an emergent or maturing research area, a previous course having become outdated or inappropriate in other ways, novel research activity or newly acquired expertise in the School, offerings of our competitors.]

This course is the work-based learning professional practice component required to deliver the level 11 graduate apprenticeship degree programme in cyber security. It has been developed to complement the taught courses and capstone project. This course is designed to ensure that all of the required skills and knowledge required by the SDS level 11 graduate apprenticeship framework in cyber security can be delivered and assessed as part of the overall graduate apprenticeship programme.

1b. Target audience and expected demand

[Describe the type of student the course would appeal to in terms of background, level of ability, and interests, and the expected class size for the course based on anticipated demand. A good justification would include some evidence, e.g. by referring to projects in an area, class sizes in similar courses, employer demand for the skills taught in the course, etc.]

This course is aimed at students undertaking the level 11 graduate apprenticeship in cyber security at the University of Edinburgh. It provides the work-based application of cyber security knowledge and skills as part of the graduate apprenticeship in cyber security. The graduate apprenticeship framework published by SDS sets out the technical cyber security skills and meta skills. This course sets out to apply these in the workplace by the graduate apprentice students and to assess them using suitable methods. The demand for this course will be driven by the uptake of the graduate apprenticeship in cyber security. The demand is set to develop from an initial cohort of 10 in September 2019 and rising to a steady state of 25-30 within three years.

1c. Relation to existing curriculum

[This section should describe how the proposed course relates to existing courses, programmes, years of study, and specialisms. Every new course should make an important contribution to the delivery of our Degree Programmes, which are described at http://www.drps.ed.ac.uk/17-18/dpt/drps_inf.htm.

Please name the Programmes the course will contribute to, and justify its contribution in relation to courses already available within those programmes. For courses available to MSc students, describe which specialism(s) the course should be listed under (see http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2017/programme-guide/specialist-areas), and what its significance for the specialism would be. Comment on the fit of the proposed course with the structure of academic years for which it should be offered. This is described in the Year Guides linked from http://web.inf.ed.ac.uk/infweb/student-services/ito/students.]

This course will contribute to the Graduate Apprenticeship in Cyber Security
which has the programme award MSc Cyber Security, Privacy and Trust

It is intended to progressively apply the learning of the taught courses delivered during year 1 (semesters 1 and 2), to the workplace.

1d. Resources

[While course approvals do not anticipate the School's decision that a course will actually be taught in any given year, it is important to describe what resources would be required if it were run. Please describe how much lecturing, tutoring, exam preparation and marking effort will be required in steady state, and any additional resources that will be required to set the course up for the first time. Please make sure that you provide estimates relative to class size if there are natural limits to its scalability (e.g. due to equipment or space requirements). Describe the profile of the course team, including lecturer, tutors, markers, and their required background. Where possible, identify a set of specific lecturers who have confirmed that they would either like to teach this course apart from the proposer, or who could teach the course in principle. It is useful to include ideas and suggestions for potential teaching duty re-allocation (e.g. through course sharing, discontinuation of an existing course, voluntary teaching over and above normal teaching duties) to be taken into account when resourcing decisions are made.]

There are no direct requirements for rooms or facilities from within the university as the course is delivered in the workplace. The course will need to be supported during year 1 and semester 1 of year 2. A role of Professional Practice Tutor has been identified and will need to be staffed to provide a support role as well as undertaking at least two visits to the graduate apprenticeship students in the workplace. Academic remote support will also need to be provided to the graduate apprenticeship students whilst they are at work during the summer periods. This may be by agreed email, telephone or other support arrangements.

SECTION 2 – COURSE DESCRIPTOR

[This is the official course descriptor that will be published by the University and serves as the authoritative source of information about the course for student via DRPS and PATH. Current course descriptions in the EUCLID Course Catalogue are available at www.euclid.ed.ac.uk under 'DPTs and Courses', searching for courses beginning 'INFR'*]*

2a. Course Title *[Name of the course.]*:

Work-based Professional Practice in Cyber Security

2b. SCQF Credit Points:

[The Scottish Credit and Qualifications Framework specifies where each training component provided by educational institutions fits into the national education system. Credit points per course are normally 10 or 20, and a student normally enrols for 60 credits per semester. For those familiar with the ECTS system, one ECTS credit is equivalent to 2 SCQF credits. See also http://www.scqf.org.uk/The%20Framework/Credit%20Points.]

20

SCQF Credit Level:

[These levels correspond to different levels of skills and outcomes, see http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf At University level, Year 1/2 courses are normally level 8, Year 3 can be level 9 or 10, Year 4 10 or 11, and Year 5/MSc have to be level 11. MSc programmes may permit a small number (up to 30 credits overall) of level 9 or 10 courses.]

11

Normal Year Taken: 1/2/3/4/5/MSc

[While a course may be available for more than one year, this should specify when it is normally taken by a student. "5" here indicates the fifth year of undergraduate Masters programmes such as MInf.]

2

Also available in years: 1/2/3/4/5/MSc

Different options are possible depending on the choice of SCQF Credit Level above: for level 9, you should specify if the course is for 3rd year undergraduates only, or also open to MSc students (default); for level 10, you should specify if the course is available to 3rd year and 4th year undergraduates (default), 4th year undergraduates only, and whether it should be open to MSc students; for level 11, a course can be available to 4th and 5th year undergraduates and MSc students (default), to 5th year undergraduates and MSc students, or to MSc students only]

n/a

Undergraduate or Postgraduate?

[If the course is only available to MSc students, then it must be classified as a Postgraduate course. All other courses, regardless of level, will be classified as Undergraduate]

Postgraduate

2c. Subject Area and Specialism Classification:

[Any combination of Computer Science, Artificial Intelligence, Software Engineering and/or Cognitive Science as appropriate. For courses available to MSc students, please also specify the relevant MSc specialist area (to be found in the online MSc Year Guide at http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2017/programme-guide/specialist-areas), distinguishing between whether the course should be considered as "core" or "optional" for the respective specialist area.]

Cyber Security

Appropriate/Important for the Following Degree Programmes:

[Please check against programmes from http://www.drps.ed.ac.uk/17-18/dpt/drps_inf.htm to determine any specific programmes for which the course would be relevant (in many cases, information about the Subject Area classification above will be sufficient and specific programmes do not have to be specified). Some courses may be specifically designed for non-Informatics students or with students with a specific profile as a potential audience, please describe this here if appropriate.]

MSc Cyber Security, Privacy and Trust (Graduate Apprenticeship)

Timetabling Information:

[Provide details on the semester the course should be offered in, specifying any timetabling constraints to be considered (e.g. overlap of popular combinations, other specialism courses, external courses etc).]

The work-based professional practice course is based upon work-based professional practice delivered during year 1 and semester 1 of year 2. The assessment is coursework and is undertaken during the work-based periods and finalised and submitted at the end of semester 1 in year 2.

2d. Summary Course Description:

[Provide a brief official description of the course, around 100 words. This should be worded in a student-friendly way, it is the part of the descriptor a student is most likely to read.]

This course is work-based and is focused on the real-world application of cyber security in a workplace environment. It includes experiencing how information and risk, threats and attacks, cyber security architecture and operations, secure systems hardening and usability and cyber security management are applied to provide resilience in a workplace organisational environment. Students who do this course will obtain practical experience in the design, implementation, and evaluation of cyber security approaches.

Course Description:

[Provide an academic description, an outline of the content covered by the course and a description of the learning experience students can expect to get. See guidance notes at: http://www.studentsystems.is.ed.ac.uk/staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

This course provides graduate apprenticeship students with a holistic approach to cyber security, privacy and trust. It is a key stage in the learning and development strategy of the graduate apprenticeship programme in cyber security. It is project based, introduced in the university and facilitated in the workplace around work-based projects.

This is a work-based learning course worth 20-credits. Students undertake work-based application throughout the GA programme and are expected to spend around 200 hours in total on this course. The university Student-Led Individually Created Course (SLICC) approach will be planned to cover the graduate apprenticeship students working with their specific employers and the work will directly link to their own contexts in the workplace.

The main topics are: the application of cyber security research techniques, developing an understanding of the application of cyber security operations to business environments. In addition, this course covers the meta skills required to operate in a professional environment including graduate attributes for: lifelong learning, aspiration and personal development, outlook and engagement, research and enquiry, personal and intellectual autonomy, personal effectiveness and communication in both university and the workplace

The year 1 courses in cyber security are applied to real world cyber security problems and projects.

Students will be directed in their learning using the SLICC approach. They will plan, propose, carry out, reflect on and evaluate a cyber security study from their own work context in cyber security. The SLICC framework requires that students use the generic learning outcomes to articulate their learning in their own defined project, reflect frequently using a blog, and collect and curate evidence of their learning in an e-portfolio. They receive relevant formative feedback on the Reflective Report, which forms the summative assessment. All this is with the guidance of a professional practice academic tutor.

The course will encourage appraisal of students' own practical experiences in cyber security and allow them to reflect on their learning in the context of cyber security.

Note: this course is not a stand-alone introduction to applied cyber security and can only be delivered as part of the Graduate Apprenticeship in cyber security.

Pre-Requisite Courses:

[Specify any courses that a student must have taken to be permitted to take this course. Pre-requisites listed in this section can only be waived by special permission from the School's Curriculum Approval Officer, so they should be treated as "must-have". By default, you may assume that any student who will register for the course has taken those courses compulsory for the degree for which the course is listed in previous years.

Please include the FULL course name and course code].

Graduate apprenticeship students must have completed all year 1 courses of the Graduate Apprenticeship in Cyber Security, core courses including:

Research Methods in Security, Privacy Trust (INFR****)

Co-Requisite Courses:

[Specify any courses that should be taken in parallel with the existing course. Note that this leads to a timetabling constraint that should be mentioned elsewhere in the proposal. Please include the FULL course name and course code].

Course Title: n/a

Prohibited Combinations:
Course Code:

[Specify any courses that should not be taken in combination with the proposed course. Please include the FULL course name and course code].

Course Title: n/a

Course Code:

Other Requirements:

[Please list any further background students should have, including, for example, mathematical skills, programming ability, experimentation/lab experience, etc. It is important to consider that unless there are formal prerequisites for participation in a course, other Schools can register their students onto our courses, so it is important to be clear in this section. Also be aware that MSc students are unlikely to have the pre-requisite courses, so alternative knowledge should be recommended. If you want to only permit this by special permission, a statement like "Successful completion of Year X of an Informatics Single or Combined Honours Degree, or equivalent by permission of the School." can be included.]

This course is not a stand-alone introduction to applied cyber security and can only be delivered as part of the Graduate Apprenticeship in Cyber Security.

Available to Visiting Students: ~~Yes~~/No

[Provide a justification if the answer is No.]

This course forms an integral part of the Graduate Apprenticeship in Cyber Security and must be employer based.

2e. Summary of Intended Learning Outcomes (MAXIMUM OF 5):

[List the learning outcomes of the course, emphasising what the impact of the course will be on an individual who successfully completes it, rather than the activity that will lead to this outcome. Further guidance is available from https://canvas.instructure.com/courses/801386/files/24062695]

Using the generic SLICC learning outcomes and reflective framework, students will define and articulate their own learning outcomes in the context of experiential learning in their own project, and the cross-disciplinary nature of data science. Their own learning outcomes will align with the SLICC learning outcomes and will mean that after completing this course, students will be able to:

1. Demonstrate an understanding of the cross-disciplinary nature of cyber security, and the complexities, challenges and wider implications of the contexts in which cyber security problems occur in the workplace;
2. Draw on and apply relevant cyber security approaches, tools and frameworks for cyber security enquiry to different settings in real world situations;
3. Review, develop and apply skills and attributes (academic, professional and/or personal) in graduate attributes, including and lifelong learning, aspiration and personal development, outlook and engagement, research and enquiry, personal and intellectual autonomy, personal effectiveness and communication in both university and the workplace;
4. Frame and address cyber security business problems, questions and issues as a cyber security project, being aware of the environment and context in which the problem exists;
5. Review, evaluate and reflect upon knowledge, skills and practices in cyber security.

Assessment Information

[Provide a description of all types of assessment that will be used in the course (e.g. written exam, oral presentation, essay, programming practical, etc) and how each of them will assess the intended learning outcomes listed above. Where coursework involves group work, it is important to remember that every student has to be assessed individually for their contribution to any jointly produced piece of work. Please include any minimum requirements for assessment components e.g. student must pass all individual pieces of assessment as well as course overall].

Written Exam 0 %, Practical Exam 0 %, Coursework 100 %

A SLICC is assessed via three key components, a self-reflective report, an agreed portfolio of outputs and a formative self-assessment.

Self-critical ‘Final Reflective Report’ (100% weighting) - The reflective report is the key component of the assessment. Apprentices are expected to document and demonstrate active self-critical reflection and responses to the application of their learning throughout experience. It is essential that the report is linked to and draws upon the e-portfolio of evidence of learning. Maximum word limit is 3000 words.

E-portfolio of evidence - At the proposal approval stage for the work-based professional practice, the work-based tutor/advisor will discuss and agree with what outputs and information need to be created, collated and submitted in the e-portfolio. This e-portfolio will support and provide evidence for the learning and development of skills throughout the programme. The e-portfolio should be constructed throughout the duration of the learning experience, demonstrating evolution, iteration and progress over-time. It must include a regular reflective blog diary. It may contain other evidence, which may take many forms including photographs, documents, reports, feedback, video, podcasts, etc.

Formative Self-Assessment - An important component of the final submission, in addition to the ability to self-critically reflect on work place experience, is to demonstrate an understanding of the achievements made in the work-based application of the GA Cyber Security learning through graded self-assessment. In the self-assessment apprentices are required to demonstrate the alignment of the grades that they have provided for each learning outcome to the justification for them, and where this is evidenced within the e-portfolio.

Assessment Weightings:

Written Examination: ___%

Practical Examination: ___%

Coursework: 100%

Time spend on assignments:

[Weightings up to a 70/30 split between exam and coursework are considered standard, any higher coursework percentage requires a specific justification. The general expectation is that a 10-point course will have an 80/20 split and include the equivalent of one 20-hour coursework assignment (although this can be split into several smaller pieces of coursework. The Practical Examination category should be used for courses with programming exams. You should not expect that during term time a student will have more than 2-4 hours to spend on a single assignment for a course per week. Please note that it is possible, and in many cases desirable, to include formative assignments which are not formally assessed but submitted for feedback, often in combination with peer assessment.]

This course is the work-based professional practice for the Graduate Apprenticeship in Cyber Security. It is focussed on the practical application of cyber security knowledge and skills in the workplace and is therefore 100% coursework assessed. The course is delivered as experiential learning using work-based application of learning from their studies. Therefore, the time spent on assignments will be 100 % coursework focussed. Formative feedback will be presented to students by both the Professional Practice tutor and the workplace mentor.

Academic description:

[A more technical summary of the course aims and contents. May include terminology and technical content that might be more relevant to colleagues and administrators than to students.]

The aim of this course is to provide graduate apprenticeship students with work-based professional practice in the application of cyber security techniques. It is delivered over the first year period and draws from the work-based experience gained therein. It provides apprentices with a practical introduction and understanding of the foundations, concepts and techniques applied to cyber security in the workplace. It is a key stage in the learning and development strategy of the graduate apprenticeship programme in Cyber Security. It is experience based, introduced in the university and facilitated in the workplace.

During this course students will have to demonstrate the ability to work independently and integrate information gained in the graduate apprenticeship in cyber security courses. Their knowledge and understanding of cyber security as it relates to real world problems will continue to develop. They will also learn generic approaches/skills such as project planning, work-ethics, problem solving, teamwork, time-keeping, reflective analysis and evaluation skills. Since the course is work-based the pedagogy approach will develop their ability to apply learning in the workplace and to reflect effectively and to articulate their learning and skills. This will enable each apprentice to develop their abilities in self-critical reflection, organisation and time-management, self-assessment, evaluation of standards and competencies achieved, application of prior learning in a defined context, and provide opportunities to further develop analytical cyber security skills.

The learning outcomes also include those derived from and embedded in the institutional ‘Graduate Attributes’. The learning outcomes are flexible to provide students with autonomy. With guidance from the assigned academic tutor, this flexibility of choice enables apprentices, in the context of their own chosen experience, to focus on their own particular ‘skills’ and ‘mindset’. They can select the specific attributes that they consider are the most important to reflect upon, looking into their current and future professional and personal aims and career aspirations.

Note: this course is not a stand-alone introduction to applied cyber security and can only be delivered as part of the Graduate Apprenticeship in Cyber Security.

Syllabus:

[Provide a more detailed description of the contents of the course, e.g. a list of bullet points roughly corresponding to the topics covered in each individual lecture/tutorial/coursework. The description should not exceed 500 words but should be detailed enough to allow a student to have a good idea of what material will be covered in the course. Please keep in mind that this needs to be flexible enough to allow for minor changes from year to year without requiring new course approval each time.]

- Information and risk: including confidentiality, integrity and availability (CIA); concepts such as probability, consequence, harm, risk identification, assessment and mitigation; and the relationship between information and system risk.
- Threats and attacks: threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities.
- Cyber security architecture and operations: physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance.
- Secure systems hardening and usability: the concepts of systems hardening and usability to ensure robust, resilient systems that are fit for purpose.
- Cyber security management: understanding the personal, organisational and legal/regulatory context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cyber security is implemented.
- Personal & professional: the ability to communicate, problem solve and work with and lead teams.

Relevant QAA Computing Curriculum Sections:
[Please see http://www.qaa.ac.uk/en/Publications/Documents/SBS-Computing-consultation-15.pdf to check which section the course fits into.]

Computing

Graduate Attributes, Personal and Professional skills:

[This field should be used to describe the contribution made to the development of a student's personal and professional attributes and skills as a result of studying this course – i.e. the generic and transferable skills beyond the subject of study itself. Reference in particular should be made to SCQF learning characteristics at the correct level http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf].

Development of graduate attributes are a key component of a graduate apprenticeship. In this course there is specific reference to the development and application of skills and attributes (academic, professional and/or personal), including and lifelong learning, aspiration and personal development, outlook and engagement, research and enquiry, personal and intellectual autonomy, personal effectiveness and communication in both university and the workplace.

Reading List:

*[Provide a list of relevant readings. See also remarks under **3d**.]*

Breakdown of Learning and Teaching Activities:

[Total number of lecture hours and tutorial hours, with hours for coursework assignments.]

[The breakdown of learning and teaching activities should only include contact hours with the students; everything else should be accounted for in the Directed Learning and Independent Learning hours.

The total being 10 x course credits. Assume 10 weeks of lectures slots and 10 weeks of tutorials, though not all of these need to be filled with actual contact hours. As a guideline, if a 10-pt course has 20 lecture slots in principle, around 15 of these should be filled with examinable material; the rest should be used for guest lectures, revision sessions, introductions to assignments, etc. Additional categories of learning and teaching activities are available, a full list can be found at:

http://www.euclid.ed.ac.uk/Staff/Support/User_Guides/CCAM/Teaching_Learning.htm]

Lecture Hours: 5 hours

Seminar/Tutorial Hours: 0 hours

Supervise practical/Workshop/Studio hours: 0 hours

Summative assessment hours: 50 hours

Feedback/Feedforward hours: 5 hours

Directed Learning and Independent Learning hours: 140 hours

Total hours: 200 hours

You may also find the guidance on ‘Total Contact Teaching Hours’ and ‘Examination & Assessment Information’ at:
http://www.studentsystems.ed.ac.uk/Staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

Keywords:

[A list of searchable keywords.]

SECTION 3 - COURSE MATERIALS

3a. Sample exam question(s)

[Sample exam questions with model answers to the individual questions are required for new courses. A justification of the exam format should be provided where the suggested format non-standard. The online list of past exam papers gives an idea of what exam formats are most commonly used and which alternative formats have been http://www.inf.ed.ac.uk/teaching/exam_papers/.]

3b. Sample coursework specification

[Provide a description of a possible assignment with an estimate of effort against each sub-task and a description of marking criteria.]

3c. Sample tutorial/lab sheet questions

[Provide a list of tutorial questions and answers and/or samples of lab sheets.]

3d. Any other relevant materials

[Include anything else that is relevant, possibly in the form of links. If you do not want to specify a set of concrete readings for the official course descriptor, please list examples here.]

SECTION 4 - COURSE MANAGEMENT

4a. Course information and publicity

[Describe what information will be provided at the start of the academic year in which format, how and where the course will be advertised, what materials will be made available online and when they will be finalised. Please note that University and School policies require that all course information is available at the start of the academic year including all teaching materials and lecture slides.]

4b. Feedback

[Provide details on feedback arrangements for the course. This includes when and how course feedback is solicited from the class and responded to, what feedback will be provided

on assessment (coursework and exams) within what timeframe, and what opportunities students will be given to respond to feedback.

The University is committed to a baseline of principles regarding feedback that we have to implement at every level, these are described at http://www.docs.sasg.ed.ac.uk/AcademicServices/Policies/Feedback_Standards_Guiding_Principles.pdf.

Further guidance is available from http://www.enhancingfeedback.ed.ac.uk/staff.html.]

4c. Management of teaching delivery

[Provide details on responsibilities of each course staff member, how the lecturer will recruit, train, and supervise other course staff, what forms of communication with the class will be used, how required equipment will be procured and maintained. Include information about what support will be required for this from other parties, e.g. colleagues or the Informatics Teaching Organisation.]

SECTION 5 - COMMENTS

[This section summarises comments received from relevant individuals prior to proposing the course. If you have not discussed this proposal with others please note this].

5a. Year Organiser Comments

[Year Organisers are responsible for maintaining the official Year Guides for every year of study, which, among other things, provide guidance on available course choices and specialist areas. The Year Organisers of all years for which the course will be offered should be consulted on the appropriateness and relevance on the course. Issues to consider here include balance of course offerings across semesters, subject areas, and credit levels, timetabling implications, fit into the administrative structures used in delivering that year.]

5b. BoS Academic Secretary

[Any proposal has to be checked by the Secretary of the Board of Studies prior to discussion at the actual Board meeting. This is a placeholder for their comments, mainly on the formal quality of the content provided above.]