UNIVERSITY FACULTY SENATE FORMS

Academic Program Approval

This form is a routing document for the approval of new and revised academic programs. Proposing department should complete this form. Detailed instructions for the proposal should be followed. A checklist is available to assist in the preparation of a proposal. Submission of new majors or requests for permanent status will find additional requirements and information here. For more information, call the Faculty Senate Office at 831-2921.

Submitted by: Stephan Bohacek_____phone number_831-4274_____

Department: Electrical and Computer Engineering_____email address bohacek@udel.edu

Date: November 28, 2016_____

Action: Establish 4+1 BEE + MS-Cybersecurity

(Example: add major/minor/concentration, delete major/minor/concentration, revise major/minor/concentration, academic unit name change, request for permanent status, policy change, etc.)

Changes when approved will be effective at the start of the next academic year unless special circumstances and a specific request is made.

Current degree Separate BEE and MS-Cybersecurity_____
(Example: BA, BACH, BACJ, HBA, EDD, MA, MBA, etc.)

Proposed change leads to the degree of: BEE and MS-Cybersecurity _____
(Example: BA, BACH, BACJ, HBA, EDD, MA, MBA, etc.)

Proposed name: 4+1 in BEE and MS-Cybersecurity _____
Proposed new name for revised or new major / minor / concentration / academic unit (if applicable)

Revising or Deleting:

Undergraduate major / Concentration:_____
(Example: Applied Music – Instrumental degree BMAS)

Undergraduate minor:_____
(Example: African Studies, Business Administration, English, Leadership, etc.)

Graduate Program Policy statement change:_____
(**Must attach** your Graduate Program Policy Statement)

Graduate Program of Study:_____
(Example: Animal Science: MS Animal Science: PHD Economics: MA Economics: PHD)

Graduate minor / concentration:_____

Note: all graduate studies proposals must include an electronic copy of the Graduate Program Policy Document, either describing the new program or highlighting the changes made to the original policy document.

Below are the additions to the Electrical and Computer Engineering Graduate Programs section of the course catalog. Within the section titled REQUIREMENTS FOR THE DEGREES, the following will be added. No other changes are required.

4+1 Bachelor of Electrical Engineering/Master of Science in Cybersecurity

The department offers a special 4 + 1 BEE/Master of Science in Cybersecurity program for highly-qualified undergraduate students. The program allows the student to earn both the BEE and the Master of Science in Cybersecurity degree in five years of full-time study in Electrical and Computer Engineering at the University of Delaware. Students must apply by April 1 of their junior year. GRE scores will be waived. For admissions to this program the following minimum criteria will be applied:

An undergraduate grade point average of 3.3 on a 4.0 scale.
A minimum of two letters of strong support from former teachers at the University of Delaware.

The application and processing instructions can be found at the Graduate Office website. Choose either an area or undecided and once you start the application, click on the 4 + 1 program option.

Students admitted to the 4 + 1 BEE/Master of Science in Cybersecurity program are required to meet all the requirements listed for the Master of Science in Cybersecurity degree and can choose either the thesis or the non-thesis option (the thesis option can take more than five years to complete.) Students are required to complete two of the courses acceptable for the Master of Science in Cybersecurity degree during enrollment in the BEE degree (600 level technical courses). These two courses can also be counted toward meeting the technical elective requirement of the BEE degree.

ROUTING AND AUTHORIZATION: (Please do not remove supporting documentation.)

Department Chairperson _____ Date 12-5-16

Dean of College _____ Date 2/10/2017
(By signing above, the Dean confirms that their college policies and bylaws have been followed correctly during consideration of the request described in this form.
The approval actions that were taken at the college level were (check all that apply) :
_____college faculty vote; _____college curriculum approval _____college senate approval

Chairperson, College Curriculum Committee _____ Date 12/6/16

Chairperson, Senate Com. on UG or GR Studies _____ Date _____

Chairperson, Senate Coordinating Com. _____ Date _____

Secretary, Faculty Senate _____ Date _____

Date of Senate Resolution _____ Date to be Effective _____

Registrar _____ Program Code _____ Date _____

Vice Provost for Academic Affairs & International Programs _____ Date _____

Board of Trustee Notification _____ Date _____

Revised 4/14/2016 khs

Provide a brief summary of the proposed program changes and describe the rationale for the change(s):
(Explain your reasons for creating, revising, or deleting the curriculum or program.)

Currently, the Department of Electrical and Computer Engineering offers the Master of Science in Cybersecurity degree in two modalities, as a thesis and non-thesis master's degree. To expand our professional degree enrollment and in order to attract and retain highly qualified domestic applicants, we propose to establish a 4+1 BEE/ Master of Science in Cybersecurity. The proposed program will give our highly-qualified and highly-motivated undergraduate students the opportunity to earn both the Bachelor's degree in computer engineering and the Master's degree in cybersecurity in five years of full-time study. Both, thesis and non-thesis options, will be offered in the 4+1 Master of Science in Cybersecurity, but the thesis option may take more than five years to complete.

List new courses required for the new or revised curriculum. How do they support the overall program objectives of the major/minor/concentrations)?
(Be aware that approval of the curriculum is dependent upon these courses successfully passing through the **Course Challenge** list. If there are no new courses enter "None")
None

Identify other units affected by the proposed changes and provide letters of support from those units. :
(This would include other departments/units whose courses are a required part of the proposed curriculum. If no other unit is affected, enter "None")
None

Changes to degree programs will explain how this new/revised curriculum supports the 5 goals of undergraduate education (do not just list the gen ed goals):
http://www2.udel.edu/gened/

New majors and minors will include support letters from the Library, Dean, and/or Department Chair

Supply a resolution for all new majors/programs; name changes of colleges, departments, degrees; transfer of departments from one college to another; creation of new departments; requests for permanent status. See example of resolutions.

Program Requirements:
(Show the complete new or revised curriculum as it should appear in the Course Catalog. If this is a revision, be sure to indicate the changes being made to the current curriculum and **include a complete side-by-side comparison** of the credit distribution before and after the proposed change. If this is a change to an honors program, be sure that the honors degree language is included.) **See example of side by side.**

Master of Science in Cybersecurity (MS)

The Master of Science in Cybersecurity program is administered through the Department of Electrical and Computer Engineering.

The Cybersecurity Master's program is structured to enable professionals to gain advanced training in this field. Unlike other programs that are solely focused on IT security, this program emphasizes design of secure software and systems, security analytics, and secure business systems. It will train individuals that have a traditional background in engineering, computer science, information systems, or related fields to have strong security skills enabling them to develop *new* secure systems and/or software, to exploit analytics for security purposes, or to develop and manage secure business systems. Thus graduates of this program will be skilled in the latest theories and practices required to address the most challenging cybersecurity issues facing the world today.

Requirements for Admission

The requirements for admission to the Master of Science in Cybersecurity are the following:

1. Applicants must hold a bachelor's degree from an accredited four-year college or university with a minimum grade point average of 3.0 on a 4.0 system.
2. Applicants must have undergraduate degrees in electrical engineering, computer engineering, computer science, mathematics, physics, or related disciplines. Applicants with degrees in other disciplines may be admitted with provisional status and may be required to complete prerequisite courses that are deemed necessary for appropriate preparation for courses in the program.
3. All applicants must take the Graduate Record Examination. The following GRE scores are competitive: Quantitative: 150, Verbal + Quantitative: 300. No GRE subject test is required.
4. International applicants must demonstrate a satisfactory level of proficiency in the English language if English is not their first language. The University requires an official TOEFL score of at least 550 on paper-based, 213 on computer-based, or 79 on Internet-based tests. TOEFL scores more than two years old cannot be considered official. Alternatively, IELTS can be accepted in the place of the TOEFL. The minimum IELTS score is 6.5 overall with no individual sub-score below 6.0.

Applications are accepted according to the standard University of Delaware deadlines. Admission to the graduate program is competitive. Those who meet the stated requirements are not guaranteed admission, and those who fail to meet all requirements are not necessarily precluded from admission if they offer other appropriate strengths.

Degree Requirements

The Cybersecurity Master's program requires 30 credit hours in either a thesis or non-thesis option. The non-thesis option requires all 30 credits to be completed through coursework, while

the thesis-option requires 24 credit hours of coursework and six credits of master's thesis (CPEG 869). The curriculum requirements for the thesis and non-thesis option are:

- 15 credits of Fundamentals of Cybersecurity courses
- 15 credits of elective courses in a chosen Concentration Area.
  - Concentration Areas are: (I) Secure Software, (II) Secure Systems, (III) Security Analytics, and (IV) Security Management.
  - Elective courses are to be taken primarily from a single chosen Concentration Area, with a maximum of six (6) credits taken from an alternative Concentration Area or as additional Fundamentals of Cybersecurity courses.
  - In the thesis option, six (6) credits of master's thesis are to be completed in lieu of six (6) Concentration Area elective credits.

Fundamentals of Cybersecurity and Concentration Area courses are listed below. Note that individual courses are typically three (3) credits, i.e., the 30 credit hours required for the master's non-thesis degree typically equates to 10 courses (or eight (8) courses and a thesis for the thesis option).

Fundamentals of Cybersecurity

Students must complete 15 credits, or five (5) courses, of Fundamentals of Cybersecurity. Courses designated as Fundamentals of Cybersecurity are:

CPEG 665	Introduction to Cybersecurity (CYBER I)	3 cr
CPEG 697	Advanced Cybersecurity (CYBER II)	3 cr
CPEG 694	System Hardening & Protection (DEFENSE)	3 cr
CPEG 695	Digital Forensics	3 cr
CPEG 676	Secure Software Design	3 cr
CPEG 671	Pen Test and Reverse Engineering	3 cr
CPEG 672	Applied Cryptography	3 cr

Concentration Areas

Students must complete 15 credits, or five (5) courses, of electives. Elective courses are to be taken primarily from a single chosen Concentration Area. Of these five (5) elective courses, a maximum of two (2) can be taken outside the single Concentration Area (from one of the other Concentration Areas or from the set of Fundamentals of Cybersecurity courses). The Concentration Areas and courses within each area are listed below.

Concentration in Secure Software

The Secure Software Concentration is designed for a professional responsible for developing secure software systems. Secure Software electives are:

CPEG 670	Web Applications Security	3 cr
CISC 621	Algorithm Design and Analysis	3 cr
CISC 663	Operating Systems	3 cr
CISC 672 OR CPEG 621	Compiler Construction Compiler Design	3 cr
CISC 675	Software Engineering Principles and Practices	3 cr
CISC 611/CPEG 611	Software Process Management	3 cr
CISC 612/CPEG 612	Software Design	3 cr
CISC 613/CPEG 613	Software Requirements Engineering	3 cr
CISC 614/CPEG 614	Formal Methods in Software Engineering	3 cr
CISC 615/CPEG 615	Software Testing and Maintenance	3 cr
CPEG 676	Secure Software Design	3 cr

Concentration in Secure Systems

The Secure Systems Concentration is designed for a professional responsible for secure systems that can include wireless and network communication systems, embedded systems, and related physical systems. Secure Systems electives are:

ELEG 635	Digital Communication	3 cr
ELEG 658	Advanced Mobile Services	3 cr
ELEG 617	The Smart Grid	3 cr
CPEG 696	Topics in Cybersecurity (Simulation-based Cybersecurity)	3 cr
ELEG 812	Wireless Digital Communications	3 cr
CPEG 675	Embedded Computer Systems	3 cr
CISC 650/ELEG 651	Computer Networks II	3 cr
CISC 853	Network Management	3 cr
CPEG 673	Cloud Computing and Security	3 cr
CISC 886	Multi-Agent Systems	3 cr
CPEG 674	SCADA Systems and Security	3 cr
CPEG 853	Computer System Reliability	3 cr

Concentration in Security Analytics

The Security Analytics Concentration is designed for a professional responsible for utilizing big data, analytics, and statistical learning methods to identify and characterize anomalous behavior and security risks. Security Analytics electives are:

ELEG 815	Analytics I – Statistical Learning	3 cr
ELEG 817/FSAN 817	Large Scale Machine Learning	3 cr
CISC 683	Introduction to Data Mining	3 cr
CISC 637	Database Systems	3 cr
CPEG 657	Search and Data Mining	3 cr
CISC 681	Artificial Intelligence	3 cr
CISC 684	Introduction to Machine Learning	3 cr
CISC 689	TPCS: Artificial Intelligence: Machine Learning	3 cr
ELEG 630	Information Theory	3 cr

Concentration in Security Management

The Security Management Concentration is designed for a professional responsible for instituting and managing security controls within an enterprise. Security Management electives are:

MISY 850	Security and Control	3 cr
FINC 855	Capital Markets & Financial Institutions	3 cr
BUAD 840	Ethical Issues in Domestic and Global Business Environments	3 cr
MISY 840	Project Management and Costing	3 cr
ACCT 806	Systems Analysis, Design and Implementation	3 cr
BUAD 870	Leadership and Organizational Behavior	3 cr
BUAD 877	Skills for Change Agents	3 cr
MISY 810	Telecommunications and Networking	3 cr