UNIVERSITY OF MARY WASHINGTON – PROGRAM CHANGE PROPOSAL

Electronically submit this completed form with attachments in one file to the Chair of the College Curriculum Committee.

COLLEGE (check one):	**Arts and Sciences**	x	**Business**	x	**Education**	
Proposal Submitted By: Andrew Marshall			Date Prepared: 10/5/15			
Department /Program:	**CAS Department of Computer Science; COB**					

Note: for any program change entailing the addition any new courses, or revisions to existing courses, separate proposal for those course actions must also be submitted.

PROPOSAL TO CHANGE EXISTING PROGRAM (check **no than one** of the following)	
Revise requirements for existing **major**	
Revise requirements for a concentration within an existing **major**	
Revise requirements for an existing **degree program**	
Revise requirements for existing **certificate** program	
Revise requirements for existing **minor**	
Implementation Date: FALL semester, year:	

REQUIRED ATTACHMENTS FOR CHANGES TO EXISTING PROGRAMS:

1. **Rationale statement** (Why is this program change needed? What purposes will it serve?)
2. **Impact Statement** (Provide details about the Library, space, budget, technology, and impacts created by this program change. Supporting statements from the Library, IT Department, etc. evaluating the resource impact and feasibility of the program change are required.)
3. **Catalog Copy** (Provide the *existing* Catalog Description **and** the complete statement of the *proposed* new Catalog description that reflects the program changes)

PROPOSAL TO CREATE NEW PROGRAM *NOT* REQUIRING STATE ACTION (check no more that **one** of the following)		
New concentration within existing major		Name:
New minor	**x**	Name: Information Security
New Major but NOT a new degree*		Name:
*Use ONLY for interdisciplinary majors that will be grouped as part of the "Special Majors/General Liberal Arts and Sciences" degree (CIP Code 24.0101) or reported as a BLS degree (CIP Code 24.0199)		
Implementation Date (semester and year):		

REQUIRED ATTACHMENTS FOR NEW PROGRAMS *NOT* REQUIRING STATE APPROVAL:

1. **Rationale statement** (Why is this additional program needed? What purposes will it serve?)
2. **Impact Statement** (Provide details about the Library, space, budget, technology, and impacts created by this program change. Supporting statements from the Library, IT Department, etc. evaluating the resource impact and feasibility of adding the new program are required.)
3. **Catalog Copy** (Provide the complete Catalog Description for the proposed new program)
4. **Any change that impacts another Department must have a written statement (such as a copy of an email) from the Chair(s) agreeing to the change.**

Department Chair Approval: Heather Dawes **Date:** **11/10/2015**

CCC Chair Approval: Dawn S Be **Date:** 11/18/15

Dean Approval: Richard Finkelstein **Date:** 11/19/15

UCC Chair Approval: Patricia Reynolds **Date:** 12/07/2015

***Provost Approval:** _____ **Date:** _____

**Required only in cases of proposals for new concentrations, new minors, or new majors that do not involve a new degree*

Date: October 13, 2015

To:
Dawn Bowen, Chair, CAS Curriculum Committee.
Lance Gentry, Chair, COB Curriculum Committee.

From:
Andrew Marshall, Department of Computer Science.
Michael S. Lapke, College of Business.

RE: Proposal for an interdisciplinary minor in Information Security.

The Department of Computer Science in CAS, together with the College of Business, proposes a new interdisciplinary minor in Information Security. The Department of Computer Science will host the program.

The requirements for the Information Security minor are as follows:

Required courses (Total Credits: 17):

- CPSC 220 – Computer Programming and Problem Solving.
- CPSC 225 – Software Development Tools.
- One of:
    - CPSC 345 – Introduction to Computer Security.
    - MIST 411 – Information Security.
- CPSC 414 – Network Principles and Applications.
- One of:
    - New course: MIST 444 - Ethical Hacking (prereq: CPSC 345 or MIST 411) -- This course introduces students to penetration testing methods that can be used in an ethical hacking situation. Students learn in interactive environments where they scan, test, hack and secure their own systems, and gain experience with essential security systems.
    - New course: CPSC 445 – Computer Security 2 (prereq: CPSC 345 or MIST 411) – A course building on the introductory material covered in the prerequisites. A course on software security and vulnerabilities. Topics include identifying software bugs and how they are exploited to compromise security, methods for detection and prevention of software bugs, and secure programming practices.
- One of:
    - CPSC 302 – Computer Ethics.
    - BUAD 464 – Business Ethics.

- PHIL 225 – Practical Ethics.

Rationale for the Information Security Minor at UMW:

Unfortunately, it seems like hardly a week goes by without some new story appearing about a recent corporate or government data breach. This is due to a number of factors at play, including; the increased connectedness (where everything is online), the increased monetary focus of the cyber criminal underground, the increased activity by government actors, the lagging security of our networked devices and infrastructure, and the lack of cyber security professionals. UMW, through faculty research, is helping to address some of these issues. However, we have an opportunity to go further by addressing the lack of security professionals and also help some of our motivated students gain entry into a challenging but important and rewarding career.

Modern information and cyber security includes a large number of sub disciplines each with a large number of varied positions requiring differing skills. In modern institutions knowledgeable personnel at many levels must address security. At the managerial level security and information protection policies must be developed along with training on those policies and practices for all personnel. Network and infrastructure engineers must incorporate those policies and security best practices into the design and implementation of the cyber infrastructure (including mobile devices). Security personnel must also employ tools and monitor the security of the infrastructure to identify and stop potential attacks. If the organization develops its own software or hardware, engineers must take pains to prevent the introduction of security flaws and fix them when they are identified. Finally, this entire process is dynamic and continually evolves with new threats at one level requiring updates and improvements at all others. Thus, there are numerous opportunities for student with a wide range of interests to pursue a carrier in cyber security. However, currently there is a shortage of knowledgeable personnel to fill all such positions.

There is currently a general consensus that there is a shortage of cyber security professionals (Burning Glass Technologies 2015). Bloomberg reports that the Pentagon is planning to triple its cyber security staff (Lawrence 2014). The FBI is planning to hire at least 1,000 more cyber security positions (FBI n.d.). The Department of Homeland Security is currently actively hiring cyber security personnel (Department of Homeland Security (DHS) n.d.). DHS has also started a new National Initiative for Cyber security Careers and Studies (NICCS) (National Initiative for Cybersecurity Careers and Studies (NICCS) n.d.). The positions are not limited to the government; a recent report (Burning Glass Technologies 2015) found that demand for cyber security workers has increased rapidly. The fastest increases in demand for cyber security workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%). UMW is particularly well geographically positioned to offer education in cyber security to our students given the proximity to Washington, DC and the numerous government agencies and contractors engaged in cyber security in our area.

Cyber Security in a Liberal Arts Setting:

It is our opinion that the liberal arts' setting of UMW provides an excellent environment to prepare students to contribute to the field of cyber security. The liberal arts' produces thinkers with broad knowledge who are better able to thrive in rapidly changing fields. The liberal arts also graduates ethical citizens who are better able to take on tough ethical questions such as those that arise in cyber security.

There are numerous specialties in the field of cyber security. The differing areas and corresponding skills required offer a range of opportunities that promise to appeal to students with varied interests. In addition, the field of cyber security evolves rapidly, as new technologies, software, and platforms are developed new security flaws and issues usually rapidly follow. Thus having the skills learned in the liberal arts; critical thinking, broad knowledge, the ability to absorbed and understand new information, communication skills, and the ability to learn new skills, will be highly valuable in such a rapidly evolving area. For example, although there is a general consensus that there is a critical shortage of cyber security professionals, there has also been a rapid increase in educational programs developed to train personnel in this area. A recent report (Libicki 2014) conducted by the Forces and Resources Policy Center of the RAND National Security Research Division (NSRD) warned that intensive two-year (junior college) programs in cyber security appear problematic. "Such education also produces a corps of intensively educated individuals that would be difficult to employ if the requirements for cyber security work change substantially— as they surely will, given the volatility of the field." Our students will have the valuable resource of a liberal arts education and will be better able to adapt and indeed thrive in the rapidly evolving field of cyber security.

Cyber security professionals are routinely faced with ethical questions, from information privacy to how to properly handle new software security flaws. Most programs in cyber security do not give students exposure to ethics, which could provide the students with the skills they will need when facing such questions. What better place than a liberal arts institution to provide the students with the needed exposure to ethics? The minor requires the students to take one of three ethics courses (PHIL 225, CPSC 302, BAUD 464). This will better prepare the students to face the ethics questions that will almost certainly arise during their careers.

Goals and Course Selection:

The goals of the information security minor are two fold.

1. Give students a thorough introduction to information security. The introduction will include exposure and practice in a broad, representative set of topics, which will give students the experience needed to obtain entry-level positions in information security. To this end we have selected and developed courses that give the students a foundations in programming, Unix systems, and networking (CPSC 220, CPSC 225, CPSC 414). We included and developed new courses which give the students a solid, in-depth, exposure to information security including, policy, system/OS security, penetration testing, software security, and defensive measures (CPSC 345, MIST 411, MIST 444, CPSC 445). The material in these courses will be continually updated to present the most up-to-date information to the students.

2. Ensure the minor is accessible to a broad range of majors. The major is structured such that a student need not major in computer science in order to be successful in the minor. Indeed due to the diversity of specialties and need for a wide variety of expertise in information security, we have developed the minor to be obtainable for students in a number of majors. Students are also given some flexibility in the minor. For example for the final capstone course students can select from MIST 444 which is more focused on systems security, or CPSC 445 which focused on software security. In addition, it is hoped that we will later be able to add a third capstone course in cryptography that will appeal to those students interested in careers in cryptography.

Pains have been taken to ensure that our students obtain a broad introduction to cyber security and have the ability to select courses in the minor to shape their education to their interests.

Resource impact:

Library: The library has the necessary material to support the minor.

Staff: Faculty within the colleges already have the expertise to teach the desired courses. One or two additional instructional adjuncts per year associated with COB or the Computer Science would allow us to teach some of the courses in the evening broadening the appeal of the minor to non-traditional students. This could be addressed in the future when resources become available.

Equipment: Very little equipment is required to support this minor, since most of it involves personal computers already available to faculty and students. The development of a specialized computer security lab would be welcomed in the future if resources become available but it is not a necessity to get the minor off the ground.

Space. We do not anticipate any impact on space resources.

Academic Catalog copy:

Requirements for the Information Security minor: Seventeen (17) credits to include CPSC 220; CPSC 225; CPSC 414; 3 elective credits between CPSC 345 or MIST 411; 3 elective credits between MIST 444 or CPSC 445; 3 elective credits from among CPSC 302 or BAUD 464 or PHIL 225.

Works Cited

Department of Homeland Security (DHS). *dhs.gov.* http://www.dhs.gov/homeland-security-careers/dhs-cybersecurity (accessed October 15, 2015).

FBI. *Cyber Careers.* https://www.fbijobs.gov/CyberCareers/ (accessed October 15, 2015).

Lawrence, Dune. *The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016.* April 15, 2014. http://www.bloomberg.com/bw/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete (accessed October 15, 2015).

Libicki, Martin C., David Senty and Julia Pollak. *Hackers Wanted: An Examination of the Cybersecurity Labor Market.* Labor Report, RAND Corporation, Santa Monica, CA: RAND, 2014.

National Initiative for Cybersecurity Careers and Studies (NICCS). *Cybersecurity Careers.* https://niccs.us-cert.gov/careers/cybersecurity-careers (accessed October 15, 2015).

Cyber Security Minor

Total Credits: 17

CPSC 220: Computer Programing and Problem Solving.
CPSC 225: Software Development Tools.
CPSC 345: Introduction to Computer Security.
CPSC 414: Network Principles and Applications.
MIST 411: Information Security.
CPSC 445: Software Security.
MIST 444: Ethical Hacking.
CPSC 302: Computer Ethics
BUAD 464: Business Ethics
PHIL 225: Practical Ethics

One of the Following Courses

CPSC 445
3-credits
Prereq: CPSC345
or MIST 411

OR

MIST 444
3-credits
Prereq: MIST411
or CPSC345

One of the Following Courses

CPSC 345
3-credits
Prereq: CPSC220

OR

MIST 411
3-credits
Prereq: MIST 201

And

CPSC 414
3-credits
Prereq: CPSC 220,
CPSC 225

Both of the Following Courses

CPSC 220
4-credits

And

CPSC 225
1-credit

And

One of the Following Courses

CPSC 302
3-credits

or

BUAD 464
3-credits

or

PHIL 225
3-credits

UNIVERSITY OF
MARY WASHINGTON
COLLEGE OF BUSINESS

October 23, 2015

Curriculum Committee
College of Arts and Sciences
University of Mary Washington

Dear Members of the Curriculum Committee,

I am writing this letter to support the Department of Computer Science's proposed minor in Security. We understand that two courses from our curriculum will be included as a part of this program, and we intend on offering those courses in the future.

Regards,

Ken Machande
Associate Dean for Faculty

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu

Telephone: (540) 654-1019
Fax: (540) 654-2430
TTY: (540) 654-1104

From: Andrew Marshall (amarsha2)
To: Jeanne Campbell (jcampbe2)
Subject: FW: New Minor and PHIL 225
Date: Thursday, October 29, 2015 10:50:59 AM

From: Craig Vasey (cvasey)
Sent: Thursday, October 29, 2015 10:33 AM
To: Andrew Marshall (amarsha2)
Subject: RE: New Minor and PHIL 225

Hi Andrew

Thanks for letting us know about this. Should not be a problem at all.

Craig R. Vasey
Professor of Philosophy & Chair
Department of Classics, Philosophy, and Religion
1301 College Ave
University of Mary Washington
Fredericksburg VA 22401
540-654-1342

From: Andrew Marshall (amarsha2)
Sent: Thursday, October 29, 2015 8:39 AM
To: Craig Vasey (cvasey)
Cc: Andrew Marshall (amarsha2)
Subject: New Minor and PHIL 225

Hi Craig,
The Department of Computer Science with the COB is planning on proposing a new Information Security Minor.
We would like the student in the minor to take an ethics course and would like to include PHIL 225 as one of the three possible courses students could take to fill the ethics requirement.

I would anticipate a small increase in demand for the class from students in the minor.
However, we are not asking for any increased offerings of PHIL 225.
I want to make sure that won't detrimentally impact the Philosophy department.
Would you be agreeable to us including the course in the minor?

I would be happy to provide you any additional information on the minor if needed.

All the Best,
Andrew

Andrew Marshall
marshall@umw.edu
Assistant Professor of Computer Science
University of Mary Washington
1301 College Ave.