**UNIVERSITY OF MARY WASHINGTON -- NEW COURSE PROPOSAL**

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

<table>
<thead>
<tr>
<th>COLLEGE (check one):</th>
<th>Arts and Sciences</th>
<th>X</th>
<th>Business</th>
<th>Education</th>
</tr>
</thead>
</table>

Proposal Submitted By: Dr. Andrew Marshall  
Date Prepared: September 19, 2014

Course Title: Introduction to Computer Security

Department/discipline and course number*: Computer Science, CPSC345

*This course number must be approved by the Office of the Registrar before the proposal is submitted.

<table>
<thead>
<tr>
<th>Number of credits proposed:</th>
<th>3</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Prerequisites:</th>
<th>(1) CPSC 220 and CPSC 225 or (2) CPSC 340</th>
</tr>
</thead>
</table>

Will this be a **new**, **repeatable** “special topics” course? (Do you want students to be able to take this new course more than once if the topic changes?)

<table>
<thead>
<tr>
<th>NO</th>
<th>X</th>
<th>YES</th>
</tr>
</thead>
</table>

Date of first offering of this **new** course: FALL SEMESTER, year Fall, 2015

Proposed frequency of offering of the course: Once per Year

List the faculty who will likely teach the course: Dr. Andrew Marshall

Are ANY new resources required? NO X YES  
Document in attached impact statement

This new course will be (check all that apply):

- Required in the major
- General Elective
- Elective in the major X General Education**

**AFTER the new course is approved, a separate proposal must be sent to the General Education Committee.

**Catalog Description:**

Prerequisites: (1) CPSC 220 and CPSC 225 or (2) CPSC 340.  
Provides an introduction to computer security.  
The focus is on providing the students a wide overview of current computer security. Topics covered include, but are not limited to, basic cryptography, network security, system security, wireless security and mobile security. In addition, course labs provide a more hands-on, in-depth exploration of specific topics.

**COURSE HISTORY**

<table>
<thead>
<tr>
<th>Course Number and Title of Previous Course</th>
<th>Semester Offered</th>
<th>Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPSC 370Z</td>
<td>Fall 2014</td>
<td>27</td>
</tr>
</tbody>
</table>

X CHECK HERE if the proposed course is to be **equated** with the earlier topics or experimental offerings. This means that students who took the earlier “topics” course will only be able to take the new course if they made a C- grade or lower in the earlier course.

**NOTE:** If the proposed course has not been previously offered as a topics or experimental course, explain in the attached rationale statement why the course should be adopted even though it has not been tried out.
REQUIRED ATTACHMENTS:
1. Rationale Statement (Why is this course needed? What purposes will it serve?)
2. Impact Statement (Provide details about the Library, space, budget, and technology impacts created by adding this new course. Include supporting statements from the Library, IT Department, etc. as needed.)
3. Sample Syllabus

Department Chair Approval: Jennifer Polack
Date: ________

CCC Chair Approval: Dawn S. Bowen
Date: ________

UCC Chair Approval: ________
Date: ________
Rationale Statement
(Why is this course needed? What purposes will it serve?)

Computer security is a fundamental problem in our very connected and network dependent world. One need only look at the recent news to see examples of how poor computer security can have an immediate and devastating effect on businesses and more importantly, individual people. The situation is actually worse than is often seen on the front pages of major news outlets since it's only the big splashy security headlines that get widely reported. Consequently, there is a daily battle in which security professionals are engaged to keep systems secure and information private.

Given this persistent threat, it is likely that students will encounter issues related to computer security in the workforce. In order to produce well-versed computer scientists, it is therefore imperative that we expose our students to the current state of computer security. This knowledge should include not only an overview of the threats, but also an exposure to the tools, methods and best practices for mitigating those threats.

The realization that computer security is an important topic in computer science education is not limited to UMW. The Association for Computing Machinery (ACM), the leading professional organization for computer science professionals, researches and educators, has listed “information assurance and security” as a knowledge area. This is a new knowledge area in the ACM curriculum guidelines due to, as the ACM states, “the world’s critical reliance on information technology and computing”. The ACM advises that there should be at least 3 credit hours at Tier1 (topics should be a required part of every computer science curriculum) and 6 credit hours at Tier2 (topics generally essential in an undergraduate computer science degree), covering topics in the knowledge area. Combined with information assurance and best practices covered in other courses this new course would provide these recommended credit hours for UMW students.

Ultimately, the new security course will provide the recommended exposure to this important area and help produce computer scientists better prepared for the challenging security environment that currently exists. In addition, the course will hopefully inspire some students to pursue a career in the field of computer security; a field that is expanding and in constant need of bright people with new ideas.

Impact Statement
(Provide details about the Library, space, budget, and technology impacts created by adding this new course. Include supporting statements from the Library, IT Department, etc. as needed.)

The college has the equipment and facilities currently on hand needed to teach this course. The course does not require additional staff time from departments other than computer science. Computer Science currently has the faculty required to teach the course. The library has the necessary material to support the course.
Course Description:

- Provide an introduction to computer security.
- Cover a wide range of topics with the goal of providing an overview of different areas of computer security.
- Hands-on practice in a selection of specific topics.
- Prepare the student for further studies in security or entry positions in system security.

WebSite: http://rosemary.umw.edu/~marshall/CPSC370

Grading Policy:

Grading based on the following break down:

- Labs: 40%,
- Midterm: 10%,
- Final: 10%,
- Homework/Readings: 40%.

Letter grade distribution:

- 100-90%: A,
- 89-87%: B+,
- 86-80%: B,
- 79-77%: C+,
- 76-70%: C,
- 69-67%: D+,
- 66-60%: D,
- < 60%: F.

The University provides the opportunity to provide grading feedback midway through the semester. This will take into account your midterm exam, homework and labs submitted up to that point. Any student receiving less than a 65% will receive an unsatisfactory (U) for their mid-semester grade. Students receiving a U should schedule a meeting with me to discuss how we may improve your performance in the class.

Student Conduct:

- Students are expected to attend class when possible and are responsible for the material covered in any class they may miss.
- Legitimate documentation is required for any exam that may be missed.
- If a student knows ahead of time that they cannot make an exam please schedule a meeting with me to discuss alternatives.
• The use of digital recording devices (such as video and audio recording devices, i.e., smartphone) in the classroom must be pre-approved by the instructor.

The Honor Code:

• Please review the Computer Science Department’s Policy regarding academic honesty
  o http://rosemary.umw.edu/CSHonorCode.html
  o Students taking this course are presumed to be aware of the policy.
• For this specific course the instructor authorizes and encourages the following:
  o Students may work together, discuss, compare approaches and in general collaborate on all homework assignments, labs, and readings.
  o However, exams are to be done individually.

Special Guidelines for this Course:

• Students should not practice or use any of the methods discussed in the course on the university's networks or any other network/system where the student has not been given explicit permission from the owner and administrators of that network/system.
• The course will include a special lab and simulation environments where the students may conduct labs and study material for this course.

Disability Policy:

The Office of Disability Services has been designated by the University as the primary office to guide, counsel, and assist students with disabilities.
If you already receive services through the Office of Disability Services and require accommodations for this class, make an appointment with me as soon as possible to discuss your approved accommodations. Please bring your accommodation letter with you to the appointment.
If you have not contacted the Office of Disability Services and need accommodations, their phone number is 540-654-1266. The office is located in Lee Hall, Room 401.

Topics:

• Overview of Computer Security:
  o Overview.
  o Threats and Types of Security.
  o Policies.
• Cryptography:
  o Overview of Cryptography.
  o Symmetric and Public Key.
  o Using Cryptography.
• System Security:
  o Overview of system security.
  o Hardening, firewalls, intrusion detection and logging.
  o Vulnerability analysis and penetration testing.
  o System exploits and prevention.
• WiFi Security:
  o Overview Wifi security.
  o Encryption and protocols.
  o Traffic capture and analysis.
• Web Applications and Security:
  o Overview
  o Vulnerabilities in websites and in browsers.
• Malicious Logic-Viruses, worms and root kits:
  o Overview.
  o Malicious logic detections and defense.
• Additional Topics- We may or may not cover based on available time and student interest.
  o Anonymity: Onion routing (Tor) and other approaches to anonymity on the web.
  o Mobile Phone: Privacy, encryption, malicious logic and other topics on mobile phones.
  o VOIP: Privacy and other topics.

Coursework:
  o Coursework will be divided between labs, readings and a midterm and final exam.
  o Labs will be conducted in either the Windows lab of the computer science department during class period or in the security lab during class period and at specially scheduled times.
  o Readings will be conducted outside class from material provided during class.
  o The midterm and final exam will both be in-class exams.
  o Class participation and discussion is encouraged.