interoffice

MEMORANDUM

DATE: March 25, 2016

TO: Rosemary Drohan

FROM: Antonio Moreira, Ph.D.
Vice Provost for Academic Affairs

SUBJECT: UDC in Cybersecurity Informatics

Attached please find the original proposal for an Upper Division Certificate in Cybersecurity Informatics. For the sake of expediency, I am also sending copies of this information simultaneously to the Faculty Senate, the Academic Planning and Budget Committee and the Undergraduate Council. Please coordinate with Drs. Shin, Walz and McDonough to obtain the endorsement from the shared governance process.

We look forward to receiving the Faculty Senate’s review.

Thank you.

AM:slm
Attachment

Cc: Dr. Sarah Shin, President, Faculty Senate
Dr. Bruce Walz, Chair, APB
Dr. Susan McDonough
Dr. Julia Ross
Dr. Aryya Gangopadhyay
Ms. Beth Wells (w/o attachment)
Proposed New Academic Plan or Name Change to Existing Academic Plan

Required steps in the review and approval process for proposed new academic plans and name changes to existing academic plans vary depending upon a number of factors. The Provost’s Office reviews each concept for a new academic plan or name change in light of UMBC campus governance procedures and USM/MHEC approval guidelines. As a result of this examination, the boxes checked on page 2 of this form reflect the steps that have been identified as required for review of the proposed new academic plan or name change of an existing academic plan shown below and attached.

Concept approved by the Program Concept Group: UDC Cybersecurity Informatics (3/3/14) Date of PCG review: 3/10/14 Date routing sheet sent: 3/10/14

This routing form and process is designed to enable more effective and efficient tracking of documents throughout the review and approval steps, ultimately leading to more timely completion of the process. This is especially important because in many cases MHEC has strict “windows” during which proposals must be submitted.

Instructions:

1. Please do not detach this routing slip from the proposal.

2. Regarding the proposed program acronym, the department proposing the new academic plan is responsible to consult simultaneously by email with Pam Hawley in the Registrar’s Office at moinnis@umbc.edu and Michael Dillon in IRADS at midillon@umbc.edu. Please send the proposed program acronym, type (BA, BS, certificate, etc) and description. If you have no preferred acronym, you can send only the description and degree type. Pam and Michael will respond with an assigned acronym. After this consultation, insert the acronym below: (1) the proposed name of the new academic plan; (2) a formal description of the proposed new academic plan (up to 30 characters); (3) a short description of the proposed new academic plan (up to 10 characters); and (4) a proposed new 4-letter acronym for the proposed new academic plan.1

3. If a new program is proposed, please send an email to Miriam Tillman at mtillman@umbc.edu to inquire whether the Marketing Department in Institutional Advancement has an interest in exploring marketing opportunities associated with this program.

4. The proposal and these routing sheets should be sent to each office indicated on this form, in the order in which each appears on the list.

5. Attach letters of support from all participating departments, assuring capacity in courses, etc.

As you sign your approval (or return it to the prior step for modification), please email Susan Mocko in the Provost’s Office at smocko@umbc.edu, giving the name of the proposal as shown above and the office to which you are sending it next, so that we can keep track of it. If you have questions about the review process, please contact Beth Wells at bwells@umbc.edu, x 58907. Thank you very much for your assistance.

Proposed name of proposed new academic plan: Cybersecurity Informatics

Proposed program acronym:

Proposed formal description of new proposed academic plan (up to 30 characters): Cybersecurity Informatics

Proposed short description of proposed new academic plan (up to 10 characters): CYBE-1NF OR

Proposed change to name of existing academic program: Current program acronym2

Additional instructions for proposal: Follow the instructions in the new program guidelines on the Provost’s website for program type.

Beth Wells
Assistant Vice Provost for Academic Affairs

1 Note that academic plan acronyms are permanent and, once established do not change in the future if the name of the academic plan changes.
interoffice

MEMORANDUM

DATE: March 25, 2016

TO: Rosemary Drohan

FROM: Antonio Moreira, Ph.D.
Vice Provost for Academic Affairs

SUBJECT: UDC in Cybersecurity Informatics

Attached please find the original proposal for an Upper Division Certificate in Cybersecurity Informatics. For the sake of expediency, I am also sending copies of this information simultaneously to the Faculty Senate, the Academic Planning and Budget Committee and the Undergraduate Council. Please coordinate with Drs. Shin, Walz and McDonough to obtain the endorsement from the shared governance process.

We look forward to receiving the Faculty Senate's review.

Thank you.

AM: slm
Attachment

Cc: Dr. Sarah Shin, President, Faculty Senate
    Dr. Bruce Walz, Chair, APB
    Dr. Susan McDonough
    Dr. Julia Ross
    Dr. Aryya Gangopadhyay
    Ms. Beth Wells (w/o attachment)
Proposed New Academic Plan or Name Change to Existing Academic Plan

Required steps in the review and approval process for proposed new academic plans and name changes to existing academic plans vary depending upon a number of factors. The Provost’s Office reviews each concept for a new academic plan or name change in light of UMBC campus governance procedures and USM/MHEC approval guidelines. As a result of this examination, the boxes checked on page 2 of this form reflect the steps that may have been identified as required for review of the proposed new academic plan or name change of an existing academic plan shown below and attached.

Concept approved by the Program Concept Group

Date of PCG review

Date routing sheet sent

This routing form and process is designed to enable more effective and efficient tracking of documents throughout the review and approval steps, ultimately leading to more timely completion of the process. This is especially important because in many cases MHEC has strict “windows” during which proposals must be submitted.

Instructions

Please do not detach this routing slip from the proposal.

2. Regarding the proposed program acronym, the department proposing the new academic plan is responsible to consult simultaneously by email with Pam Hawley in the Registrar’s Office at mcm纳斯@umbc.edu and Michael Dillon in IRADS at m Dillon@umbc.edu. Please send the proposed program acronym, type (BA, BS, certificate, etc.) and description. If you have no preferred acronym, you can send only the description and degree type. Pam and Michael will respond with an assigned acronym. After this consultation, insert the following below: (1) the proposed name of the new academic plan, (2) a formal description of the proposed new academic plan (up to 30 characters), (3) a short description of the proposed new academic plan (up to 10 characters), (4) a proposed new 4-letter acronym for the proposed new academic plan.

3. If a new program is proposed, please send an email to Miriam Tillman at mtillman@umbc.edu to inquire whether the Marketing Department in Institutional Advancement has an interest in exploring marketing opportunities associated with this program.

4. The proposal and these routing sheets should be sent to each office indicated on this form in the order in which each appears on the list.

5. Attach letters of support from all participating departments, assuming capacity in courses, etc.

As you sign your approval or return it to the prior step for modification, please email Susan Mocke in the Provost’s Office at smocke@umbc.edu giving the name of the proposal as shown above and the office to which you are sending it next, so that we can keep track of it. If you have questions about the review process, please contact Beth Wells at bwells@umbc.edu x 58907. Thank you very much for your assistance.

Proposed name of proposed new academic plan: Cybersecurity

Proposed program acronym: CYS

Proposed formal description of new proposed academic plan (up to 30 characters): Cybersecurity

Proposed short description of proposed new academic plan (up to 10 characters): CYBC

Proposed change to name of existing academic program:

Current program acronym:

Additional instructions for proposal:

Follow the instructions in the new program guidelines on the Provost’s website for program type.

Note that academic plan acronyms are permanent and once established do not change in the future if the name of the academic plan changes.

Beth Wells
Assistant Vice Provost for Academic Affairs
Department proposing program must submit the proposal for informal review to the Vice-Provost for Academic Affairs, prior to submitting it for formal review

Department proposing program must develop and get approval for proposed acronym. Follow instruction #2 on Page 1

USM requires that proposals be submitted electronically. Please send an electronic copy of the FINAL version of your proposal to Susan Meole at mcmullins@ummc.edu.

A Letter of Intent is required for this program. The format and directions will be sent to you electronically.

Send this office if checked here

<table>
<thead>
<tr>
<th>Signatures</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informal Review Assistant Vice-Provost for Academic Affairs</td>
<td>Date reviewed</td>
</tr>
<tr>
<td>Department Chair</td>
<td>3/21/16 Date approved</td>
</tr>
<tr>
<td>Vice-President for Administration &amp; Finance</td>
<td>Date budget reviewed</td>
</tr>
<tr>
<td>Vice Provost Professional Education</td>
<td>Date approved</td>
</tr>
<tr>
<td>Dean of Natural &amp; Mathematical Sciences</td>
<td>Date approved</td>
</tr>
<tr>
<td>Dean of Arts Humanities &amp; Social Sciences</td>
<td>Date approved</td>
</tr>
<tr>
<td>Dean of Engineering &amp; IT</td>
<td>Date approved</td>
</tr>
<tr>
<td>Dean of Undergraduate Education</td>
<td>Date approved</td>
</tr>
<tr>
<td>Dean of Graduate Education</td>
<td>Date approved</td>
</tr>
<tr>
<td>Please return proposal &amp; cover sheet at this point to Vice Provost for Academic Affairs</td>
<td>3/21/16 Date Letter of Intent sent to USM</td>
</tr>
<tr>
<td>Chair Undergraduate Council</td>
<td>4/21/16 Date approved</td>
</tr>
<tr>
<td>Chair Graduate Council</td>
<td>Date approved</td>
</tr>
<tr>
<td>Chair Academic Planning &amp; Budget</td>
<td>Date approved</td>
</tr>
<tr>
<td>President Faculty Senate</td>
<td>Date approved</td>
</tr>
<tr>
<td>Please return proposal &amp; cover sheet at this point to Vice Provost for Academic Affairs</td>
<td>Date approved</td>
</tr>
<tr>
<td>Provost</td>
<td></td>
</tr>
<tr>
<td>President</td>
<td>Date approved</td>
</tr>
</tbody>
</table>

University System of Maryland:
Board of Regents
and
Maryland Higher Education Commission for

Target MHEC Window submission date (subject to change):
Proposed Upper-Division Undergraduate Certificate in Cybersecurity Informatics
UMBC Department of Information Systems
Contact person: UDP Carolyn Seaman, cseaman@umbc.edu

The shortage of trained professionals in the cyber industry is well documented. Cybersecurity as a field is very broad, and universities have found it challenging to design effective undergraduate major programs that include the required prerequisite knowledge (in programming, mathematics, databases, and design), a breadth of topics that even begin to cover the cybersecurity area, and any level of depth in specific security-related topics. Thus, we propose to augment our existing undergraduate curriculum in Information Systems, which already contains rigorous technical prerequisites, with additional focus on specific informatics-related cybersecurity skills and topics through an undergraduate certificate program. Certificate students would be required to synthesize new concepts and skills acquired in the courses (in computer security, data mining, software security, and mobile computing) into a final cybersecurity informatics experience.

IS as a discipline focuses on specific approaches to solving technology problems from an organizational and people perspective. Similarly, the educational objectives of this certificate program are to equip students to solve cybersecurity-related problems in the real world, particularly those related to the protection and analysis of information in real organizational contexts. These curricular foci are different from a cybersecurity-related program in other disciplines. Cybersecurity is a very wide umbrella that covers topics and skills in many different areas. Thus, we believe having multiple cybersecurity offerings at UMBC and in the state best serves the needs of students and the industry.

The prerequisites for the core courses in the certificate limit it, except in rare cases, to Information Systems majors. Anecdotally, interest in this certificate among current IS majors is already very high. Interest is fueled by the well-publicized availability of jobs, and the national need for graduates trained in this area, as evidenced by a recent NSF grant awarded to the IS department for this purpose. The NSF grant also funds a number of outreach activities meant to generate interest in this area among current IS majors, community college students, and high school students. We expect that enrollment in the certificate program will come mainly from existing students in the first two years, and partially from new students afterwards.

Proposed curriculum (15 credits total)
Core courses: IS 471 Data Analytics for Cyber Security (3)
               IS 472 Software Security (3)
Experience: IS 478 Cyber Security Senior Project (3) OR
               IS 479 Cyber Security Internship (3)
Electives (choose two – 6 credits):
               IS 427 Introduction to Artificial Intelligence (3)
               IS 428 Data Mining Techniques and Applications (3)
               IS 430 Information Systems and Security (3)
               IS 451U or IS 451M or IS 452 (telecommunications and networking courses) (3)

All courses that are part of the cybersecurity informatics certificate curriculum will be taught by full-time, and in the case of some electives, experienced part-time, IS faculty. Oversight and advising for the certificate program will be the responsibility of the IS Department’s Director of Undergraduate Programs, as is the case with all certificate programs the Department offers. Current departmental staffing is sufficient to cover the certificate.
Department proposing program must submit the proposal for informal review to the Vice-Provost for Academic Affairs. Follow instruction #2 on Page 1 USM requires that proposals be submitted electronically. Please send an electronic copy of the FINAL version of your proposal to Susan Mocko at mocko@umbc.edu.

A Letter of Intent is required for this program. The format and directions will be sent to you electronically.

Please return proposal & cover sheet at this point to:
Vice Provost for Academic Affairs

Chair, Undergraduate Council

Date approved

Chair, Graduate Council

Date approved

Chair, Academic Planning & Budget

Date approved

President, Faculty Senate

Date approved

Please return proposal & cover sheet at this point to:
Vice Provost for Academic Affairs

Provost

Date approved

President

Date approved

University System of Maryland/
Board of Regents

and

Maryland Higher Education Commission for

Target MHEC Window submission date (subject to change) ________________________________________
Proposed Upper-Division Undergraduate Certificate in
Cybersecurity Informatics
UMBC Department of Information Systems
Contact person: UPD Carolyn Seaman, cseaman@umbc.edu

The shortage of trained professionals in the cyber industry is well documented. Cybersecurity as a field is very broad, and universities have found it challenging to design effective undergraduate major programs that include the required prerequisite knowledge (in programming, mathematics, databases, and design), a breadth of topics that even begin to cover the cybersecurity area, and any level of depth in specific security-related topics. Thus, we propose to augment our existing undergraduate curriculum in Information Systems, which already contains rigorous technical prerequisites, with additional focus on specific informatics-related cybersecurity skills and topics through an undergraduate certificate program. Certificate students would be required to synthesize new concepts and skills acquired in the courses (in computer security, data mining, software security, and mobile computing) into a final cybersecurity informatics experience.

IS as a discipline focuses on specific approaches to solving technology problems from an organizational and people perspective. Similarly, the educational objectives of this certificate program are to equip students to solve cybersecurity-related problems in the real world, particularly those related to the protection and analysis of information in real organizational contexts. These curricular foci are different from a cybersecurity-related program in other disciplines. Cybersecurity is a very wide umbrella that covers topics and skills in many different areas. Thus, we believe having multiple cybersecurity offerings at UMBC and in the state best serves the needs of students and the industry.

The prerequisites for the core courses in the certificate limit it, except in rare cases, to Information Systems majors. Anecdotally, interest in this certificate among current IS majors is already very high. Interest is fueled by the well-publicized availability of jobs, and the national need for graduates trained in this area, as evidenced by a recent NSF grant awarded to the IS department for this purpose. The NSF grant also funds a number of outreach activities meant to generate interest in this area among current IS majors, community college students, and high school students. We expect that enrollment in the certificate program will come mainly from existing students in the first two years, and partially from new students afterwards.

Proposed curriculum (15 credits total)
Core courses: IS 471 Data Analytics for Cyber Security (3)
              IS 472 Software Security (3)
Experience:   IS 478 Cyber Security Senior Project (3) OR
              IS 479 Cyber Security Internship (3)
Electives (choose two – 6 credits): IS 427 Introduction to Artificial Intelligence (3)
              IS 428 Data Mining Techniques and Applications (3)
              IS 430 Information Systems and Security (3)
              IS 451U or IS 451M or IS 452 (telecommunications and networking courses) (3)

All courses that are part of the cybersecurity informatics certificate curriculum will be taught by full-time, and in the case of some electives, experienced part-time, IS faculty. Oversight and advising for the certificate program will be the responsibility of the IS Department’s Director of Undergraduate Programs, as is the case with all certificate programs the Department offers. Current departmental staffing is sufficient to cover the certificate.