NOT FOR USE FOR CURRICULAR COURSE CHANGES
REQUEST FOR PROGRAM IMPROVEMENTS

NOTE: Changes to programs may require course changes, which must be processed electronically. Any questions should be directed to Associate Provost David Reinhold at 7-4564 or david.reinhold@wmich.edu

DEPARTMENT: CS and BIS
PROPOSED EFFECTIVE FALL YEAR: 2019

PROPOSED IMPROVEMENTS: Academic Program Proposed Improvements
- New degree*
- New major*
- New curriculum*
- New concentration*
- New certificate*
- New minor*
- Deletion*
- Revised major
- Revised minor
- Admission requirements
- Graduation requirements
- Change in Title
- Transfer

☑ Other (explain*)

** Other: Catalog Language Description Revision and Course Designation Change

Title of degree, curriculum, major, minor, concentration, or certificate: Master of Science in Information Security

Chair, Department Curriculum Committee: [Signature]
Date 11/27/2018

CHECKLIST FOR DEPARTMENT CHAIRS/DIRECTORS
☐ For new programs and other changes that have resource implications, the dean has been consulted.
☐ When appropriate, letters of support from department faculty are attached.
☐ When appropriate, letters of support from other departments in the same college are attached.
☐ The proposal has been reviewed by HIGE for possible implications for international student enrollment.
☒ The proposal is consistent with the departmental assessment plan, and identifies measurable learning outcomes for assessment.
☐ Detailed resource plan is attached where appropriate.
☒ All questions attached have been completed and supporting documents are attached.
☒ The proposal is written and complete as outlined in the Faculty Senate guidelines and the curriculum change guides.

Chair/Director: [Signature]
Date 11/27/18

CHECKLIST FOR COLLEGE CURRICULUM COMMITTEE
☐ The academic quality of the proposal and the faculty involved has been reviewed.
☐ Detailed resource plan is attached where appropriate.
☐ Consistency between the proposal and the relevant catalog language has been confirmed.
☐ The proposal has been reviewed for effect on students transferring from Michigan community colleges. Detailed information on transfer articulation must be included with undergraduate proposals.
☐ Consistency between the proposal and the College and department assessment plans has been confirmed.
☐ Consistency between the proposal and the College and department strategic plans has been confirmed.
☐ All questions attached have been completed and supporting documents are attached.
☐ The proposal is written and complete as outlined in the Faculty Senate guidelines and the curriculum change guides.

Chair, College Curriculum Committee: [Signature]
Date

Revised Sept. 2016. All previous forms are obsolete and should not be used.
1. Explain briefly and clearly the proposed improvement:

We are revising the catalog description to clarify degree requirements and remove references to “tracks” as they do not exist in the M.S. In addition, we are changing appropriate course designations from CIS to CYIS and CS to CYCS in order to match approved course designation changes for the program.

2. Rationale. Give your reason(s) for the proposed improvement.

We have been advised, and agree, that the catalog description for the M.S. degree is not as clear to students as it could be. We have revised the catalog description to note number of credits—rather than percentages—from specific courses that students from either college need to take. In addition, we have removed references to “tracks” as these do not exist in the M.S. degree. They are a remnant of verbiage from the Certificate Program catalog description.

We are changing designations from CIS to CYIS and CS to CYCS in the appropriate courses because this change has been approved under a separate Program Improvement submission. The course designation change delineates Information Security courses from other courses offered by the departments.

3. Effect on other colleges, departments, or programs. If consultation with others is required, attach evidence of consultation and support. If objections have been raised, document the resolution. Demonstrate that the program you propose is not a duplication of an existing one.

No impact on either of the departments or colleges. This is a catalog clarification and a course designation change that has already been discussed among the departments and colleges.

4. Effect on your department’s programs. Show how the proposed change fits with other departmental offerings.

This catalog description change makes it clearer for both students applying to the M.S. degree as well as those in the M.S. program. The course designation change clarifies the courses that count toward the Information Security degree versus other offered degrees and majors.

5. Alignment with college’s and department’s strategic plan, mission, and vision.

Alignment remains the same. This is a cross-disciplinary program designed by both CIS and CS faculty.

6. Effects on enrolled students: Are program conflicts avoided? Will your proposal make it easier or harder for students to meet graduation requirements? Can students complete the program in a reasonable time? Show that you have considered scheduling needs and demands on students’ time.

This catalog description change makes it clearer to M.S. students in terms of which classes they need to take. Students from CEAS need to take a minimum of 18 credits in CYCS classes. Students from HCOB need to take a minimum of 18 credits in CIS/CYIS classes.

The course designation change makes it easier for students to know which courses count toward their degree. In addition, it helps students not in the certificate program know that the courses might not count toward their degree (MBA, MS in CS, etc.).

7. Student or external market demand. What is your anticipated student audience? What evidence of student or market demand or need exists? What is the estimated enrollment? What other factors make your proposal beneficial to students?

The M.S. degree and associated courses have been offered for almost two years as part of the Information Security Graduate Certificate and the M.S. in Information Security.

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Current Catalog Language

Master of Science in Information Security: Computer Information Systems

The Master of Science in Information Security: Computer Information Systems is an interdisciplinary online offering concentrating in the growing field of information security. Two foundation courses, five to six core courses, and two to three elective courses are required to complete the degree.

Students working towards the Master of Science in Information Security: Computer Information Systems must be admitted into the Graduate College. Students must have a bachelor degree in either a technical discipline or an appropriate discipline related to information technology and management. Students with other bachelor degrees and professional experience will also be considered.

Students admitted via the College of Engineering and Applied Sciences specializing in Secure Software and Engineering must take 50% or more of their classes in CS. Students admitted via the Haworth College of business specializing in Information Security Management must take 50% or more of their classes in CIS and will receive an AACSB accredited Master of Science in Information security degree after successfully completing the program requirements.

The Master of Science in Information Security: Computer Information Systems is offered completely online. Students do not need to attend classes at the main or any regional campuses in order to earn the degree. Graduate credit is earned for all passing classes.

Required Courses (30 Credit Hours)

Foundation Courses (6 Credit Hours)

All students complete.

- CS 5710 - Network Security Fundamentals Credits: 3 hours
- CIS 5710 - Information Security Fundamentals Credits: 3 hours

Core Courses

Students must choose and successfully complete at least five of the following Core Courses.

- CS 5730 - Secure System Administration Credits: 3 hours
- CS 5740 - Web Application Security Credits: 3 hours
- CS 5750 - Secure Software Development Credits: 3 hours
- CIS 6710 - Information Assurance and Security Credits: 3 hours
- CIS 6720 - IT Governance and Service Management Credits: 3 hours
- CIS 6730 - Cyberwarfare, Cybercrime, and Digital Forensics Credits: 3 hours
Master of Science in Information Security: Computer Science

The Master of Science in Information Security: Computer Science is an interdisciplinary online offering concentrating in the growing field of information security. Two foundation courses, five to six core courses, and two to three elective courses are required to complete the degree.

Students working towards the Master of Science in Information Security: Computer Science must be admitted into the Graduate College. Students must have a bachelor degree in either a technical discipline or an appropriate discipline related to information technology and management. Students with other bachelor degrees and professional experience will also be considered.

Students admitted via the College of Engineering and Applied Sciences specializing in Secure Software and Engineering must take 50% or more of their classes in CS. Students admitted via the Haworth College of business specializing in Information Security Management must take 50% or more of their classes in CIS and will receive an AACSB accredited Master of Science in Information security degree after successfully completing the program requirements.

The Master of Science in Information Security: Computer Science is offered completely online. Students do not need to attend classes at the main or any regional campuses in order to earn the degree. Graduate credit is earned for all passing classes.

Required Courses (30 Credit Hours)

Foundation Courses (6 Credit Hours)

All students complete.

- CS 5710 - Network Security Fundamentals Credits: 3 hours
- CIS 5710 - Information Security Fundamentals Credits: 3 hours

Core Courses

Students must choose and successfully complete at least five of the following Core Courses.

- CS 5730 - Secure System Administration Credits: 3 hours
- CS 5740 - Web Application Security Credits: 3 hours
- CS 5750 - Secure Software Development Credits: 3 hours
- CIS 6710 - Information Assurance and Security Credits: 3 hours
- CIS 6720 - IT Governance and Service Management Credits: 3 hours
- CIS 6730 - Cyberwarfare, Cybercrime, and Digital Forensics Credits: 3 hours

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Proposed Catalog Language

Master of Science in Information Security: Computer Information Systems

The Master of Science in Information Security: Computer Information Systems is an interdisciplinary online offering concentrating in the growing field of information security. Two foundation courses, five to six core courses, and two to three elective courses are required to complete the degree.

Students working towards the Master of Science in Information Security: Computer Information Systems must be admitted into the Graduate College. Students must have a bachelor’s degree in either a technical discipline or an appropriate discipline related to information technology and management. Students with other bachelor’s degrees and professional experience will also be considered.

Students admitted via the College of Engineering and Applied Sciences must take at least 18 credits of their classes in the CYCS courses listed below. Students admitted via the Haworth College of Business must take at least 18 credits of their classes in the CIS/CYIS courses listed below.

The Master of Science in Information Security: Computer Information Systems is offered completely online. Students do not need to attend classes at the main or any regional campuses in order to earn the degree. Graduate credit is earned for all passing classes.

Required Courses (30 Credit Hours)

Foundation Courses (6 Credit Hours)

Students must successfully complete the following two courses.

- CIS 5710 - Information Security Fundamentals Credits: 3 hours
- CYCS 5710 - Network Security Fundamentals Credits: 3 hours

Core Courses

Students must choose and successfully complete at least five of the following Core Courses.

- CYCS 5730 - Secure System Administration Credits: 3 hours
- CYCS 5740 - Web Application Security Credits: 3 hours
- CYCS 5750 - Secure Software Development Credits: 3 hours
- CYIS 6710 - Information Assurance and Security Credits: 3 hours
- CYIS 6720 - IT Governance and Service Management Credits: 3 hours
- CYIS 6730 - Cyberwarfare, Cybercrime, and Digital Forensics Credits: 3 hours
Master of Science in Information Security: Computer Science

The Master of Science in Information Security: Computer Science is an interdisciplinary online offering concentrating in the growing field of information security. Two foundation courses, five to six core courses, and two to three elective courses are required to complete the degree.

Students working towards the Master of Science in Information Security: Computer Science must be admitted into the Graduate College. Students must have a bachelor's degree in either a technical discipline or an appropriate discipline related to information technology and management. Students with other bachelor's degrees and professional experience will also be considered.

Students admitted via the College of Engineering and Applied Sciences must take at least 18 credits of their classes in the CYCS courses listed below. Students admitted via the Haworth College of Business must take at least 18 credits of their classes in the CIS/CYIS courses listed below.

The Master of Science in Information Security: Computer Science is offered completely online. Students do not need to attend classes at the main or any regional campuses in order to earn the degree. Graduate credit is earned for all passing classes.

Required Courses (30 Credit Hours)

Foundation Courses (6 Credit Hours)

Students must successfully complete the following two courses.

- CIS 5710 - Information Security Fundamentals Credits: 3 hours
- CYCS 5710 - Network Security Fundamentals Credits: 3 hours

Core Courses

Students must choose and successfully complete at least five of the following Core Courses.

- CYCS 5730 - Secure System Administration Credits: 3 hours
- CYCS 5740 - Web Application Security Credits: 3 hours
- CYCS 5750 - Secure Software Development Credits: 3 hours
- CYIS 6710 - Information Assurance and Security Credits: 3 hours
- CYIS 6720 - IT Governance and Service Management Credits: 3 hours
- CYIS 6730 - Cyberwarfare, Cybercrime, and Digital Forensics Credits: 3 hours