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: 2020

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:

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

Chair, Department Curriculum Committee: [Signature] Date 10/8/19

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.
☐ When appropriate, letters of support from other college deans, whose programs/courses may be affected by the change, 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 10/8/19

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: Date

Revised Sept. 2018. All previous forms are obsolete and should not be used.
NOT FOR USE FOR CURRICULAR COURSE CHANGES  
REQUEST FOR PROGRAM IMPROVEMENTS

CHECKLIST FOR COLLEGE DEANS

☐ For new programs and proposed program deletions, the provost has been consulted.
☐ For new programs, letter of support from University Libraries Dean indicating library resource requirements have been met.
☐ When appropriate, letters of support from other college faculty and/or chairs are attached.
☐ When appropriate, letters of support from other college deans, whose programs/courses may be affected by the change, are attached.
☐ The proposal has been reviewed for implications for accreditation, certification, or licensure.
☐ 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.

Dean: ___________________________ Date: ___________________________

FOR PROPOSALS REQUIRING REVIEW BY:
GSC/USC; EPGC, GRADUATE COLLEGE, and/or FACULTY SENATE EXECUTIVE BOARD

☐ Return to Dean
☐ Forward to:

Curriculum Manager: ___________________________ Date: ___________________________

*needs review by

☐ Approve ☐ Disapprove
Chair, GSC/USC: ___________________________ Date: ___________________________

☐ Approve ☐ Disapprove
Chair, EPGC: ___________________________ Date: ___________________________

☐ Approve ☐ Disapprove
Graduate College Dean: ___________________________ Date: ___________________________

☐ Approve ☐ Disapprove
Faculty Senate President: ___________________________ Date: ___________________________

☐ Approve ☐ Disapprove
*needs review by

Provost: ___________________________ Date: ___________________________

Revised Sept. 2018. All previous forms are obsolete and should not be used.
NOT FOR USE FOR CURRICULAR COURSE CHANGES
REQUEST FOR PROGRAM IMPROVEMENTS

1. Explain briefly and clearly the proposed improvement:

We are changing the program name from the M.S. in Information Security to the M.S. in Cybersecurity.

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

Changing the M.S. from "Information Security" to "Cybersecurity" aligns with degree naming conventions put forth by two major accreditation bodies.

The NSA/DHS Centers of Academic Excellence (CAE) use the term "Cybersecurity" for all of their accredited programs (which we are working toward).

ABET (Accreditation Board for Engineering and Technology) uses the Cybersecurity designation for its current approved undergraduate curriculum and is examining graduate curriculum as well using the designation Cybersecurity.

Finally, we have a B.S. in Cybersecurity coming online soon. The M.S. name designation change will link these two degrees together as a coherent unit.

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 only a program name 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.

There is no impact on either department's programs. All courses, content, and curriculum integrations remain the same.

This program name change makes the M.S. focus clearer not only for students in the M.S. program but also employers looking for graduates in Cybersecurity.

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

Alignment remains the same. These 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 program name change makes the M.S. degree focus clearer to students. No other changes in the actual course work or class offerings change because of the program name change. Students can still complete this degree completely online within 20 months.

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. This name change, along with the associated program improvement form to change the Graduate Certificate name to the same, will increase student demand. Most employers understand and look for the designation of "Cybersecurity" with graduates.

Revised Sept. 2018. All previous forms are obsolete and should not be used.
8. Effects on resources. Explain how your proposal would affect department and University resources, including faculty, equipment, space, technology, and library holdings. If proposing a new program, include a letter and/or email of support from the university libraries affirming that the library resource issues have been reviewed. Tell how you will staff additions to the program. If more advising will be needed, how will you provide for it? What will be the initial one-time costs and the ongoing base-funding costs for the proposed program? (Attach additional pages, as necessary.)

No additional long-term impact. This program name change does not change any existing resources requirements or require new resources. Once approved we will work to make changes on various Web pages and fliers to reflect the new name.

9. List the learning outcomes for the revised or proposed major, minor, or concentration. The department will use these outcomes for future assessments of the program.

These are already in place and being used from the previous approved M.S. degree paperwork.

10. Describe how this change is a response to assessment outcomes that are part of a department or college assessment plan or informal assessment activities.

This program name change is in response to a need to align the program name with accreditation agency (ABET) and external industry certification (NSA/DHS). By changing the name to "Cybersecurity" we will reflect the designations used by accreditation and assessment organizations.

The program name change will also align our Graduate Certificate and planning B.S. in Cybersecurity naming conventions.

11. (Undergraduate proposals only) Describe in detail how this change affects transfer articulation for Michigan community colleges. For new majors or minors, describe transfer guidelines to be developed with Michigan community colleges. For revisions to majors or minors, describe necessary revisions to Michigan community college guidelines. Department chairs should seek assistance from college advising directors or from the admissions office in completing this section.

N/A

12. Please offer both "Current Catalog Language" and "Proposed Catalog Language" if there is to be a change in the catalog description for a given program. For the "current" language, please copy and paste relevant language from the most current catalog and for the "proposed" language, please share the exact proposed new catalog language. As possible, bold or otherwise note the key changes in the new proposed catalog language.
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'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

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Elective Courses

Students completing all six of the Core Courses above must choose and successfully complete two of the following Elective Courses. Students completing five of the Core Courses above must choose and successfully complete three of the following Elective Courses.

- CYCS 6730 - Installation Hardening Credits: 3 hours
- CYCS 6740 - Wireless Ethical Hacking Credits: 3 hours
- CYCS 6750 - Network Penetration Testing Credits: 3 hours
- CIS 6300 - Business Data Management Credits: 3 hours
- CIS 6620 - Business Project Management Credits: 3 hours
- CIS 6660 - Information Security Operations Management 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

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Elective Courses

Students completing all six of the Core Courses above must choose and successfully complete two of the following Elective Courses. Students completing five of the Core Courses above must choose and successfully complete three of the following Elective Courses.

- CYCS 6730 - Installation Hardening Credits: 3 hours
- CYCS 6740 - Wireless Ethical Hacking Credits: 3 hours
- CYCS 6750 - Network Penetration Testing Credits: 3 hours
- CIS 6300 - Business Data Management Credits: 3 hours
- CIS 6620 - Business Project Management Credits: 3 hours
- CIS 6660 - Information Security Operations Management Credits: 3 hours
Proposed Catalog Language

Master of Science in Cybersecurity: Computer Information Systems

The Master of Science in Cybersecurity: 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 Cybersecurity: 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 Cybersecurity: 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.

- CYIS 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

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Elective Courses

Students completing all six of the Core Courses above must choose and successfully complete two of the following Elective Courses. Students completing five of the Core Courses above must choose and successfully complete three of the following Elective Courses.

- CYCS 6730 - Installation Hardening Credits: 3 hours
- CYCS 6740 - Wireless Ethical Hacking Credits: 3 hours
- CYCS 6750 - Network Penetration Testing Credits: 3 hours
- CIS 6300 - Business Data Management Credits: 3 hours
- CIS 6620 - Business Project Management Credits: 3 hours
- CIS 6660 - Information Security Operations Management Credits: 3 hours

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Master of Science in Cybersecurity: Computer Science

The Master of Science in Cybersecurity: 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 Cybersecurity: 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 Cybersecurity: 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.

- **CVIS 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

Revised Sept. 2018. All previous forms are obsolete and should not be used.
Elective Courses

Students completing all six of the Core Courses above must choose and successfully complete two of the following Elective Courses. Students completing five of the Core Courses above must choose and successfully complete three of the following Elective Courses.

- CYCS 6730 - Installation Hardening Credits: 3 hours
- CYCS 6740 - Wireless Ethical Hacking Credits: 3 hours
- CYCS 6750 - Network Penetration Testing Credits: 3 hours
- CIS 6300 - Business Data Management Credits: 3 hours
- CIS 6620 - Business Project Management Credits: 3 hours
- CIS 6660 - Information Security Operations Management Credits: 3 hours