



DEPARTMENT OF
HIGHER EDUCATION &
WORKFORCE DEVELOPMENT

New Program Report

Date Submitted:

08/04/2023

Institution

Maryville University of Saint Louis

Site Information

Implementation Date:

9/1/2023 12:00:00 AM

Added Site(s):

Selected Site(s):

Maryville University of Saint Louis, 650 Maryville University Drive, St. Louis, MO, 63141

CIP Information

CIP Code:

290207

CIP Description:

A program that focuses on the technological and operation aspects of information warfare, including cyber attack and cyber defense. Includes instruction in computer and network security, cryptography, computer forensics, systems security engineering, software applications, threat and vulnerability assessment, wireless networks and satellite communications, tactical and strategic planning, legal and ethical issues, and cyber warfare systems development and acquisition.

CIP Program Title:

Cyber/Electronic Operations and Warfare

Institution Program Title:

Secure System Design

Degree Level/Type

Degree Level:

Master Degree

Degree Type:

Master of Science

Options Added:

Collaborative Program:

N

Mode of Delivery

Current Mode of Delivery

Online

Student Preparation

Special Admissions Procedure or Student Qualifications required:

No special admissions requirements.



DEPARTMENT OF
HIGHER EDUCATION &
WORKFORCE DEVELOPMENT

New Program Report

Specific Population Characteristics to be served:
Corporate partnership students only.

Faculty Characteristics

Special Requirements for Assignment of Teaching for this Degree/Certificate:
Terminal degree in cybersecurity, system architecture, or other related field preferred. Masters degree in related field in addition to 5+ years of experience required.

Estimate Percentage of Credit Hours that will be assigned to full time faculty:
0

Expectations for professional activities, special student contact, teaching/learning innovation:
N/A

Student Enrollment Projections Year One-Five

Year 1	Full Time: 2	Part Time: 20	
Year 2	Full Time: 3	Part Time: 30	
Year 3	Full Time: 4	Part Time: 40	Number of Graduates: 40
Year 4	Full Time: 5	Part Time: 50	
Year 5	Full Time: 5	Part Time: 50	Number of Graduates: 50

Percentage Statement:
n/a

Program Accreditation

Institutional Plans for Accreditation:
Program will serve a targeted student population within a corporation; as such, it does not meet ACBSP requirements for accreditation.

Program Structure

Total Credits:
30

Residency Requirements:
n/a

General Education Total Credits:
0

Major Requirements Total Credits:
30

Course(s) Added

COURSE NUMBER	CREDITS	COURSE TITLE
SSD 610	3	Development Cybersecurity Standards & Risk
SSD 640	3	Information Security Architecture
SSD 660	3	Security Architecture



DEPARTMENT OF
HIGHER EDUCATION &
WORKFORCE DEVELOPMENT

New Program Report

SSD 650	3	Cryptography & Protocols
SSD 630	3	Security Assurance
SSD 600	3	Secure Software Development
SSD 620	3	Practical Cryptography

Free Elective Credits:

0

Internship or other Capstone Experience:

N/A

Assurances

I certify that the program will not unnecessarily duplicate an existing program of another Missouri institution in accordance with 6 CSR 10-4.010, subsection (9)(C) Submission of Academic Information, Data and New Programs.

I certify that the program will build upon existing programs and faculty expertise.

I certify that the institution has conducted research on the feasibility of the proposal and it is likely the program will be successful. Institutions' decision to implement a program shall be based upon demand and/or need for the program in terms of meeting present and future needs of the locale, state, and nation based upon societal needs, and/or student needs.

Contact Information

First and Last Name: SUE
HENDERSON

Email: shenderson@maryvill.edu

Phone: 314-529-9640

Simon School of Business New Program Overview



Program: MS in Secure System Design

Program Description:

The MS in Secure System Design program is a stackable certificate graduate degree that leverages 3 distinct certificates, Systems Architecture Security, Secure Software Development, and AI in Cybersecurity. This customized program, requisitioned by MasterCard specifically for its employees, is designed to equip students with the knowledge and skills needed to develop secure digital systems and platforms. Coursework offers access to industry experts and cutting-edge content to help students explore cryptography, AI-enhanced cybersecurity, and the use of machine learning algorithms in the analysis and processing of encrypted data.

Learning Outcomes:

- **Design Secure IT Systems and Develop Secure Software:** Students will acquire the skills to design secure Information Technology systems, apply secure software development principles, and integrate cybersecurity measures throughout the lifecycle of systems and software development.
- **Apply Cryptography in Various Contexts:** Students will develop in-depth knowledge of cryptographic algorithms and will be able to correctly assess and apply different types of cryptography in systems architecture, software development, and AI-driven cybersecurity solutions.
- **Leverage AI in Cybersecurity Measures:** Students will gain a deep understanding of how artificial intelligence can be utilized to enhance cybersecurity measures, identify potential threats, and mitigate risks, especially within complex digital environments and financial technologies.
- **Ensure Quality and Security in Software Development:** Students will understand how to maintain the quality assurance of secure software, ensuring that security measures do not compromise the functionality, performance, or reliability of the software systems they develop.
- **Adapt to Evolving Cybersecurity Threats:** Given the rapidly evolving nature of cybersecurity threats, students will have the capacity to adapt their knowledge and skills to new threats, continuously updating and improving the security of IT systems, software, and AI-driven cybersecurity solutions.

Stackable Certificate Graduate Program Outline Option 1	
Certificate in Secure Software Development (12 Credit Hours)	SSD 600 Secure Software Development * SSD 610 Development Cybersecurity Standards & Risk SSD 620 Practical Cryptography SSD 630 Security Assurance
Certificate in Systems Architecture Security (12 Credit Hours)	SSD 600 Secure Software Development * SSD 640 Information Security Architecture SSD 650 Cryptography & Protocols SSD 660 Security Architecture
MS in Secure System Design (30 Credit Hours)	SSD 600 Secure Software Development SSD 610 Development Cybersecurity Standards & Risk SSD 620 Practical Cryptography SSD 630 Security Assurance SSD 640 Information Security Architecture SSD 650 Cryptography & Protocols SSD 660 Security Architecture

	+ 3 Graduate Electives
* SSD 600 is part of both certificates.	

Stackable Certificate Graduate Program Outline Option 2	
Certificate in Secure Software Development (12 Credit Hours)	SSD 600 Secure Software Development * SSD 610 Development Cybersecurity Standards & Risk SSD 620 Practical Cryptography SSD 630 Security Assurance
Certificate in Systems Architecture Security (12 Credit Hours)	SSD 600 Secure Software Development * SSD 640 Information Security Architecture SSD 650 Cryptography & Protocols SSD 660 Security Architecture
Certificate in AI in Cybersecurity (12 Credit Hours)	SSD 600 Secure Software Development * SSD 670 Fundamentals of AI in Cybersecurity SSD 680 AI-Powered Cryptography SSD 690 AI in Detecting and Mitigating Cyber Attacks
MS in Secure System Design (30 Credit Hours)	SSD 600 Secure Software Development SSD 610 Development Cybersecurity Standards & Risk SSD 620 Practical Cryptography SSD 630 Security Assurance SSD 640 Information Security Architecture SSD 650 Cryptography & Protocols SSD 660 Security Architecture SSD 670 Fundamentals of AI in Cybersecurity SSD 680 AI-Powered Cryptography SSD 690 AI in Detecting and Mitigating Cyber Attacks
* SSD 600 is part of each certificate.	