Information Technology Advisory Meeting
Fall 2026 Agenda
9/15/2026 at 6:30 pm
Zoom Meeting or M State B142

Agenda for Fall 2026

- MSCTC/M State welcome and updates
  - Additions/approval of agenda
  - Introductions and membership list updates
- Discussion of Industry Trends
  - Given AI, what are the expectations of new hires?
  - What is the worst technology currently on your mind?
  - What is the best technology holding your attention?
  - What technology/function should M State be teaching?
- Business to Business presentation – Marty
- Programs Updates
  - AI Certificate
    - Program Updates
  - Computer Programming
    - Programs Updates
  - Cybersecurity - AAS
    - Programs Updates
    - Replacement of Cisco 2 with AI class
    - Update Program Outcomes
    - Additional information at the end of this document
  - Cybersecurity-Certificate
    - Programs Updates
    - Replacement of Cisco 2 with AI class
    - Update Program Outcomes
    - Additional information at the end of this document
  - Cybersecurity – AS
    - New Program
    - Course Equivalency questions
    - Program Outcomes
    - Potential class changes (Page 10 of this document)
    - Additional information at the end of this document
  - Information Technology – AS
    - Programs Updates
    - Add discrete math class
    - Update Program Outcomes
    - Additional information at the end of this document
  - CCDC Update
    - Competition: January 30, 2027
- Program Needs
  - Partnerships
  - Equipment
  - Recruitment
  - This is a call for Internships and entry-level job opportunities for M State students.
- College update
- Other
- Next Meeting Date

Actions Items

Advisory Member Functions (MSCTC Advisory Committee Guide)

- Identify specific subject areas of program inclusion
- Prioritizing the recommended subject areas
- Specifying appropriate program content level
- Reviewing program outcomes on an ongoing basis
- Assessment of program quality
- Specifying appropriate foundational skill standards for local needs
- Identifying general education and related technical skills needed by graduates
- Recommending equipment to support the program content

Discrete Math

Minnesota State University Moorhead
MATH 210: Concepts from Discrete Mathematics
A. COURSE DESCRIPTION
Credits: 3
Lecture Hours/Week: 5

Prerequisites:
This course requires any of these four prerequisite categories
1. MATH 127 - College Algebra Or
2. MATH 127L - College Algebra with Lab Or
3. MSUM Math Above MATH 127L Or
4. A score of 1 on test Transfer Equivalent to MATH 127
Corequisites: None

MnTC Goals: Goal 04 - Mathematical/Logical Reasoning
Logic and truth tables, sets, mathematical induction, graphs, trees, and related topicsdiscrete mathematics. MnTC Goal 4.
B. COURSE EFFECTIVE DATES: 02/01/2015 - Present

C. OUTLINE OF MAJOR CONTENT AREAS
1. Euler and Hamilton circuits and shortest path problems
2. Graph isomorphisms and connectivity
3. Graph models and terminology
4. Mathematical induction
5. Predicates and quantifiers, including nested quantifiers
6. Propositional equivalencies
7. Propositional logic and truth tables
8. Sets and set operations
9. Trees, tree traversal, and spanning trees

D. LEARNING OUTCOMES (General)
1. Solve problems using basic graph theory.
2. Model applied problems with graphs or trees.
3. Know the basics of set theory.
4. Determine the truth of a compound proposition using a truth table.
5. Analyze logical statements.
6. Be able to do proofs using mathematical induction.
7. Be able to compute with binary numbers.

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies
Goal 04 - Mathematical/Logical Reasoning
1. Illustrate historical and contemporary applications of mathematical/logical systems.
2. Clearly express mathematical/logical ideas in writing.
3. Explain what constitutes a valid mathematical/logical argument(proof).
4. Apply higher-order problem-solving and/or modeling strategies.

Cisco 2 – Survey of Artificial Intelligence Chart

Cisco 2 – CPTR 1118
Course Number
CPTR1118
Credits
Lecture: 2 Lab: 1 OJT: 0

Description
This course covers the architecture, components and operations of routers and switches in small networks and introduces wireless local area networks (WLANs) and security concepts. Students learn how to configure and troubleshoot routers and switches for advanced functionality using security best practices and resolve common issues with protocols in both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) networks.

Requisites
Prerequisites
CourseCPTR1108

1. * Can be taken as a Prerequisite or Corequisite.

Competencies

2. Configure virtual local area networks (VLANs) and Inter-VLAN routing applying security best practices.
3. Troubleshoot inter-VLAN routing on Layer 3 devices.
4. Configure redundancy on a switched network using Spanning-Tree Protocol (STP) and EtherChannel.
5. Troubleshoot EtherChannel on switched networks.
6. Explain how to support available and reliable networks using dynamic addressing and first-hop redundancy protocols.
7. Configure dynamic address allocation in Internet Protocol Version 6 (IPv6) networks.
8. Configure wireless local area networks using wireless local communication (WLC) and layer 2 (L2) security best practices.
9. Configure switch security to mitigate Local Area Network (LAN) attacks.
10. Configure Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) static routing on routers.

Survey of Artificial Intelligence - CPTR1011
Course Number
CPTR1011
Credits
Lecture: 2 Lab: 1 OJT: 0

Description
This course provides an introduction to artificial intelligence (AI), machine learning (ML) and deep learning (DL). Students explore foundational concepts, real-world applications and ethical implications of AI technologies. Through hands-on labs using Python, students learn how to prepare data, build simple ML models, evaluate performance and experiment with neural networks, computer vision and natural language processing. The course concludes with a final project in which students develop and present a simple AI application.

Requisites
* Can be taken as a Prerequisite or Corequisite.

Competencies

1. Explain artificial intelligence, machine learning and deep learning.
2. Identify real-world applications of artificial intelligence in healthcare, education, transportation and finance.
3. Use Python libraries (NumPy, Pandas, scikit-learn, TensorFlow/Keras) to build machine learning models.
4. Implement regression, classification and clustering algorithms.
5. Apply evaluation metrics such as accuracy, precision, recall and F1 score.
6. Build a simple neural network for classification.
7. Experiment with computer vision and natural language processing tasks using modern tools.
8. Explain how generative artificial intelligence models, such as generative pre-trained and bidirectional encoder representation transformers, work at a high level.
9. Critically analyze ethical issues related to artificial intelligence and algorithmic bias.
10. Design and present an artificial intelligence mini-project addressing a real-world problem.

CISCO 1 - CPTR1108
Course Number
CPTR1108
Credits
Lecture: 1 Lab: 2 OJT: 0

Description
This is an introduction to networks course that covers the architecture, structure, functions and components of the Internet and other computer networks. Students achieve a basic understanding of how networks operate while building simple local area networks (LANs). Students perform basic configurations for routers and switches and implement Internet Protocol.

Requisites
* Can be taken as a Prerequisite or Corequisite.

Competencies

1. Explain how physical and data link layer protocols support the operation of Ethernet in a switched network.
2. Explain how the upper layers of the Open Standards Interconnect (OSI) model support network applications.
3. Configure switches and end devices to provide access to local and remote network resources.
4. Configure routers to enable end-to-end connectivity between remote devices.
5. Explain Internet Protocol addressing and subnetting.
6. Create Internet Protocol version 4 and Internet Protocol version 6 addressing schemes and verify network connectivity between devices.
7. Configure a small network with security best practices.
8. Troubleshoot connectivity in a small network.

Cybersecurity-AAS Program Outcomes

Current Program Outcomes

1. Use mechanisms available in an operating system to control access to resources.
2. Configure infrastructure server roles.
3. Investigate various countermeasures and security controls to minimize risk and exposure.
4. Support the ethical responsibility of ensuring software correctness, reliability and safety.
5. Illustrate, through examples, the concepts of risks, threats, vulnerabilities, attack vectors and exploits, noting there is no such thing as a perfect security.
6. Analyze known security incidents, including social engineering and physical security incidents, to trace and document the steps in the incidents.
7. Develop technical artifacts.
8. Examine ethical issues related to cybersecurity.
9. Write a companywide security policy.
10. Communicate effectively and efficiently with clients, users and peers.
11. Design and build virtual computing environments.
12. Use a variety of ciphers to encrypt plaintext into ciphertext.
13. Construct input validation and data sanitization in applications, considering adversarial control of the input channel.

.

Proposed Program Outcomes

1: Apply configuration mechanisms, administrative commands, and account security structures to manage permissions, access vectors, and fault-tolerance
2: Configure, secure, and manage enterprise services
3: Design, deploy, and evaluate network-level defenses, including packet-filtering firewalls, proxy environments, and cryptographic controls to mitigate exposure and thwart data transit exploits
4: Write, debug, and test robust administrative scripts and application code that apply secure programming techniques, logic parameters, and strict input validation to mitigate execution-tier vulnerabilities
5: Model, evaluate, and investigate cyber threats and security breaches through active network reconnaissance, controlled network attack simulation, and system audit logging
6: Implement technical solutions meeting appropriate legal compliance, data privacy regulations, and societal impact considerations
8: Translate technical forensics, network diagrams, vulnerability matrices, and audit summaries into accurate professional documentation and logical stakeholder presentations
9: Manage comprehensive information security policies that integrate privacy laws, personnel security practices, and ethics

Cybersecurity-Certificate Program Outcomes

Current Program Outcomes

1. Analyze known security incidents to trace and document the steps in the incident.
2. Use mechanisms available in an operating system to control access to resources.
3. Construct input validation.
4. Install and configure firewall rules based on business policies.
5. Investigate various countermeasures and security controls to minimize risk and exposure.
6. Examine ethical issues related to cybersecurity.
7. Demonstrate the use of proper SQL commands to retrieve specific data from a database.
8. Use protocol analyzers to identify information encapsulated in a data packet.
9. Write scripts to perform specific functions within a host and networked computing environment.

Proposed Program Outcomes

1: Apply configuration mechanisms, administrative utilities, and credential management across desktop and server operating systems to govern permissions, access vectors, and fault-tolerant server processes.
2: Design, deploy, and monitor network-level security controls, including firewalls and proxies, while inspecting communication streams and system log files to track anomalies
3: Model cyber threats, execute controlled network reconnaissance, and reconstruct security breaches to accurately document exploit vectors and operational business impacts
4: Analyze, write, and document programming logic and defensive administration scripts, utilizing proper syntax and structure to prevent standard execution vulnerabilities
5: Formulate security policies that integrate personnel safety practices, evaluate ethical choices, and establish structured self-remediation strategies to pursue industry-recognized credentials

Information Technology-AS Program Outcomes

Current Program Outcomes

1. Apply current technical practices in the core information technologies.
2. Identify the requirements to provide effective solutions for organizations or individuals.
3. Identify effective IT-based solutions.
4. Evaluate current and emerging technologies.
5. Identify the impact of technology on individuals, organizations and society, including ethical, legal and policy issues.
6. Demonstrate an understanding of best practices and standards.
7. Demonstrate independent problem-solving skills.
8. Collaborate in teams to accomplish a common goal.
9. Communicate effectively and efficiently with clients, users and peers.
10. Recognize the need for continued learning throughout one's career.

Proposed Program Outcomes

1: Apply current technical best practices, configurations, and administrative commands across core information technologies, including networking, operating systems, and computer hardware.
2: Identify, analyze, and document user and organizational requirements to design and deploy effective, tailored computing solutions.
3: Design, implement, and troubleshoot scalable internetwork addressing schemes, switching, and routing topologies to support local and remote communications.
4: Evaluate, implement, and maintain security technologies, controls, and administrative policies to safeguard information assets, maintain data integrity, and mitigate digital threats.
5: Design, develop, test, and debug secure code and automation scripts utilizing standard logic, structured data environments, and platform-appropriate programming languages.
6: Perform proactive professional development.
7: Communicate technical concepts clearly, accurately, and efficiently in written and oral formats with clients, end-users, team members, and stakeholders.
8: Collaborate effectively within diverse, multidisciplinary teams using version control, collaborative
9: Implement technical solutions meeting appropriate legal compliance, data privacy regulations, and societal impact considerations.

Cybersecurity-AS Proposal

Current Program Outcomes

1. Analyze known security incidents to trace and document the steps in the incident.
2. Use mechanisms available in an operating system to control access to resources.
3. Construct input validation.
4. Install and configure firewall rules based on business policies.
5. Investigate various countermeasures and security controls to minimize risk and exposure.
6. Examine ethical issues related to cybersecurity.
7. Demonstrate the use of proper SQL commands to retrieve specific data from a database.
8. Use protocol analyzers to identify information encapsulated in a data packet.
9. Write scripts to perform specific functions within a host and networked computing environment.

Proposed Program Outcomes

1. Apply configuration mechanisms, administrative utilities, and credential management across desktop and server operating systems to govern permissions, access vectors, and fault-tolerant server processes.
2. Design, deploy, and monitor network-level security controls, including firewalls and proxies, while inspecting communication streams and system log files to track anomalies.
3. Model cyber threats, execute controlled network reconnaissance, and reconstruct security breaches to accurately document exploit vectors and operational business impacts.
4. Analyze, write, and document programming logic and defensive administration scripts, utilizing proper syntax and structure to prevent standard execution vulnerabilities.
5. Formulate security policies that integrate personnel safety practices, evaluate ethical choices, and establish structured self-remediation strategies to pursue industry-recognized credentials.

Fundamentals of Information Technology Security Comparison
Can the M State CSEC 1110 be modified to fulfill the CSIS 362 requirements?

CSIS 362: Cybersecurity Fundamentals
Credits: 3
Lecture Hours/Week: 3
Lab Hours/Week: 0

This course will provide students with a high-level introduction to the fundamental concepts behind cybersecurity, basic information about the threats that may be present in the cyber realm and a basic understanding of how mathematical logic can be applied to the design of secure systems.

OUTLINE OF MAJOR CONTENT AREAS
1. Cybersecurity Foundations
2. Formal Methods

LEARNING OUTCOMES (General)
1. Demonstrate an understanding of the fundamental concepts of the cybersecurity discipline, used to provide system security.
2. Explain potential system attacks and their characteristics.
3. Describe and identify the bad actors in cyberspace and analyze their resources, capabilities, techniques and motivations.
4. Describe cyber defense tools and methodologies, and apply cyber defense methods to prepare a system to fend off attacks.
5. Describe appropriate measures to be taken should a system compromise occur.
6. Properly use the vocabulary associated with cybersecurity.
7. Apply formal security policy models to real world scenarios.

CSEC1110: Fundamentals of IT Security
Credits 3
Lecture: 2 Lab: 1 OJT: 0

Security is an important component of information technology. This course introduces industry-recommended security guidelines and controls. Students will practice implementing several examples of controls and encrypting data in transit and for storage.

Competencies
1. Carry out information technology policies within an organization that include privacy, legal and ethical considerations.
2. Evaluate the purpose and function of cybersecurity technology, identifying the tools and systems that reduce the risk of data breaches while enabling vital organization practices.
3. Apply appropriate tools and concepts to minimize the risk to an organization's cyberspace to address cybersecurity threats.
4. Identify the characteristics of a risk management approach for responding to and recovering from a cyber attack on systems which contain high-value information and assets such as email.
5. Implement common standards, procedures and applications used to protect the confidentiality, integrity and availability of data and information systems.
6. Analyze human facets that enable the exploitation of computing-based systems.
7. Evaluate various security breaches and their effect on business operations.
8. Summarize how governmental and environmental regulations affect an organization's environment.
9. Perform common malware analysis procedures on mobile and desktop computer systems.

Networking Class Comparison
Can the M State CPTR 1108 be modified to fulfill the CSIS 262 requirements?

CSIS 262: Introduction to Networking
Credits: 3
Lecture Hours/Week: 3
Lab Hours/Week: 0

This course will provide students with a basic understanding of how networks are designed, built and operated. The course will give students experience with basic network analysis tools and expose students to concepts in network vulnerabilities.

OUTLINE OF MAJOR CONTENT AREAS
1. Network design
2. Basic network analysis
3. Network security basics
4. Data logging

LEARNING OUTCOMES (General)
1. Describe fundamental concepts, technologies, components and issues related to communications and data networks.
2. Design a basic network architecture that meets a specific set of requirements including those for hosts or clients.
3. Analyze network traffic using packet tracing to illustrate fundamental networking concepts.
4. Use basic network monitoring and analysis tools to observe and analyze network activity and identify security issues.
5. Perform network mapping and interpret results.
6. Describe methods for data acquisition in a compute device.
7. Describe common network vulnerabilities.

CPTR1108: Cisco 1
Credits: 3
Lecture: 1 Lab: 2 OJT: 0

This is an introduction to networks course that covers the architecture, structure, functions and components of the Internet and other computer networks. Students achieve a basic understanding of how networks operate while building simple local area networks (LANs). Students perform basic configurations for routers and switches and implement Internet Protocol.

Competencies
1. Explain how physical and data link layer protocols support the operation of Ethernet in a switched network.
2. Explain how the upper layers of the Open Standards Interconnect (OSI) model support network applications.
3. Configure switches and end devices to provide access to local and remote network resources.
4. Configure routers to enable end-to-end connectivity between remote devices.
5. Explain Internet Protocol addressing and subnetting.
6. Create Internet Protocol version 4 and Internet Protocol version 6 addressing schemes and verify network connectivity between devices.
7. Configure a small network with security best practices.
8. Troubleshoot connectivity in a small network.

Linux Class Comparison
Can the M State CPTR 2224 be modified to fulfill the CSIS 360 requirements?

CSIS 360: Linux Programming and Development Tools
Credits: 3
Lecture Hours/Week: 3
Lab Hours/Week: 0

This course requires either of these prerequisites
CSIS 155 - Introduction to Computers & Programming I
CSIS 162 - Programming for Cybersecurity

An introduction to UNIX programming and program development tools. Considers the UNIX file system, shells, scripting languages, system calls, signal handling, interprocess communication, and tools for constructing, archiving, debugging, testing and installing software products.

OUTLINE OF MAJOR CONTENT AREAS
1. Linux fundimentals / review.
2. Administering your own linux system.
3. Scripting Languages.
4. Linux environment and environmental variables .
5. Linux file system and file handling at various levels (from low to high).
6. Data Management .
7. Linux development tools.
8. Processes and Signals.
9. Interprocess communication.
10. POSIX threads.
11. GUI Programming.

LEARNING OUTCOMES (General)
1. Install and configure a personal Linux system.
2. Demonstrate the use of a scripting language to perform management functions.
3. Apply version management software to project maintenance.
4. Use an IDE to develop a GUI program project.
5. Demonstrate the use of the make utility for building and installing a software package.
6. Demonstrate, via a programming project, inter-process communication using signals, pipes, and sockets.

CPTR2224: Linux 1
Credits: 3
Lecture: 2 Lab: 1 OJT: 0

This course deals with Linux installation, configuration and system administration. This course lays the groundwork for continued study of Linux.

Competencies
1. Create Linux accounts.
2. Manage Linux accounts.
3. Prepare appropriate documentation.
4. Analyze graphical environments.
5. Write simple shell scripts.
6. Manage application software.
7. Manage security.
8. Evaluate fault-tolerance solutions.
9. Use appropriate software and commands.
10. Manage printing.

Programming Class Comparison
Can the M State CPTR 1001 be modified to fulfill the CSIS 162 requirements?

CSIS 162: Programming for Cybersecurity
Credits: 3
Lecture Hours/Week: 3
Lab Hours/Week: 0
OJT Hours/Week: *.*

This course will provide students with basic skills in scripting and programming. It focuses on enabling students to write simple scripts to automate tasks and perform simple operations with a focus on security.

OUTLINE OF MAJOR CONTENT AREAS
1. Secure programming practices
2. Basic data structures and algorithms
3. Automation and scripting
4. High-level programming

LEARNING OUTCOMES (General)
1. Write and execute simple scripts to automate system administration tasks.
2. Write and execute programs in a high-level language using basic programming constructs and concepts.
3. Implement basic secure coding practices in scripts including bounds checking and input validation.
4. Use basic data structures and algorithms in simple programs and scripts.
5. Articulate conceptual understanding and apply practical use of regular expressions from a cybersecurity perspective.

CPTR1001: Introduction to Programming and Scripting
Credits: 3
Lecture: 1 Lab: 2 OJT: 0

This course is an introduction to computer programming. Emphasis will be on programming concepts, program design methodology, program debugging, problem solving and writing clear code.

Competencies
1. Describe the features and syntax of a programming language.
2. Understand how software can be written to solve business problems.
3. Use debugging and testing to create error-free code.
4. Demonstrate industry standard code development techniques.
5. Develop logic structures.
6. Develop loop structures.
7. Develop control structures.
8. Understand data types.
9. Understand functions.
10. Create, update, and process data files.
11. Understand techniques required for security in computer programming.