MASTER OF SCIENCE IN APPLIED CYBERSECURITY AND DIGITAL FORENSICS

At the conclusion of their studies, graduates of the Master of Science in Applied Cybersecurity and Digital Forensics degree should be able to:

- Design and implement a comprehensive enterprise security program using both policy and technology to implement technical, operational, and managerial controls
- Comprehensively investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law
- Technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions
- Conduct and report on significant research in the areas of cybersecurity and/or digital forensics

Illinois Institute of Technology has been designated as a National Center of Academic Excellence in Cyber Defense Education by the National Security Agency and the Cybersecurity and Infrastructure Security Agency. This designation results from meeting stringent Center of Academic Excellence criteria and mapping of information technology and management curricula to a core set of cyber defense knowledge units. Students attending Center of Academic Excellence in Cyber Defense Education institutions are eligible to apply for scholarships and grants through the Department of Defense Cyber Scholarship Program and the Federal Cyber Corps® Scholarship for Service Program. This designation reflects Illinois Institute of Technology's commitment to producing professionals with cyber defense expertise for the nation.

Students may choose from two research options to complete the degree:

Thesis Option

The thesis option requires coursework and six credit hours ITMT 591 for a total of 32 credit hours. The result is a master's thesis.

Master's Project Option

The master's project option requires coursework and three credit hours of ITMT 594 or ITMT 597 for a total of 32 credit hours. The result is a project that results in one of the following:

1. A paper submitted for publication as an article or as a technical report
2. A security or forensic software product
3. A security hardware device or appliance

Software or hardware must have an accompanying technical report and user documentation.

Master of Science in Applied Cybersecurity and Digital Forensics (Thesis Option)

Code	Title	Credit Hours
Required Core Courses		**(15)** [1]
ITMS 538	Cyber Forensics	3
ITMS 543	Vulnerability Analysis and Control	3
ITMS 548	Cyber Security Technologies	3
ITMS 578	Cyber Security Management	3
LAW 273	Evidence	3
Research Course		**(6-8)**
ITMT 591	Independent Study and Research	6-8
Elective Courses		**(9-11)**
Select seven to nine credit hours from the following:		7-9
Any 500-level ITMS course not listed in the required courses above. [2]		3
ITMM 537	Vendor Management and Service Level Agreements	3
ITMM 585	Legal and Ethical Issues in Information Technology	3
ITMM 586	Information Technology Auditing	3
ITMO 517	Shell Scripting for System Administration	3
ITMO 540	Introduction to Data Networks and the Internet	3
ITMO 556	Introduction to Open Source Software	3
ITMT 597	Special Problems in Information Technology	3

Select a minimum of two credit hours from the following: [3]		2
LAW 240	National Security Law	2
LAW 495	Electronic Discovery	2

Minimum degree credits required: 32

1. Substitutions for core course requirements may be made upon presentation of evidence of equivalent coursework, certification, or experience. Approval of course substitutions will be made by the student's adviser or an ITM associate chair.
2. ITMS 579 may be taken more than once.
3. LAW electives not listed above or ITMS electives may be substituted as approved by the student's adviser or an ITM associate chair.

Master of Science in Applied Cybersecurity and Digital Forensics (Master's Project Option)

Code	Title	Credit Hours
Required Core Courses		**(18)** [1]
ITMS 538	Cyber Forensics	3
ITMS 539	Steganography	3
or ITMS 549	Cyber Security Technologies: Projects & Advanced Methods	
ITMS 543	Vulnerability Analysis and Control	3
ITMS 548	Cyber Security Technologies	3
ITMS 578	Cyber Security Management	3
LAW 273	Evidence	3
Research Course		**(3)**
ITMT 594	Special Projects in Information Technology	3
or ITMT 597	Special Problems in Information Technology	
Elective Courses		**(11)**
Select a minimum of nine credit hours from the following:		9
Any 500-level ITMS course not listed in the required courses above. [2]	3	
ITMM 537	Vendor Management and Service Level Agreements	3
ITMM 585	Legal and Ethical Issues in Information Technology	3
ITMM 586	Information Technology Auditing	3
ITMO 517	Shell Scripting for System Administration	3
ITMO 540	Introduction to Data Networks and the Internet	3
ITMO 556	Introduction to Open Source Software	3
ITMT 597	Special Problems in Information Technology	3
Select a minimum of two credit hours from the following: [3]		2
LAW 240	National Security Law	2
LAW 495	Electronic Discovery	2
Total Credit Hours		**32**

1. Substitutions for core course requirements may be made upon presentation of evidence of equivalent coursework, certification, or experience. Approval of course substitutions will be made by the student's adviser or an ITM associate chair.
2. ITMS 579 may be taken more than once.
3. LAW electives not listed above or ITMS electives may be substituted as approved by the student's adviser or an ITM associate chair.