100% ONLINE GRADUATE CERTIFICATES
CYBERSECURITY POLICY | CYBERSECURITY MANAGEMENT

Virginia Tech and the Appalachian School of Law (ASL) have partnered to make two new Virginia Tech Graduate Certificates available to ASL students: Cybersecurity Management and Cybersecurity Policy. In addition, up to two courses from an MIT certificate may be applied to the JD requirements. We anticipate formal approval to be complete by January 2020.

A cybersecurity certificate will typically be completed in the 2L year of the Juris Doctorate degree program. However, the certificate program is very flexible because of its asynchronous, online delivery so ASL students may choose to complete it at another time. These cybersecurity certificates require tuition and fees paid directly to Virginia Tech. In order to apply for either Virginia Tech Graduate Certificate, candidates must be accepted to the ASL JD program.

CYBSERSECURITY MANAGEMENT

The purpose of this certificate is to provide a broad understanding of concepts and principles that will support management of organizations with cybersecurity concerns. The certificate will prepare students to plan, manage, and assess cyber technologies needed to secure critical corporate data and information. The emphasis will be on operational design, technology acquisition, risk assessment, and governance. This certificate will be an efficient mechanism for students from a variety of backgrounds to gain the foundation they need as leaders to posses a unique blend of technical expertise and an understanding of how to manage cybersecurity operations, align cybersecurity programs with business priorities, and develop risk mitigation strategies that consider current laws and policies.

ASL students completing the certificate in Cybersecurity Management will understand these and related areas after completing three courses:

- **BIT 5134** Cybersecurity Program Design & Operation
- **ACIS 5624** Cybersecurity Governance & Risk Management
- **MGT 5804** Strategic Leadership in Technology Based Organizations

CYBERSECURITY POLICY

This certificate aims to provide a broad understanding of key factors influencing policies on cybersecurity at all levels. Cybersecurity policy is inherently transdisciplinary, incorporating elements of technology, business, criminology, and national/international governance. The emphasis is to equip students with a strong understanding of these elements and prepare them to implement policies that improve the state and practice of cybersecurity for all stakeholders. One need look no further than recent headlines for a plethora of examples demonstrating the need for government and industry leaders who understand how to develop, interpret, and apply cybersecurity policy. The diverse set of knowledge, skills, and abilities needed to do this successfully cannot come from a predominately technology-focused curriculum. This certificate will prepare students from a variety of backgrounds to be both tech-savvy and societally-aware in implementing policies that affect cyber security, privacy, and safety in the modern age.

ASL students completing the certificate in Cybersecurity Policy will understand these and related areas after completing three courses:

- **BIT 5114** Crime and Conflict in Cyberspace
- **BIT 5124** Cyber Law and Policy for IT
- **BIT 5594** Web-based Applications & E-Commerce

COURSE DELIVERY/FORMAT (QUALITY AND FLEXIBILITY)

Certificate courses are taught online by full-time Pamplin College of Business faculty using Virginia Tech's Canvas Learning Management System. Course lectures and other materials are pre-recorded and are available to students at anytime from anywhere in the world. In addition, students may decide to attend regularly scheduled class meetings to participate in live lecture presentations, forums, and other discussions.

FOR MORE INFORMATION, PLEASE CONTACT:

ASL – Charles J. Condon Phone: (276) 244-1309
Virginia Tech MIT Program Phone: (703) 538-8384

MASTER OF INFORMATION TECHNOLOGY VIRGINIA TECH™

ASL

100% ONLINE GRADUATE CERTIFICATES
CYBERSECURITY POLICY | CYBERSECURITY MANAGEMENT

PROGRAM DETAILS (COURSE DESCRIPTIONS)

CYBERSECURITY MANAGEMENT

BIT 5134: Broad coverage of the enterprise cybersecurity lifecycle from a managerial perspective. Designing comprehensive and resilient enterprise cybersecurity program that aligns with business objectives. Establishing policies and managing resources. Overseeing and running cybersecurity operations. Assessing security posture and mitigating vulnerabilities. Responding to security threats and failures. Measuring and reporting security program effectiveness.

ACIS 5624: Cybersecurity governance and risk management programs in organizations. Governance frameworks for cybersecurity and external drivers for cybersecurity. Risk management, including existing frameworks, principles, and strategies related to risk assessment and implementation of cybersecurity policies, controls, and procedures. Budgeting and evaluation of risk management programs. Compliance with organizational cybersecurity programs, including risks of insider threats, management of security-related personnel, and establishment of cyber hygiene. Cybersecurity governance in relation to cybersecurity regulation.

MGT 5804: This course focuses on the role of the leader in crafting corporate and business strategies where technology provides the basis for the firm's competitive advantage.

CYBERSECURITY POLICY

BIT 5114: In-depth exploration of the cyber threat landscape and motives, methods, and mechanisms that shape it. Investigation into the complex and evolving nature of security, privacy, and safety in cyberspace. Examination of the consequences posed by cyber threats at the individual, corporate, national, and societal levels. Designed for students with diverse backgrounds and interests across technical, managerial, and policy aspects of cybersecurity.

BIT 5124: Key legal and policy cyber governance and cyber security topics for managers and information security officers. Legal rights, remedies, and limitations related to cybercrime, computer intrusion, national security, and data breaches. Privacy laws and standards, impact assessments, privacy and security by design as policy and legal requirements. Comparison of international approaches to relevant laws and policies. Fundamentals of managing legal and policy aspects of information technology and security.

BIT 5594: An examination of the concepts, technologies, and applications of electronic commerce. Topics include the World Wide Web as a platform for electronic commerce; intranets; electronic data interchange; electronic banking and payment systems; security and firewalls; software agents; and the social, legal, and international issues of electronic commerce.

JD/CERTIFICATE REQUIREMENTS

1. Applicants must hold a GPA of 3.0 or greater at ASL;
2. Applicants must be approved for the program by both VT and ASL; and
3. Students must remain in good standing with both institutions to continue in the program

2019-20 TUITION AND FEES

- Tuition per credit hour: $975.00 ($2,925 per course)
- Technology Fee: 1 to 6 hours = $19.00
- Library Fee: 1 to 6 hours = $24.75

A typical student will enroll in two courses in the fall semester and one course in the spring. The total cost is:

- 3 courses at $2,295.00 = $8,775.00
- 2 semesters technology fee at $19.00 = $38.00
- 2 semesters library fee at $24.75 = $49.50
- Total cost per certificate = $8,862.50

FOR MORE INFORMATION, PLEASE CONTACT:

ASL – Charles J. Condon Phone: (276) 244-1309
Virginia Tech MIT Program Phone: (703) 538-8384

MASTER OF INFORMATION TECHNOLOGY VIRGINIA TECH™

ASL