WASHINGTON STUDENT ACHIEVEMENT COUNCIL
EDUCATION · OPPORTUNITY · RESULTS

Notification of Request for Authorization under the Degree-Granting Institutions Act

Date posted:	October 6, 2017
Institution:	Washington Technology University
Current status:	Undergoing review for authorization to offer a degree program in Washington State
Nature of request:	Authorization to offer a degree program in Washington State
Proposed program:	Bachelor of Science in Information Security
Location:	200 112th Ave. NE, Suite 200 Bellevue, WA 98004

Background:
Washington Technology University is a private, for-profit institution with classroom facilities in Bellevue, WA, and a corporate office in North Bend, WA. It is currently undergoing review for authorization to offer a degree program in Washington.

Nature of the review:

Prior to granting authorization to offer degree programs in Washington State, the Washington Student Achievement Council/Degree Authorization reviews elements such as institutional infrastructure, financial solvency, administrative staff qualifications, program outcomes, course requirements, method of course delivery, faculty credentials, and student services.

The program to be offered by Washington Technology University appears to meet the requirements of the Degree-Granting Institutions Act.

Information on the program can be found at the end of this notice.

Timeline:

The WSAC will accept comments on this application until October 20, 2017.

Any individuals with knowledge that may indicate the institution and/or the program does not meet the authorization requirements of WAC 250-61 are requested to submit comments to: Degree Authorization.

If you would like to know more about the current law and regulations that govern the program, they can be found at the following links: the statute is Chapter RCW 28B.85 and the regulation is WAC 250-61.

917 Lakeridge Way SW
PO Box 43430
Olympia, WA 98504-3430
www.wsac.wa.gov
360.753.7800

Bachelor of Science in Information Security

Program Description

The Bachelor of Science in Information Security at Washington Technology University is designed to provide an in depth understanding of information technology as well as prepare students to address a wide range of vulnerabilities and threats that affect private, corporate and government computer information systems. This program prepares students to design and implement key technologies and processes needed to protect critical information in cyberspace.

The BSIS program provides the knowledge, skills and competency to successfully analyze, build, support, and defend information systems against cyber-attacks. While a foundational study of computer hardware, software, and networking is provided, the focus of the program is development of practical cyber security knowledge accumulated through lectures, interactive exercises and projects.
The first series of courses emphasis technology. The second set builds on this core knowledge by concentrating exclusively on information security. An exclusive focus on security courses serves to improve the absorption and retention of critical concepts and encourages the development of a clear and interconnected understanding of Information Security and its impact on society.

The Information Security degree at WTU is designed to ensure proficiency of concepts and ideas related to modern Information Security. No prior technical knowledge is required to enter, it is designed for anyone interested in Information Security. Those seeking to enter the fields of cyber security, information assurance, computer forensic analysis, or network security should consider entering the program.

Program Learning Outcomes:

- Identify the elements of an information system and understand how software is developed and used within the information system
- Use and apply mathematical concepts appropriate to the development of software for a computer and information system

- Demonstrate background knowledge of Operating Systems, Networking, Data Communications, Database Technology, Information Systems Planning, and Project Management
- Analyze an information systems problem, define performance requirements and specifications needed to solve an information security problem
- Identify solutions while recognizing the social and ethical impact of computing on individuals, organizations and society
- Demonstrate effective team communication
- Use current techniques, skills, and tools necessary for information systems practices by recognizing the need for, and the ability to engage in, continuing professional development
- Understand professional, ethical, legal, security, social issues and responsibilities
- Demonstrate the use of various computer forensic software tools and techniques as well as follow proper legal procedures for obtaining, analyzing, and reporting digital forensic evidence
- Explain the findings of a cyber forensic investigation in both written form and in oral form
- Identify and analyze legal issues within technology, regarding standards, compliance, contracts, computer crime, privacy, obscenity, and intellectual property
- Compare and contrast techniques for preventing unauthorized access to computer networks and apply measures for minimizing the damage caused by network intruders.
- Evaluate and implement security controls for an information system to provide assurance where the security processes or controls are implemented
- Evaluate an implemented Governance Framework for its effectiveness and usefulness to an organization.
- Identify the security mechanisms contained within various computing devices used to protect it while allowing it access to external data and other connected devices.

Accreditation Objectives: Organization: ABET | Location: Bellevue | Group: Computing Accreditation Commission | Criteria: General Criteria Only (CAC)

The curriculum is designed around 6 blocks of 3 months each (1 quarter), and each block contains 3 one-month instructional content to allow students to focus each month on a single subject.

Courses Available

Foundations (15 Credits)

This class provides students with foundational concepts needed to succeed in the program. Analytical and numerical methods are covered as well as legal and ethical issues in information systems and information security are covered.

Content Block 1: Statistics and Calculus

TOPICS: Summarized Descriptive Data, Frequency Distributions, Measures of Central Tendency and Dispersio, Curve Fitting, Sampling Theory and Distributions, Chi-Square Testing, Hypothesis Testing, Linear Equations, Matrices, Linear Programming, Differential Equations, Exponential Functions

MATH 200 Quantitative Tools and Methods (5)

Content Block 2: Computing Methods and Data Management

TOPICS: Discrete Mathematics, Computer Networks, Computer Hardware, Databases, Database Design, Number Systems

CPSC 210 Computer Systems Foundations (5)

Content Block 3: Information Ethics and Legal Issues in Information Security

TOPICS: IT Ethics, Moral and Social Issues, Information Privacy, Data Privacy, Legal Liability, International Information Privacy Laws.

INSE 300 Legal and Ethical Issues in Information Security (5)

Software Platforms (15 Credits)

This course covers software platforms necessary for program completion. The student learns tools and techniques used in software development including data structures and algorithms and operating systems. Finally, students cover the software used to manage and run data needed by the software.

Content Block 1: Programming and Web Development

TOPICS: Introduction to Python, Development Environments, Type Declarations, Control Statements, Structured Programming Concepts, Object Oriented Concepts, File Creation, Searching and Sorting Algorithms, Web Page Creation, HTML/DHTML Basics, CSS, XML, Deployment Environments, JavaScript, Event Handling.

CPSC 250 Programming Fundamentals (5)

Content Block 2: Operating Systems

TOPICS: Introduction to Windows, Linux, UNIX. PowerShell and Bash basics, Concurrency, Threads, Swapping, Memory Management, Scheduling, I/O, File Systems

CPSC 220 Operating Systems Foundations (5)

Content Block 3: Databases

TOPICS: DBMSs, MS Access, SQL, Relational, Normalization, Data Modeling

CPSC 310 Database Management Systems (5)

Systems (15 Credits)

This class is dedicated to the study of the management, analysis, design and implementation of data communications systems. Tools and techniques related to its development along with key concepts needed to describe, model, and develop data communications systems.

Content Block 1: Project Management

TOPICS: Project Life Cycle, Triple Constraint, Project Charter, WBS, Gantt Chart, Cost, Budgeting, Scope Creep, SWOT, PMBOK, Risk Analysis, Network Diagrams, Earned Value, Outsourcing, Negotiations, Project Sponsors, Executive Report Outs.

INSE 335 Project Management (5)

Content Block 2: Systems Analysis and Design

TOPICS: Business Models, Information Models, Structured Analysis, Object-Oriented Analysis, Agile Methods, SDLCs, Requirements Engineering, UML, FDD, JAD, RAD, DFDs, Data Dictionaries, CASE tools, RFP, RFQ, Design Patterns

INSE 310 Systems Analysis and Design (5)

Content Block 3: Data Communications Systems (Networking)

TOPICS: OSI and IP models, QoS, Error Correction, VLANs, Ethernet, LAN Protocols and Topologies, IP Addressing, IPv4/6, Bluetooth

INSE 320 Data Communications and Networking (5)

Security (15 Credits)

This course covers the basic concepts in information security. It also develops advanced security concepts needed to understand how organizations manage their information systems to prevent unauthorized access.

Content Block 1: Fundamentals of Information Security

TOPICS: Security Life Cycle, Confidentiality, Integrity, Availability, EAA, Authentication, Risks, Cyber Attackers, Laws, Regulations, Attack Methodologies, Attack Types, Cryptography, Organizational Culture, Vulnerability Assessment

INSE 400 Fundamentals of Information Security (5)

Content Block 2: Corporate Governance, Policy, Risk, CyberCrime

TOPICS: Risk Classification and Identification, Response, Recovery, Management, IT Infrastructure Compliance, Business Drivers, Policy Creation and Frameworks, Data Classification, Handling Policy, Enforcement

INSE 410 Corporate Governance, Policy, Risk, Cybercrime (5)

Content Block 3: Computer and Network Security

TOPICS: CIA Model, Security Levels, Access Control Lists, Device Hardening, Computing Service Management, Perimeter Construction and Hardening, Thread Identification and Classification, Stealth Firewalls, Authentication and User Account Management, Network Intrusion Detection, Cloud Security

INSE 415 Computer and Network Security (5)

Detection, Investigation & Prevention (15 Credits)

This course develops tools and techniques used to detect information security breaches. It also provides the students with concepts used to investigate security incidents as well as the tools and techniques to build in safeguards to protect the organization from electronic and social vulnerabilities.

Content Block 1: Security Strategies for Windows, Linux and Applications

TOPICS: Threat identification, User Privileges and Permission Hardening, Filesystem, Kernel Security and Risk Management, Image Baselining, Networked File System Securing, Platform Encryption, Malware Detection, System Administration

INSE 420 Security Strategies for Operating Systems and Applications (5)

Content Block 2: Computer and Network Forensics, Investigation and Response

TOPICS: Computer Crime, Computer Forensic Methods, Data Collection, Email Mining, Seizure, and Protection, Data Recovery Techniques, Windows- Linux-Mac Data Recovery, Mobile Platform Specific Forensic Techniques, Incident Response

INSE 425 Computer and Network Forensics (5)

Content Block 3: Auditing IT Infrastructure for Compliance

TOPICS: Compliance Laws, Scope of Compliance, Auditing Standards, Audit Planning, Conducting Audits, Infrastructure Audits, User Domain, Workstation, LAN, LAN-to-WAN, WAN Domain Compliance, Remote Access Compliance and Standards, Application Compliance, IT Audit Certifications

INSE 430 Compliance Auditing the IT Infrastructure (5)

Hacking & Capstone (15 Credits)

This final course in the sequence explores hacking and the tools and techniques used to exploit common vulnerabilities of modern information systems. The course also investigates security for wireless and mobile networking technology. Finally, the course includes a capstone project where students get an opportunity to apply their knowledge to a project of their choosing.

Content Block 1: Hacker Techniques, Tools, and Incident Hacking

TOPICS: Footprinting Overview and Tools, Port Scanning Techniques, Enumeration and Computer Hacking, Wireless Vulnerability Detection Techniques and Exploitations, Web and Database Attacks, Malware Concepts, Hacking Tools Sniffers, Session Hijacking, and DoS, Penetration Testing, Social Engineering

INSE 435 Hacker Tools and Techniques (5)

Content Block 2: Internet, Wireless and Mobile Device Security

TOPICS: Securing Web Applications, Site Migration Risks, Reducing Web Application Vulnerabilities, Site Vulnerability Testing and Assessment, Securing Communications, WLAN Security, WLAN Auditing, WLAN Risk Assessment, Mobile Device Hardening, Mobile Footprinting, Wireless Attack Vectors and Mitigations

INSE 440 Internet, Wireless, and Mobile Device Security (5)

Content Block 3: Capstone Project

TOPICS: Topic Identification and Selection, Team Building, Project Development, Weekly Statusing, Team Presentation, Project Collaboration and Report Generation.

INSE 495 Capstone Project (5)

Program Requirements (90 credits)

Technology Core (45 Credits)	Pre-requisites
MATH 200 Quantitative Tools and Methods (5)	None
CPSC 210 Computer Systems Foundations (5)	None
CPSC 220 Operating Systems Foundations (5)	Math 200 & CPSC 210

CPSC 250 Programming Fundamentals (5)	Math 200 & CPSC 210
CPSC 310 Database Management Systems (5)	Math 200 & CPSC 210
INSE 300 Legal and Ethical Issues in Information Security (5)	Math 200 & CPSC 210
INSE 310 Systems Analysis and Design (5)	Math 200 & CPSC 210
INSE 320 Data Communications and Networking (5)	Math 200 & CPSC 210
INSE 335 Project Management (5)	Math 200 & CPSC 210

Depth of Study (40 Credits)	**Pre-requisites**
INSE 400 Fundamentals of Information Security (5)	Math 200, CPSC 210, CPSC 220, CPSC 250, CPSC 310, INSE 300, INSE 310, INSE 320 & INSE 335
INSE 410 Corporate Governance, Policy, Risk, Cybercrime (5)	INSE 400
INSE 415 Computer and Network Security (5)	INSE 400
INSE 420 Security Strategies for Operating Systems and Applications (5)	INSE 400
INSE 425 Computer and Network Forensics (5)	INSE 400
INSE 430 Compliance Auditing the IT Infrastructure (5)	INSE 400
INSE 435 Hacker Tools and Techniques (5)	INSE 400
INSE 440 Internet, Wireless, and Mobile Device Security	INSE 400

Capstone Requirement (5 Credits)	Pre-requisites
INSE 495 Capstone Project	All Program Courses

Course Descriptions

Math 200 - Quantitative Tools and Methods (5cr)

There are concepts employed in science and technology to quantify the natural and theoretical worlds. Explore ways to collect, define, describe and communicate real-world facts. Tools, techniques and methodologies commonly used for analysis, computation, decision making and quantification are covered. Decision analysis, truth tables, conditional logic, data analysis, are discussed. Concepts such as conditional probability, statistics, discrete mathematics, Boolean logic, functions, distributions, reasoning and methodologies are reviewed.

CPSC 210 – Computer Systems Foundations (5cr)

This course introduces students to computers, computer systems, and basic structures supporting computer programming and data communications. Throughout this course, fundamental concepts in Computer Science are covered. Topics include digital building blocks of computers, computer networks, operating systems, and large-scale computing.

ISNE 300 – Ethics in Information Security (5cr)

Cybersecurity and IT ethics is a subject that addresses the crossroads between the need for a computerized modern world and a human desire for fairness, objectivity, security and reason. The course explores the historical, theoretical, and thematic dimensions of ethics as it relates to information technology and cybersecurity. Historical context, frameworks, challenges and theories are explored. Information security standards, computer viruses, hacktivism, cyberstalking and ethical behavior using social media are topics covered.

CPSC 151 – Programming Fundamentals (5cr)

Explore the basics of computer programming: from data types, to control and data structures, foundational elements that form a programming language. Key structural concepts such as functions, modules, interfaces and libraries are covered. Immerse in

the subject through examples and programming exercises. By the end of the course students should have the ability to design and build basic software applications.

CPSC 220 – Operating Systems Foundations (5cr)

An operating system is special software connecting user applications to the computing hardware. Learn the basic elements of a computer operating system in this course. Explore the history of modern operating systems, learn how they operate, understand what it takes to manage them and become familiar with different types. Topics feature memory management, process control and task scheduling.

CPSC 310 – Database Management Systems (5cr)

Learn about data modeling, design, normalization, data dictionaries, client server architecture, SQL, relational databases, and MySQL in this foundational level course on databases and their management systems. Special focus is provided on understanding the critical nature of information resources and why they must be carefully managed. The course uses examples and project-based assignments to support learning.

INSE 335 – Project Management (5cr)

In this introductory course on project management, key concepts, tools, techniques, and standards needed to deliver products or services in a timely manner and on budget are covered. Special emphasis is placed on task scheduling, resource management, and risk planning. An IT based project is used as the application of study. In addition, team dynamics and project leadership are explored. Upon completion, students should be able to apply basic project management concepts including the triple constraint, resource optimization, scheduling, work breakdown structures, Gantt Charts, network diagrams, risk management, and project planning.

INSE 310 – Systems Analysis and Design (5cr)

Learn how to translate business requirements into information systems and software that support a company's short- and long-term objectives. Real world case studies and applied assignments teach analytical reasoning, critical thinking, and problem-solving skills and systematic decomposition of problems into solutions. Data and systems

modeling are covered along with common approaches to system and software design mythologies.

INSE 320 – Data Communications and Networking (5cr)

Computer networks and data communications systems power the Internet and enable modern telecommunications systems that carry voice and data around the world. Learn how this technology provides access, transmission, security, and routing of information within an organization over wide geographical areas. Understand how networks are interconnected, how they are designed and how they communicate with each other.

INSE 400 – Fundamentals of Information Security (5cr)

The digital revolution has created the need for a focus on information systems security. New risks, threats and vulnerabilities associated with the transformation into a digital world have emerged. A review of compliance law, best practices in IT security, principles of network security, and an overview of operation security process and methodologies are covered in this course. In addition, a specific focus is given on application data and computer security, threat identification, vulnerability assessments, access control, identity management and cryptography.

INSE 410 – Corporate Governance, Policy, Risk, and Cybercrime (5cr)

The risks associated with cybersecurity threats increases as our world becomes ever more interconnected. Learn how to comprehensively manage cybersecurity risks as they relate to modern information systems. This course covers the fundamentals of risks and risk management. Topics include risk identification, threat categorization, and vulnerability assessments. Relevant laws are presented along with approaches to risk mitigation and organizational planning. Organizational impact analysis and continuity planning are reviewed.

INSE 415 – Computer and Network Security (5cr)

Learn the tools, techniques, processes and software used to secure data communications networks. This course provides a review of network vulnerabilities, common attack vectors, and methods for preventing, detecting and techniques for minimizing the effects of network attacks using commonly available software tools. Learn how to best

implement network security and incorporate best practices into an organization to defend networks.

INSE 420 – Security Strategies for Operating Systems and Applications (5cr)

Computer operating systems and software applications are commonly exploited by hackers. An in depth understanding of characteristic risks, threats, vulnerabilities associated with specific modern operating systems and applications is important to understand in order to protect them. Learn the tools and techniques needed to decrease or remove risks arising from these vulnerabilities: OS hardening, application security, and vendor specific incident management such as bug patching, and software configuration control.

INSE 425 – Computer and Network Forensics (5cr)

Explore tools and techniques used to find, follow, and extract digital markers from computers and networking devices used in cybercrimes. The course examines the fundamentals of system forensics including an overview of forensics, a discussion of computer crime, the challenges of system forensics, and forensics methods. Learn the tools, techniques, and methods used to perform computer forensics and investigation including collecting evidence, investigating information-hiding, recovering data, and scrutinizing e-mail in hands on labs and a summative project.

INSE 430 – Compliance Auditing IT Infrastructure (5cr)

Learn how compliance laws are used to safeguard organizational and consumer data. Learn the details of operational requirements for proper documentation and implementation of security controls and protocols within an organization. Audit standards, frameworks, security controls, and personnel certifications are covered.

INSE 435 – Hacker Tools and Techniques (5cr)

Discover the history of hacking and understand the difference between ethical and black-hat hacking in this course. Examine how attackers target networks and the methods they use including footprinting, port scanning, enumeration, malware, sniffers, denial of service, and social engineering. The course provides concepts in incident

response, defensive technologies and common approaches to defense. Concepts are reinforced through hands on labs and a project.

INSE 440 – Internet, Wireless, and Mobile Device Security (5cr)

Explore network security threats and vulnerabilities for wireless and mobile devices in this course. Emphasis is on wireless local area network security and mobile device communications protocols. Security solutions and risks to wireless networks and mobile devices are covered as are models for information security and risk mitigations as they relate to mobile devices and wireless networks.

INSE 495 – Capstone Project (5cr)

The degree program culminates with a capstone project where students have an opportunity to apply the concepts learned throughout the degree program to a real-world problem or an applied research project. The capstone will begin with the selection of a project, a collection of project requirements, a review of background information which could be research or customer requirements. Students will build a short timeline of deliverables and list of necessary resources. Finally, students will implement the project. The project may be performed individually or as a group. The course concludes with a submission of report of work and a presentation of results.

Course Delivery

WTU will offer its instruction in an innovative format. The program will be offered in 6 quarters—continuously so as to reduce the time to degree. The objective is to have students continuously enroll for 18 months and exit with a Bachelor degree. Each Quarter, for 6 consecutive Quarters—no summer break from learning--3 one-month content classes are offered sequentially.

Recognizing that the vast majority of Community College transfer students and Associate Degree completers in our community are employed more than ½ time, and many need to work full time, classes will be offered in a clustered sequence and students

will be assured of their course schedule for the full 18 months. In other words, students will enroll, subject to enrollment limitations, in either a morning cohort, afternoon cohort, or evening cohort, so they can if necessary arrange their work or family schedule in alternative times and assure their employer they will be available to work a constant schedule while they pursue their higher degree. Following best practices, students will continue their program in a cohort, thus receiving from their fellow students, and the University, the support they often need to be successful.

Every class is taught in a mixed mode format, with classes taught 3 days a week on site, and 2 days a week online. Thus, students will receive 15 contact hours of instruction each week, participating in 3, five-credit sequential courses during the quarter. Every course will utilize the University's learning management system, Moodle, allowing the common facilitation of all schedules and communication among and between faculty and students.