Cuyahoga Community College®

Cybersecurity and Airport Administration

This course explores cybersecurity in airport management, focusing on protecting financial data, administrative systems, and communication channels from cyber threats. Key topics include securing financial transactions, compliance with federal regulations, safeguarding property management data, and managing cybersecurity risks in capital projects.

COURSE OUTCOMES

Course Outcome 1

Students will be able to demonstrate an understanding of the cybersecurity measures necessary to protect stakeholder data and ensure secure communication in airport administration.

Objectives 1

- Recall the basic principles of data integrity and availability related to airport management systems.
- Describe the importance of secure communication between airport stakeholders and its role in protecting sensitive information.
- Evaluate the integrity and availability of airport historical management data to ensure accurate, secure and uninterrupted access for stakeholders.
- Analyze stakeholder communication systems to determine vulnerabilities and propose methods for securing sensitive exchanges.
- Design an access control system using role-based access to ensure that only authorized personnel can modify sensitive administrative and stakeholder data.

Course Outcome 2

Students will be able to explain how cybersecurity impacts the safety and integrity of flight operations within the U.S. airspace system, ensuring secure communication and data exchange.

Objectives 2

- Recall common cybersecurity risks associated with air traffic control (ATC) systems.
- Explain the role of encryption in protecting communication between aircraft and ground control from unauthorized access.
- Assess the effectiveness of intrusion detection systems (IDS) in preventing cyberattacks on ATC systems.
- Apply encryption protocols to secure flight operation data exchanges between aircraft and ATC.
- Develop a cyber incident response protocol specific to potential attacks on flight operation systems.

Course Outcome 3

Students will be able to analyze the role of governance structures in implementing cybersecurity practices that comply with federal regulations and protect airport management systems.

Objectives 3

- Identify key federal regulations that guide airport cybersecurity practices.
- Understand the role of governance structures in enforcing cybersecurity policies within airports.
- Evaluate compliance with cybersecurity regulations by conducting periodic audits to ensure adherence to FAA and TSA standards.
- Create strategies to secure governance and legal data related to airport sponsor agreements.
- Monitor and adapt cybersecurity practices to stay aligned with updates to federal and state regulations.

Course Outcome 4

Students will be able to apply cybersecurity protocols to protect financial management systems, ensuring compliance with federal policies and preventing unauthorized access to sensitive financial data.

Objectives 4

- Recall the basic principles of the Payment Card Industry Data Security Standard (PCI DSS) and their importance in securing financial transactions.
- Summarize the key components of multi-factor authentication (MFA) and how it protects financial data.
- Implement and evaluate financial transaction security protocols that ensure compliance with PCI DSS standards.
- Analyze financial activity data using machine learning algorithms to detect and prevent potential fraud.
- Design an MFA system for airport financial systems to enhance security.

Course Outcome 5

Students will be able to evaluate cybersecurity risks in airport commercial development and property management, applying solutions to safeguard digital systems and tenant data.

Objectives 5

- Recall the importance of encryption in securing tenant and contractor data during commercial transactions.
- Understand the relationship between cybersecurity measures and the protection of airport property management systems.
- Assess tenant and contractor data protection measures to ensure compliance with airport cybersecurity protocols.
- Develop security measures to protect digital property management systems and ensure the confidentiality of sensitive data.
- Analyze potential cybersecurity risks in commercial development projects and propose solutions to mitigate them.

Course Outcome 6

Students will be able to assess the cybersecurity considerations in managing the Airport Improvement Program (AIP) and capital development funding processes to prevent cyber threats and ensure data integrity.

Objectives 6

- Identify common cybersecurity risks in digital grant management systems.
- Explain the role of vendor cybersecurity practices in ensuring the security of capital development projects.
- Assess the cybersecurity of systems used for capital development and grant applications under AIP.
- Evaluate the cybersecurity practices of vendors and contractors to mitigate third-party risks.
- Develop a secure grant management system that protects funding-related data from cyber threats.

METHODS OF EVALUATION

Evaluation can include any combination of the following:

- Assignments
- Quizzes
- Exams
- Lab Assignments
- Projects
- Reports
- Oral Evaluations

COURSE CONTENT OUTLINE

1. Overview of Airport and Airport Administration

a. Overview of Airport Management
   i. History of airport finance and administration
   ii. Stakeholders in airport management
   iii. Core administrative functions in airport operations

b. Cybersecurity Fundamentals in Airport Administration
   i. Basic principles of cybersecurity
   ii. Common threats in airport administrative systems (e.g., data breaches, phishing, malware)
   iii. Introduction to regulatory requirements (TSA, FAA)

2. Stakeholder Data Security and Communication

a. Understanding Airport Stakeholders
   i. Identifying internal and external stakeholders (e.g., airlines, passengers, vendors)
   ii. Expectations for data security from each stakeholder group

b. Cybersecurity in Stakeholder Communications
   i. Secure communication protocols (e.g., encryption, secure email platforms)

        ii. Risk assessment of communication channels
        iii. Case studies of communication breaches in airport administration

3. Securing Financial Transactions and Budgeting Systems

a. Overview of Airport Financial Management
    i. Airport revenue streams (e.g., landing fees, retail, parking)
    ii. Digital financial management tools used in airports

b. Cybersecurity in Financial Transactions
    i. Payment Card Industry Data Security Standard (PCI DSS) compliance
    ii. Securing online payment systems and transactions
    iii. Multi-factor authentication (MFA) for financial systems

c. Preventing Financial Fraud
    i. Threat detection in financial systems
    ii. Case studies of financial cyber fraud in aviation

4. Airport Regulatory Compliance and Cybersecurity

a. Understanding Federal Regulations Impacting Airport Cybersecurity
    i. FAA, TSA and federal mandates regarding airport cybersecurity
    ii. Compliance standards for airport financial and administrative systems
    iii. Legal consequences of noncompliance and data breaches

b. Implementing Cybersecurity Compliance Measures
    i. How to audit and assess airport cybersecurity measures
    ii. Tools and techniques for regulatory compliance monitoring

5. Protecting Administrative Data and Systems

a. Overview of Airport Administrative Systems
    i. Human resources, payroll and administrative databases
    ii. Physical and digital access control systems

b. Cyber Threats to Administrative Systems
    i. Common cyber threats (e.g., insider threats, ransomware, malware)
    ii. Risk management in administrative systems

c. Implementing Access Controls and Encryption
    i. Role-based access control (RBAC)
    ii. Encryption protocols for sensitive data
    iii. Tools for monitoring and logging administrative system access

6. Cybersecurity in Airport Governance and Legal Structures

    i. Understanding airport governance structures
    ii. The role of airport executives in cybersecurity decision-making
    iii. Types of airport governance models (public, private and hybrid)

b. Cybersecurity in Legal Contracts and Governance
    i. Securing sensitive legal documents
    ii. Cybersecurity clauses in vendor and tenant contracts
    iii. Protecting governance-related communications

7. Airport Commercial Development and Cybersecurity

a. Overview of Airport Commercial Activities
    i. Commercial real estate, retail and property management
    ii. Revenue from airport concessions and partnerships

b. Cybersecurity Risks in Commercial Development
    i. Securing digital leasing systems and tenant data
    ii. Risks in commercial vendor networks (third-party vulnerabilities)
    iii. IoT devices in commercial spaces (e.g., smart kiosks, digital signage)

c. Developing Cybersecurity Solutions for Commercial Operations
    i. Best practices for securing commercial operations
    ii. Case studies of successful cybersecurity implementations

8. Managing Cybersecurity for Capital Development and Funding

a. Introduction to the Airport Improvement Program (AIP)

   i. Overview of funding mechanisms (federal, state and private)
   ii. AIP application processes and associated financial systems

b. Cybersecurity in Grant and Capital Project Management
   i. Securing digital grant management systems
   ii. Managing cybersecurity for large-scale capital projects
   iii. Vendor cybersecurity requirements for airport construction projects

c. Fraud Prevention in Capital Development
   i. Threat detection for capital funding and development projects
   ii. Case studies of cybersecurity breaches in airport capital projects

9. Risk Management and Incident Response

a. Introduction to Risk Management in Airport Finance and Administration
   i. Identifying risks (e.g., financial, operational, cyber threats)
   ii. Risk assessment tools and frameworks (e.g., NIST)

b. Developing a Cybersecurity Incident Response Plan
   i. Building a response team for airport administration cybersecurity
   ii. Key elements of an effective incident response plan
   iii. Testing and updating response strategies

c. Case Study: Real-World Cybersecurity Incidents in Airport Finance and Administration
   i. Analysis of past cybersecurity incidents
   ii. Lessons learned and strategies for future prevention

10. Future Trends in Airport Finance and Administration Cybersecurity

a. Emerging Cybersecurity Threats
   i. New trends in cyberattacks targeting financial and administrative systems
   ii. Threats posed by advanced technologies (e.g., AI-driven attacks, ransomware-as-a-service)

b. Innovative Solutions and Future Technologies
   i. The role of artificial intelligence (AI) in cybersecurity
   ii. Blockchain technology for securing financial transactions
   iii. The future of encryption and data privacy

c. Planning for Long-Term Cybersecurity in Airport Finance and Administration
   i. Developing a long-term cybersecurity strategy
   ii. Continuous monitoring and improvement of cybersecurity measures
   iii. Final project: Develop a comprehensive cybersecurity plan for airport finance and administration