Prepared by the Department of Business
Date of Departmental Approval: December 7, 2009
Date approved by Curriculum and Programs: February 22, 2010 Effective: Fall 2010

1. **Course Number: BIT236**
   Course Title: Wireless Networking

2. **Description:** Using a hands-on approach, students learn the fundamentals of planning, installing, maintaining, and troubleshooting a network supported by unbounded media. Assuming no prior knowledge of wireless networks and devices, students are prepared to apply and support wireless technology in personal, LAN, and WAN networks. Many of the skills required for the Certified Wireless Network Administration (CWNA) exam are covered while exploring all current IEEE wireless protocols.

3. **Student Learning Outcomes:**
   Upon successful completion of this course, students are able to do the following:
   - Describe the history of wireless communication.
   - Identify wireless applications.
   - Differentiate between the various wireless organizations.
   - Describe the wireless standards and product certifications.
   - Explain the Radio Frequency basics including range, speed, signal characteristics and encoding techniques.
   - Configure wireless devices using Wi-Fi features and functionality.
   - Implement and manage wireless network devices and antennas.
   - Perform testing using wireless client devices and application software.
   - Plan wireless LANs using site surveys, and protocol/spectrum analyzers.
   - Install and troubleshoot wireless LANs.
   - Administer and optimize a Wireless LAN using the proper procedures.
   - Troubleshoot wireless LANs.
   - Identify, describe, and resolve WLAN security techniques.
   - Differentiate wireless LAN architectures.

4. **Credits:** Three credits

5. **Satisfies General Education Requirement:** No

6. **Prerequisite:** BIT187

7. **Semesters Offered:** Fall

8. **Suggested General Guidelines for Evaluation:** Tests, projects, and homework are used to evaluate student progress.

9. **General Topical Outline:** History of Wireless Communications, Wireless Applications, Wireless Organizations, Wireless Standards and Product Certifications, Radio Frequency Basics, Characteristics of Wi-Fi Technology, Wireless Networking Devices (network components and antenna), Administering and Optimizing Wireless LANs, Troubleshooting Wireless LANs, and Wireless Security. See attached competencies

BIT236. Wireless Technology
Course Competencies

1. Explain the many different needs and uses for wireless applications.
2. Distinguish between the government operated and private sector wireless organizations that improve standardize and advance wireless technologies. (IEEE, Wi-Fi Alliance and Regulatory Domain Governing Bodies)
3. Configure a wireless network knowing which of the many amendments or working groups for the 802.11 standards should be selected and why (b, a, g, n, e, i, r, and k).
4. Read through the Wi-Fi Alliance certifications for hardware and software to determine which devices can communicate.
5. Effectively implement a Radio Frequency based network (RF) by taking into consideration factors that impact the distance or range of the RF signal. (Line of sight, first Fresnel Zone clearance, interference devices).
6. Identify the difference between a gain or a loss in signal strength and what may cause it.
7. Explain the behavior of RF waves so that a working wireless network can be configured (reflection, refraction, diffraction, scattering, absorption, polarization and diversity).
8. Successfully implement and manage as RF-based network by determining the power levels of the RF signal using milliwatts and decibels and signal to noise ratios.
9. Identify the differences among different 802.11 standards based on frequencies and encoding techniques. (DSSS and HR/.DSSS, OFDM, FHSS, Infrared and MIMO).
10. Test products in actual implementation to determine the true range (distance) and coverage (availability) provided by a device.
11. Configure a device so that is knows which signal to monitor by knowing the difference between RF noise and intentional RF by looking at frequencies and channels and thus provide the needed coverage in most facilities
12. Set up a PAN using Bluetooth technology and already established channels (ie FHSS).
13. Troubleshoot existing wireless implementations based on if they are in ad hoc/IBSS (peer-to-peer) or infrastructure modes/BSS (client-server) and ESS.
14. Create a name for the network the wireless device is on based on the SSID
15. Set up the client station to find a WLAN by configuring it with active or passive scanning and then authenticate and associate to the network.
16. Configure medium and large wireless networks so that devices can roam moving seamlessly from one BSS to another without losing the network connection.
17. Select the appropriate wireless devices for more complex infrastructure configurations as well as discuss common and unique features.
18. Evaluate, select, install, configure and troubleshoot antennas to propagate the wireless signals into the air
19. Use the correct connectors, amplifiers and mounting kits to set up a wireless device on a wireless network
20. Suggest the most appropriate client devices and software for a wireless network.
21. Install client software that comes with the client wireless client.
22. Define requirement, perform site surveys and document recommendations for planning a wireless LAN
23. Do any of the four types of site survey; i.e. manual automated, assisted and predictive.
24. Use a simple NetStumbler protocol analyzer to determine what security is being used, the data rate of the communications, and the type of data being transmitted.
25. Use a software or hardware spectrum analyzers to gain insight into the RF activity in a spectrum or frequency range.
26. Identify different interference sources so that you can install a Wi-Fi network that functions effectively.
27. List the recommended documents that need to be filled out during a site survey
28. Be able to deploy a wireless network based on the environment in which the wireless connections are implemented.
29. Implement a wireless network by using step-by-step procedures in a case study.
30. Transition to maintenance mode once the wireless network has been installed, by applying firmware, updating client drivers and updating clients and servers.
31. Create best practices that allow administrators of wireless networks to optimize a wireless LAN.
32. Determine the benefits and drawbacks of a single MAC model and a Split MAC model within an AP
33. Resolve multipath and hidden path node problems.
34. Intuitively select amongst four different troubleshooting processes and then initiate it; REACT, OSI model, Hardware/Software model, and Symptoms, Diagnosis and Solution.
35. Explain the inherent weaknesses in standards-based 802.11 networks that use WEP, MAC filtering and disabling the broadcast SSIDs from access points

36. Make a wireless network secure by implementing the newest version of Clause 8 in a secure fashion based on original 802.11 amendments
37. Identify the common attack methods used against WANs in order to better comprehend security solutions; eaves dropping, hijacking, man-in-the-middle attacks, denial of service attacks, management interface exploits, encryption cracking, authentication cracking, MAC spoofing, peer-to-peer attacks and social networking
38. Research the governing bodies that define and enforce regulations related to many different knowledge domains and information management and know their policies.
39. Explain the concept of implementing a very large WLAN that uses complex architectures so that ongoing administration of the network is much less time consuming. This is not the same implementation many simple individually configured APs and clients.
40. Visualize the benefits of configuring a wireless mesh network for areas that would have had many LOS obstructions and data routing redundancy.
41. Use WLAN power management features implemented in 802.11 WLAN devices in order to provide longer battery life.
42. Prepare for the CWTS certification exam.