Murrieta Valley Unified School District **Board Submission: May 2018**
HIGH SCHOOL COURSE OUTLINE

Course Title: Cybersecurity

Department: Career Technical Education

Course #: 7573

Grade Level/s: 11 - 12

Length of Course: Year

Prerequisite/s: Successful completion of Exploring Computer Science and AP Computer Science Principles or Approval of Instructor

UC/CSU (A-G) Req: G (Pending)

Brief Course Description: The cybersecurity course prepares students for a career in network administration and technical support with a focus on cybersecurity. The course includes a series of technical subjects that provide hands-on knowledge and skills in computer hardware, operating systems, networking and security concepts. Industry-based curricula are utilized in a networked environment to assist in preparing students for industry recognized certifications. Students will engage in intricate problem-solving exercises that mimic real world technical challenges. The program targets students preparing for careers in information and communications technology and cybersecurity. Activities in this course include work-based learning that connects students to industry and the local community.

I. GOALS

The students will:

A. Analyze ethical issues in hacking/cybersecurity
CTE Anchor Standards – Ethics and Legal Responsibilities

B. Diagnose and remove viruses from a computer system
CTE Anchor Standards – Technical Knowledge/Skills and Problem Solving & Critical Thinking

C. Create a “Map of Network Topology” and determine IP address schemes
CTE Anchor Standards – Technology

D. Install, configure and share a network printer
CTE Anchor Standards – Technical Knowledge/Skills

E. Troubleshoot and repair a computer documenting findings, actions and outcomes

CTE Anchor Standards – Academics, Problem Solving & Critical Thinking and Technical Knowledge/Skills

F. Install and configure a TCP/IP network, applying the suite of network commands and protocols to troubleshoot and monitor performance issues
CTE Anchor Standards – Technical Knowledge/Skills and Problem Solving & Critical Thinking

G. Collect quantitative and qualitative data on preferred operating systems to create/analyze database records
CTE Anchor Standards – Communication and Demonstration and Application

H. Engage in mock interviews that represent industry practices
CTE Anchor Standards – Career Planning and Management

II. OUTLINE OF CONTENT FOR MAJOR AREAS OF STUDY

Semester 1

A. Security Environment
   1. Threats, vulnerabilities and consequences
   2. Advanced persistent threats
   3. State of security today
   4. Why security matters to the Department of Defense

B. Ethics in Technology
   1. Code of ethics and conduct
   2. Political issues and impact
   3. Legality and reporting
   4. COPPA, HIPAA and U.S. Patriot Act
   5. Client confidentiality, protection and intellectual property

C. Networking Principles
   1. Suite of Internet Protocols
   2. Medium access control in LANs and routing
   3. OSI Model
   4. Architecture of networks
   5. TCP/IP, DNS and Command-Line Interface (CLI)

D. Hardware Fundamentals
   1. Key components (CPU, RAM, ROM, CMOS, BIOS, etc)
   2. Configuration and compatibility
   3. Storage Devices
   4. Motherboards and microprocessor genealogy

E. Principles of Cybersecurity
   1. Interrelated components of computing environment
   2. Cybersecurity models (CIA triad, star model and Parkerian hexad)
   3. SSP (System Security Plan)
   4. Architecting the enterprise

Semester 2

A. Risk Management
   1. Types of risk
   2. Risk strategies
   3. RMF (Risk Management Framework)
   4. Security standards and controls

B. Operating Systems
   1. Windows, Mac, Android, Linux, Unix, etc.
   2. File management, command line and syntax
   3. IRQ, DMA and I/O address system resource allocation
   4. Recovery, restore, boot failure and diagnosis tools

C. Network Security
   1. Antivirus software and scanners
   2. Firewall components (ports, ACL, port forwarding, etc.)
   3. Securing the network perimeter
   4. Configure user and file security (NTFS permissions)
   5. Prevention (secure passwords, internet browser options and data issues)

D. Security Threats
   1. DDoS (UDP Flood, SYN Flood, Ping of Death, Zero Day, etc.)
   2. Viruses, Worms and Malware
   3. Ransomware, Spyware and Trojans
   4. Social Engineering, Spear Phishing, Pretexting and Hacking

II. ACCOUNTABILITY AND DETERMINANTS

A. Key Assignments
   1. Browser Security Project -- Students will research the top reasons why computer systems are compromised or infected while surfing the Internet. They will compare outcomes with available browser security settings to identify a best practice procedure. This will include testing settings and taking screen shots of each confirmed step to create a “How to Secure Your Windows Browser” guide. Students will conduct peer reviews of projects to include testing, critiquing and providing feedback.
   2. Malware Analysis Project – Students will investigate the two methods of examining malware through Dynamic and Static Analysis. They will execute malware and observe run-time behaviors (dynamic) and dissect source code without malware execution (static). Low-interaction and high-interaction use of computers (honeypots) will be used to observe live security vulnerabilities. Students will be documenting their detections and developing a Security Action Plan.

B. Assessment Methods
   1. Skill mastery and quality of work
   2. Classwork/Homework
   3. Performance Tasks
   4. Projects
   5. Presentations

6. Quizzes
7. Response Questions
8. Multiple Choice Tests
9. End of Unit Exams
10. Semester Final Exams
11. Oral language Personal Communications Skills

III. INSTRUCTIONAL MATERIALS AND METHODOLOGIES

A. Required Textbook(s):
Title: Cybersecurity Essentials
ISBN: 9781119362395
Format: Print
Author(s): Brooks, Craig and Short
Publisher: Sybex Publishing (division of Wiley Publishing)
Year: 2018

B. Supplementary Materials:
1. VMWare
2. Codehs.org online curriculum
3. Router/Switches/Computers
4. Cabling and Fiber termination kits

C. Instructional Methodologies
1. Teacher lectures/direct instruction
2. Class discussions
3. Cooperative learning
4. Guided Inquiry
5. Simulation activities
6. Close reading
7. Collaborative peer review
8. Teacher and student lead inquiry
9. Flowchart development
10. Group project/presentations