Based on ABET CAC Student Learning Outcomes

1. **Course Number and Name:**
   CSET 4850 Network Security Fundamentals
2. **Credits and Contact hours:**
   Credits: 4 hours, Contact: 3 lecture hours; 1 lab hours
3. **Instructor's or course coordinator's name:**
   Weiqing Sun
4. **Text book, title, author, and year:**
   Introduction to Computer Security, Matt Bishop, 2004
   a. **Other supplemental materials:**
      None
5. **Specific Course Information:**
   a. **Brief description of the content of the course (catalog description):**
      Theory and practice of network security. Topics include firewalls, Windows, UNIX and TCP/IP network security. Security auditing, attacks, viruses, intrusion detection and threat analysis will also be covered.
   b. **Pre-requisites, or co-requisites:**
      CSET 4750
6. **Specific goals for the course:**
   a. **Specific outcomes of instruction:**
      1. Understand secret key, message digest, and public key algorithms, and how each is used
      2. Understand and be able to use authentication and key agreement protocols.
      3. Identify attacks and efficiently block the attacks.
      4. Develop firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as UNIX.
      5. Study a security related problem and recommend solutions.
   b. **Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course: 1, 2, 3, 4**
      1. An ability to analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions;
      2. An ability to design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline;
      3. An ability to communicate effectively in a variety of professional contexts.
      4. An ability to recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
7. **Brief list of topics to be covered:**
   1. Introduction, Ethics and Expectation, Fundamentals of Network Security
   2. Access control

3. Security Policies
4. Symmetric Key Cryptography
5. Public Key Cryptography
6. Key Management and Public Key Infrastructure (PKI)
7. Authentication
8. Security Design Principles
9. Confinement Problem
10. Auditing
11. Malicious Logic
12. Intrusion Detection
13. Network Security
14. System Security
15. Program Security
16. Advanced Research Topics