K1 Level

Unit-1

1. _____ is a system security attribute that refers to the delivery of functional capability when required.
   a) Antivirus
   b) Performance
   c) **Availability**
   d) None of the above

2. _____ is a measure of the amount of data that can simultaneously traverse through a telecommunications line.
   a) **Bandwidth**
   b) Bit
   c) Gigabyte
   d) None of the above

3. _____ is an information systems security management certification offered by the Information Audit and Control Association. Certification requires a test of an enterprise security body of knowledge as well as independent attestation of education and experience.
   a) Certificate Information Security Manager(CISM)
   b) Certified Information Secure Manager (CISM)
   c) **Certified Information Security Manager (CISM)**
   d) None of the above

4. _____ is the act of charging an Internet site for a user selecting a link to it, when no real person clicked on the link, often accomplished with automated software.
   a) **Click fraud**
   b) Hacking
   c) Double Click
   d) None of the above

5. _____ is a file integrity detection and alerting system, such as tripwire.
   a) Host Instruction Detection System (HIDS)
   b) **Host Intrusion Detection System (HIDS)**
   c) Host Information Detection System (HIDS)
   d) None of the above

6. _____ is a system that allows software on an electronic device to communicate with multiple satellites in order to determine its location on earth.
   a) **Global Positioning System (GPS)**
   b) General Packet Radio Services (GPRS)
   c) Global System for Mobile Communications (GSM)
   d) None of the above

7. _____ is a system that monitors and controls physical processes.
   a) **Industrial control system (ICS)**

b) Antivirus
c) Protocol
d) None of the above

8. _____ Software that monitors file attributes to detect and alert when files are modified or deleted.
   a) Antivirus
   b) Firmware
   c) **Tripwire**
   d) None of the above
9. _____ is an addressable place in memory on a computer that sends and receives network communications.
   a) **Port**
   b) Drive
   c) RAM
   d) None of the above
10. _____ is the ability to use the resources of a computer without being collocated with it, usually via a phone line or Internet connection, but may be wireless or satellite enabled.
    a) Direct access
    b) **Remote access**
    c) Sequential access
    d) None of the above
    e)

Unit-2

1. _____ is an electronic device deployed to intercept all traffic sent and received between two networks for the purpose of restricting the type of data protocols allowed between them.
   a) Firewall
   b) port
   c) switch
   d) None of the above

2. _____ is "e" is short for electronic, and e-commerce refers to business conducted over the Internet.
   a) e-Commerce
   b) e-mail
   c) e-communication
   d) None of the above

3. _____is a Software created for the purpose of executing CAAS.
   a) Crimeware
   b) Firmware
   c) Firewall
   d) None of the wall

4. _____ Software designed with malicious intent, to spy on user activities, steal data, or damage the integrity of targeted computers.
   a) Aware
   b) Firmware

c) **Malware**
d) None of the above

5. _____ is a computer program that allows hardware to be controlled using a standard set of utilities that are the same no matter what hardware is being accessed.
   a) **Operating system**
   b) DOS
   c) CMOS
   d) None of the above
6. _____ is a generic term for a department whose mission is to ensure that systems function as expected.
   a) Function
   b) Performance
   c) **Operations**
   d) None of the above
7. _____ is a software security quality assurance technique that checks for known vulnerabilities, a form of badness-ometer.
   a) Black box test
   b) **Penetration test**
   c) White Box Test
   d) None of the above

8. _____ Information use to identify a user and authenticate that user to a computer, also referred to in shortened form as *credentials*.
   a) **Login**
   b) Personal
   c) Public
   d) None of the Above
9. _____ a department within an enterprise whose mission is to detect and respond to security incidents.
   a) Secret operating center (SOC)
   b) **Security operations center (SOC)**
   c) Service opting center (SOC)
   d) None of the above
10. _____ is a cryptography-enabled method of confidential communication between multiple computers over a public network.
    a) **Virtual private network (VPN)**
    b) Encryption
    c) Virtual Public Network (VPN)
    d) None of the above

Unit-3

1. _____ Software that allows an operating system to allocate its resources to only authorized users by interrupting all resource requests and comparing them to access control lists before allowing them to be answered.

   a) **Reference monitor**
   b) Resource manager
   c) Requirement monitor
   d) None of the above

2. _____ Malware that enables remote access.
   a) Remote authorization tool (RAT)
   b) Remote Authentication Tool (RAT)
   c) Remote access tool (RAT)
   d) None of the above

3. _____ Protocol for data communications between an operating system and peripherals.
   a) **Universal serial bus**
   b) Universal serious bus
   c) Unique service bus
   d) None of the above

4. _____ is the context of cyberspace, refers to information represented by data.
   a) Data
   b) Knowledge
   c) **Content**
   d) None of the above

5. _____ is an adjective to describe a system that may be accessed via the public Internet.
   a) **Internet-facing**
   b) Internet-firewall
   c) Information
   d) None of the above

6. _____ the term originated as a canned meat product, but now refers to undesirable messages, most frequently email.
   a) **Spam**
   b) E-mail
   c) Internet
   d) None of the above

7. _____ Information that can be used to create consumer relationships of financial liability.
   a) Professional Identification Number (PIN)
   b) Professional Identification Information (PII)
   c) Personally identifiable information (PII)
   d) None of the above

8. _____ is a network-connected electronic device which has communication capabilities.
   a) **Node**
   b) switch

c) Port
d) None of the above

9. _____ is a messaging structure used to communicate commands within industrial control systems.
   a) Serial Bus
   b) **Modbus**
   c) chip
   d) None of the above
10. _____Disclosing embarrassing or otherwise damaging personal information about someone on the Internet.
   a) **Doxing**
   b) Boxing
   c) Malware
   d) None of the above

Unit-4

1. _____ Created by Executive Order 13231 in 2001, the NIAC advises the U.S. President on the security of information systems for critical infrastructure.
   a) National Information Advisory Council (NIAC)
   b) National Instruction Advisory Council (NIAC)
   c) National Infrastructure Advisory Council (NIAC)
   d) None of the above

2. _____ is a cyber security professional who emulates cyber criminal behavior in order to test systems security. The origin of the term is old Western movies where the bad guy typically wore black while the good guy wore white.
   a) Black hat
   b) Red hat
   c) White hat
   d) None of the above

3. _____ is a process of examining systems and/or software to determine how it works.
   a) Reverse engine
   b) Reverse engineer
   c) Reverse programming
   d) None of the above

4. _____ is a computer that is designed to intercept network communications bounds for a given destination, such as the Internet, and check it against a set of rules for acceptable use prior to allowing it to continue to its destination.
   a) **Proxy servers**
   b) CPU
   c) Serial Bus
   d) None of the above

5. _____ is a method of electronic communication used to convey information on the Internet.
   a) Internet protocol (IP)
   b) Information Management
   c) Information Control
   d) None of the above

6. _____ is a more recent specification and update to SSL.
   a) **Transport Layer Security (TLS)**
   b) Transport Layer Protocol
   c) Transmission Layer protocol
   d) None of the above

7. _____ Copying network traffic to a device for which it was not addressed, for the purpose of eavesdropping on network communications.
   a) Network identification
   b) **Network listening**
   c) Network Control
   d) None of the above
8. _____ is a set of network addresses for which communications security is managed by surrounding them with common traffic chokepoints with similar traffic filters.
   a) Network port
   b) Network resource
   c) **Network zone**
   d) None of the above

9. _____ is a business that sells connections to the Internet.
   a) **Internet service provider (ISP)**
   b) Information service provider
   c) Intranet service provider
   d) None of the above

10. _____is an explosive configured with trigger mechanisms customized to explode when approached by a specific target.

    a) Information explosive device
    b) Instruction explosive device
    c) **Improvised explosive device (IED)**
    d) None of the above

Unit – 5

1. _____ software representation of information used to view information on and/or operate computers.
   a) Command prompt
   b) Procedure oriented
   c) Graphical user interface (GUI)
   d) None of the above

2. _____ the standard name for a proposed Internet technology standard, indexed by number, title, author, and keywords.
   a) Request for access
   b) **Request for comment (RFC)**
   c) Remote sense access
   d) None of the above

3. _____ is a generic term to refer to all secure communications protocols that allow traffic between end users and web servers to be encrypted.
   a) Secure Socket Layer (SSL)
   b) Transmission Control Layer
   c) Transport Layer
   d) None of the above

4. _____ is an intentional shutdown of system communications.
   a) Graphical User Interface (GUI)
   b) Command Prompt
   c) **Denial of service (DOS)**
   d) None of the above

5. _____ **is** the process of using cryptography to hide data content.
   a) **Encryption**
   b) Decryption
   c) Security
   d) None of the above

6. _____ is a device that allows manual command entry in a SCADA system.
   a) **Remote terminal unit (RTU)**
   b) Request processing unit (RPU)
   c) Central processing unit CPU)
   d) None of the above

7. _____ Deprivation of the ability to view systems status, or otherwise corrupt the data normally viewed by a system operator.
   a) Control panel
   b) **Denial of view**
   c) Derivation view
   d) None of the above

8. _____is a system security attribute that refers to its ability to restrict access to information to an identified set of system users.
   a) **Confidentiality**
   b) Accuracy
   c) Perfection
   d) None of the above

9. _____a generic term to refer to any process by which messages are sent electronically, via server protocols such as email, chat, or peer-to-peer protocols.
   a) E-mail

b) **Messaging**
c) Contact
d) None of the above

10. _____ is a cryptographic protocol that allows users to verify the integrity of email and its provenance.
    a) **Domain Keys Identified Mail (DKIM)**
    b) Encryption
    c) Decryption
    d) None of the above

16UCS5E1 - CYBER SECURITY

K2 Level Questions

Unit – I

1. **Define Antivirus:** Software designed to detect and minimize the damaging impact of malicious self-replicating software.

2. **What is Badness-ometer:** A scale on which every reading indicates security is bad.

3. **Explain about Certified Information Security Auditor (CISA):** A technology audit certification offered by the Information Audit and Control Association (formerly the EDP Audit Association). Certification requires a test in information systems audit tools and techniques as well as independent attestation of education and experience.

4. **Explain about Chief Information Security Officer (CISO):** A title associated with the highest ranking individual whose sole function within an organization is to manage an organization-wide security program.
5. **Define Freeware:** Software that anyone may use, though authorized use may require acceptance of a license agreement. Often confused with Open Source, but different because freeware source code is not always available.

6. **Defend Compensating control:** A security measure that mitigates the security risk of a vulnerability for which a primary control is ineffective. Typically a detection and response capability, the measure would compensate for the lack of system features that would prevent the vulnerability from exploit.

7. **Illustrate Computer Emergency Response Team (CERT):** An organization whose mission is to receive reports of cyber incidents and gather a team qualified and motivated to resolve them.

8. **Define Content filters:** Strings of text that may be compared to data to determine whether it contains specific information, for example, NNN-NN-NNNN where N translated to any number is often used as a content filter for a U.S. social security number.

9. **Explain Control activity:** Any combination of people, process, and technology whose purpose is to achieve a control objective.

10. **What is Control objectives:** Statement of management intention on security posture.

Unit – II

1. **Define Credentials:** information used to identify a user and authenticate that user to a computer; also referred to as *login credentials*.

2. **Explain National Security Telecommunications Advisory Committee (NSTAC):** A committee of telecommunications industry stakeholders whose goal is to develop recommendations for the President of the United States to assure vital telecommunications links through any event or crisis, created under Executive Order 12382.

3. **Defend Explain North Atlantic Treaty Organization (NATO):** An alliance of countries from North America and Europe committed to fulfilling the goals of the North Atlantic Treaty signed on April 4, 1949.

4. **Explain Online behavioral advertising:** Gathering information about an individual's behavior on the Internet in order to provide customized advertising to be displayed to that individual.

5. **What is Defense Industrial Base (DIB):** Companies whose primary customer is the U.S. government.

6. **Define Denial of control:** Deprivation of the ability to enter system commands.

7. **Explain about Dial-back:** A mechanism that records a phone number calling, disconnects the incoming call, and initiates an outbound call to the same number only if it has been previously authorized to connect to that number.

8. **Defend about Discretionary access control (DAC):** Computer access control mechanisms that allow a user who can access data to grant that access to another user without administration collusion.

9. **Explain about Distributed control systems (DCSs):** Systems that allow multiple avenues of administration.

10. **Defend about Distributed denial of service (DDOS):** An intentional shutdown of system communications caused by multiple, independently operating computers whose activities are purposefully coordinated.

Unit – III

1. **Define Distributed Network Protocol (DNP3):** A set of industrial control system communications protocols that segment messages into three components (physical, data, and application).

2. **Explain Domain Name Services (DNSs):** A way to identify at which Internet address the computer corresponds to an Internet Universal Resource Locator.

3. **Defend Domain squatting:** Using a company or individual trademark, copyright, or an identifier similar to register a domain name on the Internet that appears with probability to belong to that company or individual.

4. **Explain about Email:** Originally, email as in e-commerce, where "e" stood for "electronic," now in mainstream vocabulary as email, or messages sent or received using Internet mail protocols.

5. **Defend End user:** a person who uses a computer or mobile device, typically used to refer to those without the advantage of administrative privileges.

6. **Explain about End User License Agreements (EULAs):** Software industry standard verbiage created to form a legal compact between software buyers and sellers.

7. **Define Federal Emergency Management Administration (FEMA):** The U.S. federal government agency with primary responsibility for responding to a domestic consequence management incident.

8. **What is Field instrumentation:** Physical sensors and mechanism with electronic circuits that integrate with industrial control systems (ICSs).

9. **What is FUD Factor:** Fear, uncertainty, and doubt in the context of a discussion about security, usually introduced in order to influence a spending decision.

10. **Define Hactivism:** Political protest conducted in cyberspace. Typically accomplished by sabotaging one or more government or enterprise websites that are associated with the political protest target.

Unit – IV

1. **Defend Certificates:** Cryptographic keys which may be verified to be associated with organizations or individuals.

2. **What is Identity theft:** Impersonation of an individual using data that are associated with computerized records that identify the individual.

3. **Explain Internet Corporation for Assigned Names and Numbers (ICANN):** The organization that sets the rules for determining how Internet users may claim ownership to address space and name space.

4. **Explain Crime as a service (CAAS):** Cyber attacks for hire, such as denial of service attacks.

5. **What is Cryptography:** A method of hiding data in bit format by using complex methods of diffusion and confusion in combination with large sequences of other bits (keys). In this context, diffusion means disseminating the message into a statistically longer and more obscure format, and confusion means to make the relationship between the message and the key very long and involved.

6. **Define Cyber security:** Security modified with an adjective referring to the cyberspace properties of the thing to be secured. In general, cyber security refers to methods of using people, process, and technology to prevent, detect, and recover from damage to confidentiality, integrity, and availability of information in cyberspace.

7. **Defend Cyberspace:** The global collection of electronic circuits that allow people to share information without physical connectivity.

8. **What is Impersonation:** A method by which a user may manipulate data within an authentication session or order to appear to the authenticating system as a different individual, who is also an authorized system user.

9. **Explain Information Systems Audit and Control Association (ISACA):** An international association of cyber security and audit professionals who certify members for the professional practice of Information Systems Audit, Security, Governance, and Risk Management.

10. **Define Information technology (IT):** Refers in general to the computer systems and associated management processes designed to achieve organizational goals for information processing.

Department of Computer Science

16UCS5E1 - CYBER SECURITY

K3 Level Questions

Unit – I

1. Explain about the technological operations carried out by Cyber Security Policy.
2. Explain the Counter Measures of Cyber Security.
3. Sketch what is cyber security policy?
4. Explain the Challenges of cyber security.
5. Sketch the evolution of cyber security.
6. Explain about e-com in detail.
7. Explain about internet in detail.
8. Write about the technical operation of cyber security.
9. Write about the technical configuration of cyber security..
10. Explain in detail about laws in security

Unit – II

1. Generalize security management goals.
2. Explain about policy as a project of cyber security.
3. Explain short notes on a) Cyber security metrics b) Security management goals
4. Explain about a) Arriving at goals b) Cyber security documentation
5. Explain about counting vulnerabilities
6. Explain about security framework
7. Explain about the objectives of security policy
8. Explain the role of cyber security in E-COM
9. Explain the ICS in cyber security
10. Write in detail about the cyber security management

Unit – III

1. Elucidate the evolution of internet.
2. Explain documentation of cyber security.
3. Give a sketch about a) Internet names and numbers b) Email and messaging
4. Give a sketch about a) Geolocation b) Privacy

5. Give a sketch about the catalog format in cyber security.
6. Explain in detail about cyber security policy taxonomy
7. Give a sketch on network neutrality?
8. Give a sketch Malvertising?
9. Give a note on Impersonation?
10. Discuss about cyber sabotage?

Unit – IV

1. Explain about Catalog Format.
2. Explain about cyber security issues.
3. Generalize about fiduciary responsibility, risk management in cyber management issues.
4. Generalize industrial control system in the field cyber security.
5. Write about Professional Certification.
6. Discuss about Supply Chain
7. Sketch out Security Principles in security
8. Write short notes on Banking and finance
9. Write about Health Care.
10. Discuss about Industrial Control systems

Unit – V

1. Discuss about the Bombing of New York's World Trade Center on February 1993.
2. Give a sketch about Cyber Attacks against the United States Air Force.
3. Give a sketch about U.S Federal cyber security strategy
4. Give a sketch about on Espionage and nation-state actions.
5. Analyze the Rise of Cyber Crime.
6. Write about Brief History of Cyber Security Public Policy Development in the U.S. Federal Government.
7. Give a sketch about Citibank Caper, June–October, 1994: How to Catch a Hacker.
8. Briefly Generalize National Strategies.
9. Give a sketch on Solar Sunrise - 1998.
10. Write about Presidential Decision Directive -1998.

Department of Computer Science

16UCS5E1 - CYBER SECURITY

K4 Level Questions

Unit – I

1. Analyze about cyber security policy.
2. Analyze in detail about Domain of cyber security policy.
3. Categorize the following on a) Productivity b) Countermeasures.
4. Analyze in detail about e-Commerce.
5. Categorize Laws and Regulations of Cyber Security Policy.

Unit – II

1. Analyze in detail about Cyber Security Metrics.
2. Categorize cyber security management goals? Explain.
3. Analyze in detail about cyber security vulnerabilities.
4. Differentiate security frameworks followed in cyber security?
5. Classify security policy objectives.

Unit – III

1. Classify about any two governance issues.
2. Classify Net Neutrality and Copyrights & Trademarks.
3. Analyze about cyber user issues.
4. Categorize cyber conflict issues in detail.
5. Classify Email & Messaging in detail.

Unit – IV

1. Analyze about Cyber Management Issues Fiduciary Responsibility.
2. Explain about Risk Management in cyber security.
3. Classify Professional Certifications in cyber security.
4. Discuss in detail about Supply Chain.
5. Analyze in detail about Security Principles in cyber security.

Unit – V

1. Give a neat sketch about U.S. Federal Cyber Security Strategy.
2. Give a brief note on History of Cyber Security.
3. Give a brief note on Citibank Caper, June–October, 1994: How to Catch a Hacker.
4. Analyze the Rise of Cyber Crime.
5. Differentiate Espionage and Nation-State Actions.

Department of Computer Science

16UCS5E1 - CYBER SECURITY

K5 Level Questions

Unit -1

1. Elaborate Cyber Security Policy.
2. Compare and contrast Strategy vs Policy.
3. Appraise all the technology operations available in cyber security.
4. Judge all the technology configurations available in cyber security.
5. Evaluate a) Laws and Regulations b) Enterprise Policy in cyber security concern.

Unit-2

1. Criticize Tone at the Top in detail.
2. Appraise the following cyber security management lists
   a) Arriving at goals. b) Cyber Security Documentation.
3. Elaborate about Catalog Format.
4. Judge the Cyber Security Policy Taxonomy in brief.

Unit-3

1. Elaborate about Malvertising in a cyber scenario.
2. Elaborate the cyber crime, attacks and causes.
3. Criticize about copyrights and trademarks.
4. Elaborate about Intellectual Property Theft.
5. Criticize a) Cyber Warfare b) Cyber Sabotage in cyber espionage.

Unit-4

1. Elaborate about Research and Development.
2. Compare Cyber Infrastructure Issues in detail.
3. Appraise about Banking and finance.
4. Judge about Health care.
5. Appraise Industrial Control systems in the concern of cyber security.

Unit-5

1. Elaborate the Policy Response to Growing Espionage Threats: U.S. Cyber Command.
2. Evaluate Congressional Actions involved in cyber crime.
3. Criticize the Terrorist Attacks against the United States—September 11, 2001.
4. Appraise Solar Sunrise—1998 in US government sector.
5. Elaborate Joint Task Force—Computer Network Defense (JTF-CND)—1998.