A

• Accountability: The state of being answerable for something.
• Agapeism: An ethical theory that equates good with love and bad with hate.
• Agathism: An ethical theory that views good as an indefinable intrinsic feature of various situations and states and evil as either an indefinable intrinsic feature of other situations and states or simply as the absence of good.
• Alert: An automatic signal that is triggered by an unusual or an unexpected occurrence.
• Altruism: An ethical theory that considers an action as right, if the consequences of that action are favorable to all except the actor.
• **Auditing**: A process of examination or verification of records.
• **Authentication**: The process of determining whether someone is who he or she claims to be or something is what it claims to be.
• **Authorization**: The process of approving or allowing something.
• **Autonomy**: The concept of being independent; to live one’s life free of other influences and being able to reason and act on one’s own and not be manipulated by external forces.
• **Availability**: The state of safely providing access to an asset whenever authorized users want it.

B

• **Behavior**: Activities humans routinely do; conduct, on the other hand.
• **Biometric**: A physical authentication or identifying trait, like a fingerprint.
• **Buffer overflow**: A condition where the process tries to store data beyond its allocated location.

C

• **Ciphertext**: Data after the encryption transformation.
• **Competence**: Having the necessary skills to accomplish an assigned task.
• **Compliance**: The tendency or willingness to agree or yield to something.
• **Computer virus**: Is a computer program, usually software, that can alter the expected running of a computer through modification or destruction of the logical sequence of normal computer instructions.
• **Commitment**: Being obliged to something or someone.
• **Conduct**: The more specific behavior or human activity that involves human management skills.
• **Confidentiality**: The right of and ensuring accessibility to information by all who are legally authorized to access it.
• **Consequentialism**: An ethical theory that considers an act right only if it produces good consequences.

• **Criteria**: Standards for the judgment of things.

• **Cross-site scripting**: A process that allows Web application users to inject malicious code into Web pages that can infect other computers if they visit the infected Web sites.

• **Cyberspace**: “Space” or an environment created by the interconnection of computers and computer-aided devices, and the movement of data between these devices following complex protocols developed by humans.

• **Cynicism**: An old Greek philosophy concerned with virtue and in the belief that virtue was the cause of happiness and the good life.

\[D\]

• **Deontology**: An ethical theory that does not concern itself with the consequences of actions, but rather with the will of the action.

• **Detection**: The process of controlling access to system assets by uncovering criminal acts taking place.

• **Deterrence**: The process of controlling access to system assets by discouraging or preventing acts and activities by either making examples of deviants or making the consequences known.

• **Digital signature**: An electronic signature used in identifying an individual in an electronic exchange of data.

• **Dilemma**: A situation in which a choice must be made between usually two equally bad options.

• **Duty of care**: The individual implicit responsibilities in whatever is done to other individuals in society.

\[E\]

• **Egoism**: An ethical theory that puts an individual’s interests and happiness above everything else.
• **Emotivism**: An ethical theory that maintains that ethical statements are neither true nor false and cannot be proven; they are really only statements about how someone feels.

• **Encryption**: A security process of transforming data from one form into a safer unintelligible form before it is transmitted.

• **Eudemonism**: An ethical theory that equates good with happiness and bad or evil with unhappiness.

• **Exploit**: Anything, including a software code or hardware device, that allows an intruder to take advantage of an existing weakness or a loophole in the system to compromise the system’s integrity.

G

• **Globalization**: A process of bringing world commerce, the arts, and businesses together through cyberspace.

• **Grievance**: A complaint for a perceived wrong or an unfair treatment.

• **Guilt**: One’s feeling of remorse, regret, or responsibility for negative circumstances, something unaccomplished, or a misdeed.

H

• **Hedonism**: An ethical theory that equates good with pleasure and bad or evil with pain.

I

• **Information infrastructure**: An environment consisting of computer or computer-related hardware, software to run on the hardware, and humanware to run both.

• **Integrity**: The state of having expected quality; a state of being honest.
L

- **Licensure**: A process of granting a license for something.

M

- **Malware**: An acronym for malicious software.

N

- **Nonrepudiation**: A cryptographic process of guaranteeing that senders of electronic messages do not turn around and deny them.

P

- **Penalty**: A punishment or a handicap encountered for failing to meet a set standard.
- **Plaintext**: Data before it is encrypted into an unintelligible form.
- **Platonism**: A Greek philosophy from Plato that revolves around a theory or doctrine of ideas of something whose originality, in particular, does not exist in the reality of the time-space continuum, except through instantiation of the idea.
- **Privacy**: State of being secluded.
- **Proxy server**: A network server sitting between two servers, for example, a client server on one side and a Web-server on the other, with the purpose of filtering all traffic to improve performance and security.

R

- **RAM**: Random access memory.
- **Relativism**: An ethical theory that takes right and wrong to be relative to society, culture, or the individual.
- **Responsibility**: The state of having authority and being answerable for something.
• **Risk:** The probability of encountering harm or danger.
• **ROM:** Read only memory.

**S**

• **S/Key:** An authentication security protocol by Bellecore that uses a one-time challenge-response password to access a system resource.
• **Sanctions:** A series of penalties for failing to meet specified standards.
• **Security:** A state of being free from risk, harm, or danger.
• **Sniffers:** Devices or software code intended to illegally monitor network traffic.
• **Software buyers:** All people who buy or use finished software from the developer to satisfy a need.
• **Sophism:** An ancient Greek philosophy that emphasizes rhetoric, rather than virtue.
• **Spam:** An unwanted and unsolicited e-mail or any other electronic message.
• **Spyware:** A computer program, usually software, that once launched on a user’s computer, collects all of the information it chooses, without consent of the computer user.
• **Standards:** An accepted model for comparisons.

**T**

• **Threat:** The probability of an occurrence of harm or danger.
• **Trust:** The state of having faith or confidence in an individual or a thing.

**U**

• **Utilitarianism:** An amoral theory that considers an act as right only if it produces good consequences.
Vulnerability (computer): The presence of a weakness or a loophole in a system that lets an attacker exploit the system.