




## Assignment

Module Name	BDSE-ISE-IT Security
Course Name	IT Security
Assignment Title	Explain

Learner Name	Francis Roel L. Abarca – bdse-0922-113
--------------	--

Learner declaration	
<p>I certify that the work submitted for this assignment is my own and research sources are fully acknowledged.</p>	
Student signature: 	Date: 2/17/2024

## Task Wise Solutions:

1. List the various Infosec Planning Types
  - a. Application Security
    - Protects software vulnerabilities in web and mobile applications.
  - b. Infrastructure Security
    - Protects the entire technological infrastructure, including both hardware and software systems.
  - c. Cryptography
    - Secures communication to ensure only intended recipients can view and decipher it.
  - d. Incident Response
    - The organization's plan for responding to, remediating, and managing the aftermath of a cyberattack or another disruptive event.
  - e. Contingency Planning
    - Provides resilience needed to respond to technical disruptions and ensure the system is available.
2. Explain what is InfoSec Policy
  - a. An InfoSec Policy is a set of rules enacted by an organization to ensure that all users of networks or the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. It governs the protection of information, which is one of the many assets a corporation needs to protect.
3. List the 3 general categories of InfoSec policy and explain them
  - a. Acceptable Encryption and Key Management Policy
    - This policy outlines the acceptable methods for encryption and the management of encryption keys.
  - b. Data Breach Response Plan
    - This policy outlines the steps to be taken in the event of a data breach.
  - c. Disaster Recovery Plan Policy
    - This policy outlines the steps to be taken to recover and restore operations in the event of a disaster.
4. List the components of Information Security Planning
  - a. Confidentiality
    - Ensuring that information is accessible only to those authorized to have access.
  - b. Integrity
    - Safeguarding the accuracy and completeness of information and processing methods.
  - c. Availability
    - Ensuring that authorized users have access to information and associated assets when required.

- d. Information System Contingency Plan (ISCP)
  - Contains information about the system hardware and software, application and data backups, dependent processes, data interfaces, support staff and vendors, recovery priorities, and plan maintenance.
- 5. List various professional certifications for InfoSec consultants.
  - a. CompTIA Security+
  - b. EC-Council Certified Ethical Hacker (CEH)
  - c. (ISC) Certified Information Systems Security Professional (CISSP)
  - d. ISACA Certified Information Security Manager (CISM)
  - e. ISACA Certified Information Systems Auditor (CISA)
  - f. (ISC) Certified Cloud Security Professional (CCSP)
  - g. CompTIA CASP+
  - h. Offensive Security Certified Professional (OSCP)