**IT Security & Risk Management**

**1. Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data. Companies often grant access to information and assets to staff even if it is not relevant to that member of staff’s role. Describe access control methodologies and implementation for purpose of security? Give detailed justifications for your recommendations. (10 Marks)**

**Ans 1.**

**Introduction:**

**Access Control:**Security approaches used in a computing environment to assist govern who can examine what resources within an organization are known as access control. The primary notion of access control is to reduce the risk to organizations as much as possible. Physical access control and logical access control are the two types of access control that can be used. The physical access control system helps to restrict access to certain buildings, rooms, campuses,

Its Half solved only

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session September 2021,**

your**last date is 28th Aug 2021**.

https://ssl.gstatic.com/ui/v1/icons/mail/images/cleardot.gif

Lowest price guarantee with quality.

Charges**INR 199 only per assignment.**For more information you can get via mail or Whats app also

Mail id is [aapkieducation@gmail.com](mailto:aapkieducation@gmail.com)

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

Contact no is +91 87-55555-879

**2. As a term, *people, process, and technology (PPT)* refers to the methodology in which the balance of people, process, and technology drives action: People perform a specific type of work for an organization using processes (and often, technology) to streamline and improve these processes. What do you mean by security awareness for people, process, and technology? (10 Marks)**

**Ans 2.**

**Introduction:**

**Security awareness:**Organizational security awareness is defined as the attitude and knowledge held by members of an organization about the protection of the firm's physical and informational assets. Several firms provide formal security awareness training to their workers when they first begin working for the company and then on an ongoing basis after that. Workplace security, security badges, computer security problems, methods of preserving sensitive information,

**3. A database managed by an Indian state government healthcare agency was left connected to the Internet without a password, where it exposed more than 12.5 million medical records for pregnant women. Records go as far back as five years, to 2014, and include detailed medical information for women who underwent an ultrasound scan, amniocentesis, or other genetic testing of their unborn child. The database belonged to the Department of Medical, Health and Family Welfare of a state in northern India. The reason is that the database is still available online without a password. The good news is that the medical records have been removed from the database. However, removing these records wasn't an easy task and it took more than three weeks to have them taken offline. The database was discovered by Bob Diachenko, a security researcher with cyber-security consulting firm Security Discovery, in early March 2019. The database was eventually secured with the help of the experts, but the entire process took three weeks, during which time the server and the medical records remained exposed for anyone to download. The government agency secured the leaky server after 3 weeks of intial discovery. While the database did not contain information about all pregnancies recorded inside the unnamed Indian state, it did contain medical records for women who suffered pregnancy complications and abortions, data that some families would have liked to remain private, due to obvious reasons.**

**a. What changes would you suggest to prevent such oversight in future? (5 Marks) –**

**Ans 3a.**

**Introduction:**

**Cybersecurity:**

Cybersecurity, also known as information technology security, is a strategy that protects networks, data, computers, mobile phones, servers, electronic systems, and other similar devices from being attacked or threatened by malicious software. These dangers can be split into three categories: cyber-attacks, cybercrime, and cyber-terrorism, respectively. Network security,

**b. With reference to the above case discuss the data privacy standards and guidelines in India vis a vis a country such as US, Canada or UK. (5 Marks)**

**Ans 3b.**

**Introduction:**

**Privacy of data:** Data privacy is a subfield of information security that deals with the handling of personal data. It is referred to as information privacy in some circles. Among the topics covered are: how to share data with third parties, whether to share data with other parties, how to