The three tenets of network security are: Confidentiality: For sensitive data, the network must secure data transmissions by limiting access, encrypting the payload or transmission, and ensuring the data is secure at rest. Nonrepudiation in network security is the ability to prevent a denial in an electronic message or transaction by confirming its authenticity. Integrity: The data itself must be accurate and not altered. This means the network must transmit bits and bytes without any errors to ensure data integrity for the user. Availability: Availability ensures that the network, systems, applications, and data are accessible to its users. Without an available network, users cannot access applications or data and perform work. Answer the following question(s): Does a single network control ensure all three tenets of network security? Explain your answer.

**Network security:**

The word "network security" is broad and encompasses a variety of technologies, tools, and procedures. Using both software and hardware technologies, it can be defined as a collection of guidelines and configurations intended to safeguard the reliability, accessibility, and integrity of computer networks and data. Every organization requires some kind of network security solutions in place to protect it from the ever-expanding landscape of cyber threats that exist in the wild today, regardless of size, industry, or infrastructure.

Step 2 of 3

**The fundamentals of network security**

Confidentiality, integrity, and availability (sometimes known as the "CIA trinity") are the three principles that make up the idea of network security. A network can only be deemed safe when all three components are active at the same time.

The goal of confidentiality is to keep private information secure and hidden from the general public. This is related to the availability concept, which aims to maintain data and resource accessibility for individuals with the appropriate access rights. DDoS assaults or equipment malfunction might pose problems with availability. In order to preserve the data dependable, accurate, and trustworthy, the concept of integrity works to protect it from alterations that are either purposeful or unintentional.

Explanation

Measures to maintain confidentiality are intended to guard against illegal information dissemination. The confidentiality principle's goal is to guarantee that confidential information stays confidential and can only be seen or accessed by people who require it to carry out their job responsibilities.

Integrity entails safeguarding data from unauthorized alterations (such as addition, deletion, or change). The goal of the integrity principle is to guarantee that data can be relied upon to be correct and that it hasn't been improperly altered.

Protection of support system operation and assurance that data is entirely accessible at the precise moment (or duration required) when it is required by its users are two aspects of availability. Making sure data is accessible for usage is the goal of availability when it is needed to make decisions.

Step 3 of 3

From the viewpoint of information security, the optimal result is produced by correctly implementing all three Security Triad principles. Take this scenario into consideration: A firm acquires or develops a piece of sensitive data that it intends to use in the course of its operations. Due to its sensitivity, the data should only be accessible to those employees who require it to order to do their duties. It ought to be secured against unauthorized access. This serves as an illustration of the confidentiality concept.

When the individual who needs a data item to carry out a work requirement is ready to utilize it, it must be quickly and reliably accessible (i.e., online) so that the job duty may be completed on time and the organization can carry on processing. This is how the availability principle is described. Finally, computations that affect the organization's next business decisions and investments will use the data. For computations and results that are used to reach judgments to be reliable, the data must be accurate. Integrity refers to the notion that calculations and conclusions can be trusted to be accurate since there is faith that the data has not been unlawfully altered.

**Final Answer**

**Conclusion:**

Confidentiality, integrity, and availability are the fundamental principles of information security. Each component of the information security program needs to be created with one or more of these concepts in mind. They are collectively known as the CIA Triad.