

What is DATA Security? Why is data security important for an organization? Who is responsible for Data security and what other roles do s/he have?

→Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used. The data that any organization creates, collects, stores, and exchanges is a valuable asset. Safeguarding it from corruption and unauthorized access by internal or external people protects your computer from financial loss, reputation damage, consumer confidence, disintegration, and brand erosion. Key pieces of information that are commonly stored by business, be that employee records, customer details, loyalty schemes, transactions, or data collection, need to be protected. This is to prevent that data from being misused by third parties for fraud, such as scams and identity theft.

A database administrator (DBA) is responsible for data security. The responsibility as a DBA will be the performance, integrity and security of a database. Here are some responsibilities of DBA: -

- Software installation and maintenance
- Data extraction, transformation and loading
- Database backup and recovery
- Security
- Performance monitoring
- Authentication
- Capacity planning