**Database Security and Best Practices**

****

**Table of Contents**

[Introduction 4](#_Toc105574798)

[What is a Database? 4](#_Toc105574799)

[Importance of Database Management 4](#_Toc105574800)

[What is Database Security? 4](#_Toc105574801)

[Why is the Database Security Critical? 5](#_Toc105574802)

[Consequences of Poor Database Security 5](#_Toc105574803)

[Database Security Threats: Keeping It Real 5](#_Toc105574804)

[Data Base Management System (DBMS) Privacy Concerns 6](#_Toc105574805)

[1. Human Blunder 6](#_Toc105574806)

[2. Threats From Within 6](#_Toc105574807)

[3. Vulnerabilities in the Company’s Software 7](#_Toc105574808)

[4. Malware 7](#_Toc105574809)

[5. Attacks Made Backup Systems and Injection Threats in SQL/NoSQL 7](#_Toc105574810)

[6. Site Analysis Confidentiality 7](#_Toc105574811)

[Database Security Best Practices 7](#_Toc105574812)

[1. Establish Physical Database Security 7](#_Toc105574813)

[2. Distinct Database Server Software 8](#_Toc105574814)

[3. Configure an HTTPS VPN Connection 8](#_Toc105574815)

[4. Do Not Use the Default Network Ports 8](#_Toc105574816)

[5. Implementing Real-time DBMS Monitoring 9](#_Toc105574817)

[6. Make Use of Web Application and Database Firewalls 9](#_Toc105574818)

[7. Implement Strong Encryption Security Measures 9](#_Toc105574819)

[8. Make Routine Backup Copies of Your Database 10](#_Toc105574820)

[9. Maintain Application Updates 10](#_Toc105574821)

[10. Consider Making Use of a Robust Authentication Process 10](#_Toc105574822)

[11. Make use of Firewalls 11](#_Toc105574823)

[12. Use Security Software and Apps 11](#_Toc105574824)

[13. Exercise Database Encryption 11](#_Toc105574825)

[14 Secure the User Access 11](#_Toc105574826)

[15. Update Regularly 12](#_Toc105574827)

[16. Carry Out Security Testing 12](#_Toc105574828)

[17. Enhance the Customer Experience 12](#_Toc105574829)

[18. Establish Procedures and Steps for Sensitive Datasets 13](#_Toc105574830)

[19. Data Security is Synonymous with Asset Security 13](#_Toc105574831)

[20. Keep Device Security 13](#_Toc105574832)

[Conclusion 13](#_Toc105574833)

# **Introduction**

Life and work have become more efficient and convenient as digital technology and the internet has advanced. The amount of data collected has increased with more internet usage. Data have become a more valuable asset in businesses than ever before. It also increased the need to secure data from cyber threats. Therefore, data security has gained more importance. Data Security refers to procedures for preventing a cyber-attack in a database structure. Data leakage, unauthorized access, and even network outage are severe implications of failing to have a database security plan.

You can maintain the database's reliability by regularly implementing and following defined procedures and database security best practices. This document gives your insight into database security, the significance of security, database threats, and database security best practices.

You must read the article ahead to discover the benefits of database security. Next, what best network security practices can you use to protect your network against threats? Finally, you'll have a plan to keep your data safe while keeping your users and customers satisfied.

# **What is a Database?**

A database is nothing but a collection of various information sequentially to be easily accessible and updated if needed. The database is essential in every field, whether education, hospitals, or industries. For example, if a student's required information like name, address, marks, and percentage, needs to be stored as it is necessary for the school purposes needs to be stored.

So, it is when databases and database systems come into play. You might have used databases and their strategies in everyday life without acknowledging how and what. It simply helps one write the data efficiently and is readily available whenever needed by the necessary person.

# **Importance of Database Management**

* Maintaining various database systems makes a human's life much more straightforward, thus giving more time.
* It provides security options for sensitive information, thus ensuring privacy for confidential works.
* Assures data consistency and provides a reduction in replicated datasets.
* It is available to anybody, anywhere, with good internet connectivity.

· It can be used in different ways depending on the user's work and is also available in various applications and beneficial help.

## **What is Database Security?**

Database security combines controls and countermeasures for securing a database management system. Database security's best practices cover physical and digital data center components and information protection. In other words, Security testing is a strategy for protecting data that comprises tools, policies, and processes.

A database's security decreases once information gets leaked to the public. It protects management information systems from illicit exploitation, illegal access, and hostile intrusions by ensuring security, privacy, and integrity. Security considerations arise because users require access to data items. To ensure the integrity of the data, use as many cryptographic precautions as feasible.

# **Why is the Database Security Critical?**

Data protection is a highly secure operation. As per a study conducted by the Risk-Based Security of 2020, over 36 billion data were hacked between January and September 2020. Such statistics emphasize the importance of adequate database security procedures. Furthermore, the database contains vital information for the company. All of those are highly confidential information in the incorrect hands and can result in the disclosure of the company's and the client's data which could lead to economic devastation for the business. That's why database safety is crucial.

# **Consequences of Poor Database Security**

* Damage to the business's reputation and high chances of the sales going down the hill.
* Expenses of damages are caused by investigating the breach and implementing the right solution.
* Intellectual property compromise
* Penalties and fines for noncompliance
* Large loss of investments and finances of the company

Though the internet and digital technology have made our personal and work-life simpler, they have also raised the risks to businesses and consumers. Database security practices differ from websites, and physical actions, software solutions, and even employee education are part of the former. Organizations can use "in the cloud" databases to organize and store massive amounts of data. However, it is crucial to secure your site to limit the attack routes that cybercriminals might use.

Though the internet and digital technology have made our personal and work-life simpler, they have also raised the risks to businesses and consumers. Database security practices differ from websites, physical actions, and software solutions for every organization. However, it's crucial to protect your website or sensitive information from the attack routes of cybercriminals.

# **Database Security Threats: Keeping It Real**

It's a fantastic idea to start a business via online mode using websites and technology. Unfortunately, the chances of your data being stolen or exploited are significantly higher and riskier than in a physical store. Burglars often sneak into the business company or retail store and take goods, cash, and confidential papers if they have a physical location. Streamlining costs by moving backend office and administrative operations to internet platforms is a smart option with an economical budget.

Restricted Cameras or Closed-Circuit televisions (CCTV) can assist the company in locating the criminals. However, a high-tech security system could thwart their efforts.

On the other hand, threats to database security might occur daily, and identifying the offenders is extremely difficult. Malicious hackers can strike at any time and from any location. In many cases, the affected business owner is unaware of data theft resulting in the breach of sensitive personal information.

As a result, database security aids in the protection of various vital assets:

* The necessary data or information.
* Any connected applications or APIs.
* Applications servers (both online and offline)
* People log in to the system using network and cloud technology to access the database.
* The system administration of database structures
* The database server's physical location.

When sensitive data is easily accessible, it becomes more vulnerable to attacks. The database gets immune to threats whenever security personnel strengthens their protective mechanisms and tools. The drawback is that it gets more challenging to utilize and access confidential information with strict security measures. Limit access to crucial data could affect the business operations of the organization. Regardless of the potential for user friction, enterprises now have even less choice but to err here on the side of caution.

# **Data Base Management System (DBMS) Privacy Concerns**

From various database security threats themselves, database security features arise. The following are the types of database maintenance issues:

## **1. Human Blunder**

Accidental data erasing or exploiting sensitive information, user account sharing, unencrypted passwords, and other undesirable user behaviors continue to be the root cause of most reported data breaches.

## **2. Threats From Within**

Following are the three sources listed below, each of which has access to the personal database:

* An observer obtains credentials or rumors of data through social engineering or other tactics and accesses the database.
* Many careless employees could potentially expose the database to attack within the organization through their unwanted actions.
* A suspicious hacker has some malicious information based on the company's lifeline.

A Malicious insider in the company is said to be one of the most common causes of database security breaches. Also, these frequently occur because many employees are granted privileged user access for various work purposes.

## **3. Vulnerabilities in the Company's Software**

Security flaws are present in every software, even if it is the best of the bests discovered daily. For such problems, open-source database management platforms and commercial database software regularly take essential steps to secure the data. However, the software will likely go down and be handed over to cyber criminals if these measures are absent.

However, if the organization takes appropriate measures on time, there could still be the removal of everyday minor attacks. But increased chances of zero-day attacks occur when hackers explore crooks and corners of software and hack frailty that has been discovered by the company yet.

## **4. Malware**

Malware is a virus put up on computers to exploit the system or damage the database. Malware can likely infiltrate various database and client-relationship information networks via any endpoint device. Thus, installing Anti-malware is the accurate solution since the software is critical on any endpoint. For example, anti-malware is highly essential on database servers due to its high value and confidentiality of information. It creates a protection wall to prevent a data breach.

## **5. Attacks Made Backup Systems and Injection Threats in SQL/NoSQL**

A database-specific danger is using arbitrary non-SQL and SQL attack strings in database queries. These typical queries are extensions received via HTTP requests or web application forms. Suppose an organization does not take the appropriate measures, like secured coding practices, regular code testing, and providing security steps, and any organization is at an unseen risk. Its database system will be mainly vulnerable to these attacks.

## **6. Site Analysis Confidentiality**

To launch several cyberattacks, attackers could leverage the surplus data stored in nearby locations of the memory space in the computer. It can usually happen as memory leakages when written data is in a particular drive.

# **Database Security Best Practices**

Let's glance at ten database security best practices likely to help individuals and organizations protect their personal information and essential datasets.

## **1. Establish Physical Database Security**

Suppose a cyber-criminal gains remote exposure to your logical and physical data modeling server. In that case, the hackers perhaps rob the relevant information and data, corrupt it, or even plug a hazardous trojan that could delete all files and data of the system. Because these attacks can circumvent digital security protocols, they are frequently challenging to detect without additional security measures.

Before selecting a hosting provider, an organization should remember that the respective host has a history and proven record of measures to protect. Physical attacks from an outsider or even an insider are likely to occur in the data warehouses, buildings, or even the cloud services of respective companies facing trouble.

When a company uses virtual machines, physical safeguards like fully-equipped security personnel, locks, and camera systems, are highly needed for confidentiality and protection from harmful hackers. Furthermore, the companies should track the physical server access and restrict them to certain persons to decrease malicious activity.

## **2. Distinct Database Server Software**

Database management systems necessitate technical measures to safeguard them from cybercrime. Furthermore, placing an individual's information on the same domain controller as the website's homepage exposes some information to numerous attack coordinates targeting internet sites.

For Instance, assume a company has an online marketplace with its website, non-sensitive data, and sensitive data on the same server. Also, the company can figure out various cyber-attacks and has the power to protect itself from any threats using appropriate privacy measures with tight security.

Nevertheless, the company has not realized that their critical information is now easily seen on the e-commerce website platform, and many coding experts can access it. Moreover, such a slight invasion could easily compromise the company and its website, which could take down the website or result in information leaked simply because the hacker can foreseeably gain access to your database.

Therefore, companies must design their database management system with high security and intelligent solutions to reduce the chances of security breaches. Using security-relevant data and event tracking, which is committed to fetching data in a confidential and encrypted manner, allows organizations to take instantaneous action regarding an uncalled network breach.

## **3. Configure an HTTPS VPN Connection**

Network device analysis requests are sent from a workstation to access the database server. The server acts like a security guard making a protective wall in some way or another as it keeps all the semi-request out without giving access to essential information. The most widely used proxy server protocol is HTTP. Working with crucial credentials, private information, or financial details involves using HTTPS patterns and the main server. As a result, data encryption provides an extra layer of security to secure the data flowing via the remote gateway node.

## **4. Do Not Use the Default Network Ports**

The UDP and TCP protocols secure information and datasets, sensitive or not, when transmitted between servers. When the configuration of these protocols happens, the companies make use of the default network ports.

Default ports are utilized for brute force attacks frequently. In other cases, the attacker break-in by the hit-and-trial method of multiple port number variants. Because of the additional work required, the assailant may be discouraged from continuing their attack attempts.

Whenever you allocate a new port, you must ensure that the users do not use the dock anywhere. You can check this with the help of the Internet Assigned Numbers Authority's port register.

## **5. Implementing Real-time DBMS Monitoring**

Vigorously inspecting your dataset for attempted breaches strengthens your protection and allows you to respond to potential attacks.

Tracking software helps track every event inside the database server and even alarms in case of potential breaches. Set up escalation mechanisms to keep your critical data further protected in the case of an attack.

Keep a record of database activity and all information. For example, keep track of when who, and which database sections are accessed. In addition, take account of all login attempts, including those that fail. Equally, keep track of the devices connected to the database to ensure that all devices connected to the servers are secured and authorized. The ability to track progress offers some insight into any questionable behavior or unauthorized attempts.

Another important security practice is regularly auditing your database security and organizing cybersecurity penetration tests. These enable you to detect possible security weaknesses and repair them before they cause a breach.

## **6. Make Use of Web Application and Database Firewalls**

Security systems are the first line of defense against unauthorized access. Aside from safeguarding your site, it would help if you also built a firewall or anti-virus to protect your databases from multiple attack channels.

The types of Firewalls commonly used to secure a network are:

* Firewall proxy server
* Firewall with packet filtering
* In-depth Stateful packet inspection (SPI)

Close any security gaps through correct configuration to ensure firewall safety. Keeping your firewalls up to date is critical because they shield important sites and databases from new and undiscovered cyber-attacks.

## **7. Implement Strong Encryption Security Measures**

Encoding your data is essential for protecting your trade secrets and having to move or stash sensitive personal information. Even if malicious hackers gain access to your data, it ensures security. In addition, placing data encryption techniques in place minimizes the risk of a significant cyber assault.

Username and password provide a weak defense but are insufficient on their own. Individuals routinely prefer easy-to-remember passwords over long, unique passwords that strengthen their security.

To restrict access, you can utilize multi-factor authentication. The attackers are less likely to access your database with these measures, even if your login credentials are compromised.

## **8. Make Routine Backup Copies of Your Database**

Although frequently changing respective websites' data, regularly creating your database backups is also critical. Therefore, it reduces losing sensitive information due to targeted hackers or computer viruses.

Backup and restore aid in restoring valuable information in a compromise or data loss. Running backups is an essential security practice, particularly for databases. However, standby versions of databases frequently contain historical data vulnerable to compromise. Therefore, maintain backups secure and limit access to avoid compromising data integrity.

Making database backups on the two most common servers is essential: Windows and Linux. Additionally, ensure that the restored data is stored and password-protected on a separate server to improve security. Consequently, your information is recoverable and safe even if the primary database server is compromised or inaccessible.

## **9. Maintain Application Updates**

Through several types of research, firms compromise and settle by using out-of-date software and its applications at a rate of nine out of ten. If this happens in different fields, there is a great concern for their privacy and security. Also, a paper on plug-ins discovered that companies failed to update approximately 17,384 plug-ins in the last twenty months. Moreover, 13,655 plug-ins have not been slight changes or minutely adjusted over the previous three years. Therefore, locating new bugs and problems with appropriate fixes is mandatory in all reputable software applications, as much as a standard security protocol.

The same applies to plug-ins, widgets, and other applications linking with the main database. Additionally, the companies should avoid those apps that have been untouched and not updated for six months.

## **10. Consider Making Use of a Robust Authentication Process**

Verizon Wireless's latest studies show that disrupted passcodes are responsible for 80% of data breaches. Furthermore, it demonstrates that passwords alone aren't a good security measure, owing to the human element of creating long and complex encryption.

We need to implement a multi-verification mechanism to combat this issue and provide another degree of protection to your database. Cyber Criminals would struggle to circumvent this security protocol even if credentials are compromised.

To further decrease the danger of security breaches, you need to restrict access to the database to verified IP addresses. While Email accounts can be copied or masked, the attacker must exert additional effort.

## **11. Make use of Firewalls**

Firewalls increase storage security by preventing unauthorized traffic from entering. A firewall enables only essential inbound and outbound database traffic when correctly designed. If requests from an unknown or known source seem very suspicious should be turned down or rejected without a second thought. It is because, without a firewall, threats can range from data breaches to Distributed Denial-of-service attacks.

## **12. Use Security Software and Apps**

Protecting the applications with firewalls and other cyber-secure methods on external sites is mandatory.

For Instance, when the suspicious web page used for communication purposes gains access to the important data.

Regardless of whether the program is safe, the firewall used to protect the data is enabled but could allow the suspicious webpage to access the necessary information. In addition, during unknown attacks and steals of information, the database acquires easy access and is subject to SQL injection attacks. You can avoid these instances with the help of a firewall that safeguards your database from potential hackers.

## **13. Exercise Database Encryption**

Encoding is one of the best database security practices in general. Encrypting data, whether at rest or in transit, ensures that it is unreadable by anyone who does not have the encryption key.

Data encryption for all backups is also a good countermeasure. You must keep the encryption keys separate from the description key, and at the time, you must follow all the security guidelines laid down by the management.

## **14 Secure the User Access**

The number of people who may access the database must be limited. Only grant privileges when a user works with the database.

Illegal access to a database can create new vulnerabilities. In addition, when too many employees or users have privileged access to the database, data violations frequently happen.

Even though team dynamics are unworkable in small companies with fewer employees, they must impose them. Therefore, enabling group access for certain situations is better than granting permissions to individuals. Employees join pre-existing groups as a company grows, which is convenient. Several data access development is applied based on the role of the company in the present business field rather than an individual's research.

Furthermore, convenient account security steps for such malicious attacks a company can take are as follows.

* Can utilize secure passwords.
* Can use encrypted password hashes.
* Do not share secure information and passwords of administrators and all employees.
* Let the software lock the accounts and information automatically after 2 to 3 times of failed login attempts.
* All accounts of currently working employees and resigned employees are deactivated.

## **15. Update Regularly**

Also, use the most current edition of database management software. To maintain safety from the most recent security threats, try operating the OS with daily updates and security steps. Each outsider application that connects to the database poses a security risk. So, keep all the plug-ins updated daily to avoid external hacking and troubleshoot hacking-related pop-ups.

Also, ensure that the privacy controls and security measures are activated by default if the company shares the database with any third-party apps or companies for work purposes.

## **16. Carry Out Security Testing**

Undertake vulnerability scanning after you've taken all of the necessary security precautions. Discover unsecured sections of confidential information and various hacks that hackers could access, conduct many security checks and tests, and address the problems and bugs as soon as possible.

It aims to unravel ways to hack before others do. Using penetration testing and security scanning tools and applications to test and know how much data is secured and whether sensitive information is highly private or not. Implement all assessments and detections before a data set goes live.

## **17. Enhance the Customer Experience**

Privacy protection is far more than a tick-box exercise to satisfy regulatory bodies. Online customers must be cautious about what they disclose and whom they disclose over the internet.

According to Deloitte, 73 percent of consumers are more willing to share information if they believe the organization is open about how it uses the data. As a result, database security is critical for instilling trust in your target audience. In addition, it enhances your customer experience every time.

## **18. Establish Procedures and Steps for Sensitive Datasets**

Consider taking certain protocols and security checks for clearly defined and not easily cracked situations, like setting warning and privacy notifications with respective guidelines like cloud security, data protection policies, and more for other accessed users.

Accidents, poor habits, and a lack of awareness can cause data breaches. Don't ever assume that everyone is aware of and understands security practices.

## **19. Data Security is Synonymous with Asset Security**

A DBMS violation is not a minor occurrence. Several threat factors can cause damage to your database, irrespective of whether they are inside or outside. A whole other issue is the possibility of direct denial-of-service attacks. It is a source of concern for retailers riding the crest of the resurgent e-commerce industry. By spending more resources establishing strong database security, users might avoid breaches and lessen the possibility of assaults such as ransomware, spyware, and firewall infiltration.

## **20. Keep Device Security**

Although the world is moving to the cloud, physical servers have advantages. You can have greater access and control over your network and greater uptime.

Physical security is the most underappreciated gem of database security. The hybrid network, a combination of virtual and physical servers, ensures that all the physical components of the hardware, such as cameras, locks, and security officers, remain intact with basic security measures. Users can also monitor server access and log all entries. Multiple attacks and mishaps are common in data centers and private servers, often difficult to detect.

Hopefully, appropriate encryption methods and other database security practices ensure database safety, whether on-premises or in the cloud.

# **Conclusion**

Keeping threats at bay becomes more difficult as the nature of cyberattacks evolves. How you secured your data and network last year might not work this year.

Using the database security best practices, you can assist your database with a robust cybersecurity framework and safeguard your data and servers. Protecting a company's dataset's security from determined intruders and cyber attackers is a difficult task which thus covers everything, including the location of the local server, to limit the chances of making mistakes as a human.

Even though data breaches are becoming more common, maintaining healthy security protocols reduces the risk of being targeted and aids in preventing a successful breach attempt.

Finally, the more proactive you are in averting cyberattacks and securing sensitive information, the more effective can be your long-term client connections. It also encourages durable and trustworthy business arrangements to aid your organization's growth.