

# Microsoft SQL Server

## Table of Contents

1. [Minimize Surface Area](#)
2. [Secure MSDE installations](#)
3. [Create security awareness program](#)
4. [Prevent SQL injection](#)
5. [Backup policy](#)
6. [Secure install](#)
7. [Use secure file Systems](#)
8. [Ensure the physical security of your server.](#)
9. [Stay current on patches](#)
10. [Execute Microsoft security utilities periodically](#)
11. [Enable security auditing](#)
12. [Encrypt sensitive data](#)
13. [Control remote data execution](#)
14. [Manage catalog](#)
15. [Manage access to database objects](#)
16. [Manage Schemas](#)
17. [Manage Database Ownership](#)
18. [Restrict Administrative Privileges](#)
19. [Ensure strong password policy](#)
20. [Disable System Stored Procedures](#)
21. [Secure Network Setup](#)
22. [Authenticate accounts](#)
23. [Manage Service Accounts](#)

## 1. Minimize Surface Area

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 2. Secure MSDE installations

If MSDE is distributed with application, the following additional guidance applies:

Install MSDE using "Windows security mode" as the default.

When distributing MSDE to customers, use the Microsoft-supplied installer rather than merge modules.

When installing an instance of MSDE that will operate only as a local data store, disable the Server Net-Libraries.

If product includes MSDE, make this known to end customers. In the future, end customers may need to install or accept MSDE-specific software updates.

MSDE installs SQL Server Agent by default, but leaves the Service startup type to "Manual." If application does not use SQL Server Agent, change this to "Disabled." Include security best practice information in your product documentation.

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 3. Create security awareness program

Ensure that members of your development team understand major security issues: current threats, security trends, changing security environments, and attack scenarios. Require relevant security training for all developers and testers. Increase the awareness of issues like cross-site scripting, buffer overflows, SQL injection, and dangerous APIs. Identify specific categories of threats that apply to your product — for example, denial of service, escalation of privileges, spoofing, data tampering, information disclosure and repudiation.

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 4. Prevent SQL injection

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 5. Backup policy

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 6. Secure install

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 7. Use secure file Systems

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 8. Ensure the physical security of your server.

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 9. Stay current on patches

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 10. Execute Microsoft security utilities periodically

### MAINOPTIONS

Versions: SQL Server 2005

---

## 11. Enable security auditing

Enable security auditing of Sysadmin actions, fixed role membership changes, all login related activity, and password changes. After selecting appropriate auditing options, script the audit, wrap it in a stored procedure, and mark that stored procedure for AutoStart. Auditing is scenario-specific. Balance the need for auditing with the overhead of generating additional data. Audit successful logins in addition to unsuccessful logins if you store highly sensitive data. Audit DDL and specific server events by using trace events or event notifications. DML must be audited by using trace events. Use WMI to be alerted of emergency events.

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 12. [Encrypt sensitive data](#)

Encrypt high-value and sensitive data.

### REFERENCE

If application requires data encryption, consider using the products of such vendors as Protegrity and Application Security Inc.

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 13. [Control remote data execution](#)

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 14. [Manage catalog](#)

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 15. [Manage access to database objects](#)

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 16. [Manage Schemas](#)

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 17. [Manage Database Ownership](#)

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 18. Restrict Administrative Privileges

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 19. Ensure strong password policy

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 20. Disable System Stored Procedures

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 21. Secure Network Setup

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 22. Authenticate accounts

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---

## 23. Manage Service Accounts

### MAINOPTIONS

Versions: SQL Server 2005, SQL Server 2008 Express

---