Installation Security

MySQL:

1. Linux: mysql_secure_installation
2. Change password (default password is blank)
3. Change username of root passwords
4. Do not share root access
5. Remove or disable all anonymous accounts
6. Disable remote access
7. Do not leave your ports wide open
8. Use IP addresses to restrict access to the database
9. Encrypt the connection to the sever using SSH or SSL

MS SQL Server:

Prior to installation—

1. Place severs behind firewalls and locked doors
2. Create subnets
3. Isolate database servers from public networks
4. Configure ports on an individual basis
5. Use an NTFS file system
6. Encrypt the connection to the sever using SSH or SSL

During installation—

1. Use TDE
2. Apply passwords to services individually and uniquely
3. Choose Windows authentication over Mixed authentication
4. Strong password
5. Change default usernames (Change username of root passwords)

After installation—

1. Never store passwords in plain text
2. Multilayer
3. Run separate accounts
4. Use least privileges (never use administrator account to run --)
5. Update
6. Review logs files
7. Disable all guest accounts
8. Group different users
9. Try read-only whenever possible

Oracle:

1. Harden the OS
2. Close unused ports
3. Use firewalls
4. Update
5. Restrict run time
6. Restrict using IP address
7. Include only required software
8. Encryption
9. Enforce access control
10. Restrict users with OS access
    - Database Vault
    - Label Security
    - TDE
    - Data Redaction
    - Virtual private database