Best Practices for SQL Server Security

- Force encryption of connection on both sides (server and clients)
- Do not use self-signed auto-generated certificate
- Prepare procedure and evaluate on regular basis changes in:
    - Logins mapped to the "dbo" user in each database
    - CONNECT or other permissions granted to the "guest" user (BP: should not be granted)
    - Database users, permissions and application roles for each database
    - Linked Servers and Linked Server Logins
    - Find logins without permissions
    - Find orphaned or broken users in all of the databases
    - Identify orphaned Windows logins
- Check password policies and expiration for the SQL logins
- Verify that "sa" login has been renamed and/or disabled and has password policy/expiration enabled
- Allow to use Linked Servers only to limited subset of Logins
- Logins without permissions should be removed
- Orphaned users in all of the databases should be corrected or revoked connect permission
- Remove orphaned Windows logins
- SQL Server Instance options that should not be enabled (unless required by LOB):
    - allow updates
    - cross db ownership chaining
    - clr enabled
    - Database Mail XPs
    - xp_cmdshell
    - Ad Hoc Distributed Queries
    - contained database authentication
- SQL Server Service should run under Virtual Account or Group Managed Service Account
- Block outgoing internet connection from your servers
- Block outgoing connections to workstation/clients subnets – if not used
- Protect and monitor physical access to servers
- Use centralized logging solutions and alerts (third-party products)
- If possible use TDE in cooperation with HSM module
- Encrypt backups
- Monitor users activity with extended events and auditing
- Avoid using deny permission
- Grant permissions to roles