Protecting database contents [Mandatory]

- Database administrators and database users should know the sensitivity or classification associated with databases and their contents. In cases where all of a database’s contents are the same sensitivity or classification, an organisation should classify the entire database at this level and protect it as such.
- Alternatively, in cases where a database’s contents are of varying sensitivities or classifications, and database users have varying levels of access to the database’s contents, an organisation should protect the database’s contents at a more granular level. Restricting database users’ ability to access, insert, modify or remove database contents, based on their work duties, ensures that the likelihood of unauthorised access, modification or deletion of database contents is reduced.
- Furthermore, where concerns exist that the aggregation of separate pieces of content from within a database could lead to malicious actors determining more sensitive or classified content, the need-to-know principle can be enforced through the use of minimum privileges, database views and database roles. Alternatively, the content of concern could be separated by implementing multiple databases, each with restricted data sets.

Revision #2
Created 26 September 2025 11:34:26 by RISA
Updated 26 September 2025 12:55:02 by RISA