# RDBMS Guidelines

## Abstract

Most database systems utilize the Relational Database Management Systems (RDBMS) model. Because it is the popular choice for information storage, developers must learn more about RDBMS security issues, known threats, and the decisions you can make to keep the databases secure. See [RDBMS Concepts](a) for more reference information about the technology.

## What’s New in this Guideline

This guideline is updated to showcase the security features of RDBMS. For an itemized summary of the RDBMS Security topics discussed in these guidelines, see RDBMS Security Summary and Checklists.

## Scope and Assumptions

These guidelines concentrate on access control and logical integrity issues. They do not focus on physical integrity requirements like database back-up, data recovery, and hardware planning.

It is assumed that the customer organization has a defined security policy in place. The security policy should address the general information security goals of the organization, as well as how the overall policies apply to databases. Furthermore, the guidelines do not address operating system security issues. It is assumed that the operating system used for an RDBMS has been evaluated and secured in accordance with the organizational security policies.

## Discussion

### RDBMS Security Requirements

The general security requirements of an RDBMS are similar to those for other information system components. In the context of database operations, the primary requirements are:

* User authentication – The database, or trusted operating system functions, must identify users.
* Access Control – Database mechanisms must determine which data sets, database functions, or administrative privileges are authorized for a specific user.
* Auditability – Records of user actions, such as reading and writing data, can be used to detect and monitor possible abuses of the system.
* Element Integrity – The correctness and accuracy of data elements in a database depends on user actions during data collection, calculation, and entry.
* Logical Database Integrity – The relationships between data must be preserved.
* Physical Database Integrity – Data must be protected against corruption from power failures, system crashes, or other external events.

### Security Controls

A variety of controls are available to realize the security requirements for a database. All controls have cost in the form of resources (equipment, software, and personnel), performance, or usability. Decision makers must balance appropriate security with the level of resources required, and acceptable performance degradation. The database controls discussed here are:

* Access controls
* Integrity controls
* Inference controls
* Auditing and accountability
* Design issues

### Database Security Threats

Some security threats to databases are similar to those for other information system resources. Others are specific to databases. The major threats are:

* Direct disclosure of data – Unauthorized users gaining access to data, or legitimate users retrieving data elements in unexpected combinations to gain classified information.
* Unauthorized modification of data – Unauthorized or legitimate users corrupting or destroying data through an accident or malicious intent.
* Data contamination – Inaccurate data causing errors to propagate throughout the database when data is combined for derived values and reports.
* Aggregation – Collecting small, seemingly unimportant pieces of data and combining them to reveal unintended information.
* Inference – Use of statistical methods to create queries that can deduce information about individual entities.

Malicious code – Codes like trojans horses and viruses that disrupt or subvert normal application behavior. Trojan horses are programs that add undocumented functions to an information system. Attacks through malicious code can be in stored database procedures or database applications.

This sample is discontinued here on purpose.