RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

BACK TO BASICS

RELATIONAL DATABASES

With this guide, ANSSI - the French Cybersecurity Agency – aims to help organizations achieve the secure implementation of relational databases (DB) through 10 key best practices:

→ **Keep database management software (DBMS) up to date** using official repositories, and install security updates as prescribed in ANSSI's Configuration recommendations of a GNU/Linux system, in particular R58, R59, R60 and R61.

→ **Secure the administration of servers hosting the DB** – please refer to ANSSI's Recommendations to secure administration of IT systems - and **minimize the use of plugins and administration tools**.

→ **Log events and administrator access** by applying Appendix A of ANSSI's *Recommandations de sécurité pour l'architecture d'un système de journalisation* (guide only available in French), in particular R3, R9, R26 and R27.

→ **Secure access:**

- use separate access accounts (for human users and applications) and clearly define their use;
- systematically authenticate access (beware of default accounts and direct access) and use state-of-the-art cryptographic mechanisms – refer to ANSSI's *Guide des mécanismes cryptographiques* (only available in French);
- scan regularly the native administrator account, which should only be used as a last resort;
- implement multi-factor authentication for administrators - see ANSSI's *Recommandations relatives à l'authentification multifacteur et aux mots de passe* (only available in French) .

→ **Apply the principle of least privilege**:

- limit user rights to what is strictly necessary;
- define roles and assign them to users.

→ **Harden configuration:**

- isolate configuration files data by storing it on separate partitions or directories;
- disable advanced BDD features which read/write/execute operating system files;
- impose data typing.

→ **Set backup parameters**, as recommended in ANSSI's guide *Sauvergarde des systèmes d'information* (only available in French) and the "Back to Basics" The golden rules of backup.

[redacted]

→ **Protect sensitive data:**

- prevent data leaks by ensuring that production data is not used in development (or similar) environments;
- pay close attention to SaaS format DB (risk of data being shared between customers);
- encrypt on-transit and at-rest data;
- dedicate DB servers to each level of data sensitivity;
- use internal DB mechanisms to limit data access (e.g. views).

→ **Follow best development practices for DB access** (e.g. use prepared queries to protect against injections).

→ **Set up DB supervision** on the server's physical and/or virtual resources (storage, CPU, RAM), and audit potentially suspicious events.

[redacted]