Security Documentation

Dokumen ini menjelaskan mekanisme perlindungan data sensitif SPI.

Manajemen Akses (RBAC) Sistem menggunakan *Database Roles* untuk membatasi akses:

- db_kepala_spi: Akses Penuh (*Select, Execute*).
- db_analis_audit: Akses Baca/Tulis ke *Staging*, Baca ke *DW*.
- db_viewer: Akses Baca Saja (*Read-Only*) ke Dashboard/Views.
- db_etl_operator: Hak eksekusi prosedur ETL.

Perlindungan Data (Data Masking)

- Kolom NIP Auditor (ID_Sistem_Sumber): Menggunakan fungsi partial(0, "XX-XXX-", 4) agar tidak terlihat oleh user biasa.
- Kolom Penanggung Jawab: Menggunakan fungsi default() untuk penyensoran penuh.
- Unmasking: Hanya role db_kepala_spi dan db_analis_audit yang memiliki izin UNMASK untuk melihat data asli.

Audit Trail Setiap perubahan data (INSERT, UPDATE, DELETE) pada tabel sensitif dicatat otomatis ke dalam tabel dbo.AuditLog melalui *Database Trigger*, mencakup informasi pengguna (UserName) dan waktu kejadian (EventTime).