

# Manajemen Sistem Basis Data Integrity dan Security

Lintang Yuniar Banowosari

<http://staffsite.gunadarma.ac.id/lintang>

# Data Integrity

---

Data konsisten dan valid pada keadaan apapun dan konstrain apapun.

# ATURAN KEINTEGRITASAN DATA

---

- Entity integrity. Nilai atribut primary key tidak boleh null (tidak dikenal)

Contoh PEGAWAI(NIP, Nama, Alm, Gaji, KdDiv)

NIP sebagai primary key tidak boleh bernilai null atau kosong atau tidak dikenal.

- Referential integrity. Nilai atribut foreign key harus sesuai dengan nilai atribut rujukan (primary key) pada relasi lain.

Contoh: PEGAWAI(NIP, Nama, Alm, Gaji, KdDiv)

DIVISI(KdDiv, Ket, Lokasi)

Atribut KdDiv sebagai foreign key pada relasi PEGAWAI Harus mempunyai nilai yang sesuai dengan rujukannya atribut KdDiv pada DIVISI.

# ATURAN KEINTEGRITAS DATA

---

- Entity participation

Keharusan / ketidakharusan adanya keanggotaan dari suatu relationship, pada saat perancangan database.

- Domain constraint

Domain merupakan sekumpulan nilai yang diizinkan untuk satu atau lebih dari satu atribut.

# ATURAN KEINTEGRITASAN DATA

---

- Enterprise constraint

Aturan yang dispesifikasikan oleh DBA atau pemakai.

# **DATABASE SECURITY / PENGAMANAN BASIS DATA**

---

- Pengamanan atau perlindungan database terhadap ancaman dengan menggunakan pengontrolan secara teknis dan administratif.
- Ancaman Merupakan situasi atau kejadian yang direpresentasikan oleh orang atau lingkungan disengaja maupun tidak disengaja yang mengenai sistem ataupun organisasi sehingga dapat merugikan organisasi yang bersangkutan.

# DATABASE SECURITY / PENGAMANAN BASIS DATA

---

Contoh:

1. Kehilangan privacy
  - Penggunaan password orang lain
  - Pemerasan
  - Kesalahan pada software yang mengakibatkan pengaksesan melebihi normal.
  - Pelatihan pegawai yang tidak berkualitas

# DATABASE SECURITY / PENGAMANAN BASIS DATA

---

## 2. Kehilangan kepercayaan

- Seperti no. 1
- Entri ilegal oleh hacker
- Pemogokan pegawai

## 3. Pencurian dan penggelapan

- Seperti no. 1 dan 2
- Usulan perubahan yang bukan wewenangnya
- Pengubahan program yang dapat menembus mekanisme pengaman
- Pencurian



# DATABASE SECURITY / PENGAMANAN BASIS DATA

---

4. Kehilangan integrity
  - Radiasi dan interferensi elektronik
  - Kebakaran
  - Terputusnya kabel
  - Terdapatnya virus
  - Korupsi data
  - Pelatihan yang tidak berkualitas
5. Kehilangan ketersediaan
  - Seperti no. 4 (point 1-4)
  - Ancaman bom

# Pengontrolan Berbasis Komputer

---

Menghadapi ancaman diperlukan pengontrolan secara fisik, prosedur administratif atau keduanya.

- Authorization
- Encryption
- Checkpointing
- View
- Integrity
- Password
- Backing Up
- Journaling

# Pengontrolan Berbasis Komputer

---

## ■ Authorization

Pemberian otoritas/hak operasi yang legal pada user/program agar dapat mengakses sistem serta tabel, view, aplikasi, dan prosedur.

Pemberian otoritas/hak operasi dengan menggunakan GRANT dan REVOKE.

Jenis operasi/privilege : select, insert, update, delete, references dan usage

Sintaks GRANT :  
GRANT operasi/ALL PRIVILEGES  
ON objek TO pemakai/PUBLIC  
[WITH GRANT OPTION];

Sintaks REVOKE :  
REVOKE [GRANT OPTION FOR]  
Operasi/ALL PRIVILEGES  
ON objek FROM pemakai/PUBLIC  
[RESTRICT/CASCADE];

# Pengontrolan Berbasis Komputer

---

Contoh Authorization :

GRANT ALL PRIVILEGES  
ON PEGAWAI TO Manager  
WITH GRANT OPTION

GRANT SELECT, UPDATE(GAJI)  
ON PEGAWAI TO admin;

GRANT SELECT  
ON DIVISI TO  
Public;

REVOKE SELECT  
ON DIVISI FROM  
Public;

# Pengontrolan Berbasis Komputer

---

## ■ VIEW

Merupakan hasil dinamik dari operasi relasional terhadap satu atau lebih relasi untuk mendapatkan relasi lain.

Mekanisme view dapat menyajikan data relevan dengan pemakai, sedangkan yang lain 'disembunyikan'.

# Pengontrolan Berbasis Komputer

---

Sintaks pembuatan view :

```
CREATE VIEW namaview [kolom,...]  
AS subselet [WITH [CASCEDE/LOCAL]  
GRANT OPTION]  
FROM namatabel;
```

# Pengontrolan Berbasis Komputer

---

Contoh pembuatan view diperuntukkan manager divisi 2 yang ingin mengakses data pegawai di divisi 2 secara detail.

```
CREATE VIEW peg2
```

```
AS select FROM pegawai WHERE KdDiv='2';
```

```
CREATE VIEW peg3 AS select NIP,Nama,Alm FROM  
pegawai where KdDiv='3' WITH CHECK OPTION;
```

```
DROP VIEW peg3;
```

# Pengontrolan Berbasis Komputer

---

## ■ Password

Verifikasi user dengan menggunakan suatu kata tertentu.

## ■ Backing-up

Proses yang secara periodik mengcopy database dan journal ke dalam media penyimpanan tertentu.

## ■ Encryption

Pengcodingan data dengan algoritma khusus sehingga data tidak dapat dibaca oleh program apapun tanpa adanya kunci deskripsi dan data yang dikirim tidak dapat dibaca sebelum proses deskripsi.



# Pengontrolan Berbasis Komputer

---

## ■ Journaling

Pembuatan journal dari semua perubahan database agar pemulihan dapat secara efektif dilakukan pada saat terjadi kegagalan ataupun kesalahan.

Jurnal mungkin akan berisi data:

### 1. Record transaksi

- identifikasi dari record
- tipe dari record jurnal (transaksi start, insert, update, delete, abort, commit)
- item data sebelum perubahan (operasi update dan delete)
- item data sesudah perubahan (operasi insert dan update)
- informasi manajemen jurnal, seperti pointer sebelum dan record jurnal selanjutnya untuk semua transaksi

### 2. Record checkpoint

# Pengontrolan Berbasis Komputer

---

## 7. Checkpointing

Titik sinkronisasi antara database dan transaksi log file. Informasi pada jurnal digunakan untuk pemulihan database dari kegagalan yang dilakukan. Satu kesulitan dengan skema ini adalah ketika kegagalan terjadi, tidak diketahui seberapa jauh jurnal untuk kembali mencarinya dan berakhir dengan melakukan transaksi REDO. Untuk membatasi pencarian dan pemrosesan secara teratur digunakan teknik checkpoint/pos pemeriksaan.

## 8. Integrity

Pengontrolan keintegritasan data untuk menjamin data tetap valid.

# PENGONTROLAN TIDAK BERBASIS KOMPUTER

---

Pengontrolan yang berhubungan dengan politis, persetujuan dan administrasi

Pembuatan *Security policy* dan *Contingency plan*

*Security policy* mendefinisikan pemeliharaan sistem yang aman pada organisasi, meliputi :

- Area bisnis
- Tanggungjawab dan kewajiban pegawai
- Sanksi kedisiplinan
- Prosedur yang haru diikuti

# PENGONTROLAN TIDAK BERBASIS KOMPUTER

---

*Contingency plan* mendefinisikan bagaimana suatu organisasi dapat berfungsi pada saat darurat.

- Penentuan personal kunci dan alternatif serta bagaimana cara menghubunginya
- Siapa yang menentukan *Contingency plan* dan bagaimana cara penentuannya
- Kebutuhan teknis dan operasional untuk operasi pentransferan
- Siapa personal di luar organisasi yang dapat dihubungi
- Terdapatnya jaminan terhadap situasi ini

# PENGONTROLAN TIDAK BERBASIS KOMPUTER

---

## 2. Pengontrolan personel meliputi

- Adanya prosedur perekrutan pegawai maupun penempatan pegawai pada pos-pos kunci
- Pelatihan pegawai
- Pemisahan pekerjaan dan tanggungjawab
- Pengontrolan pekerjaan lain

# PENGONTROLAN TIDAK BERBASIS KOMPUTER

---

3. Penempatan peralatan yang aman
4. Software dan data yang aman
5. Terdapatnya persetujuan antara sipembuat software dan kliennya
6. terdapatnya persetujuan pemeliharaan software dan hardware
7. Pengontrolan pengaksesan secara fisik baik internal dan eksternal
8. Pengontrolan gedung terhadap resiko kebakaran dan banjir
9. Persiapan terhadap situasi darurat

# PENGAMANAN BENTUK LAIN

---

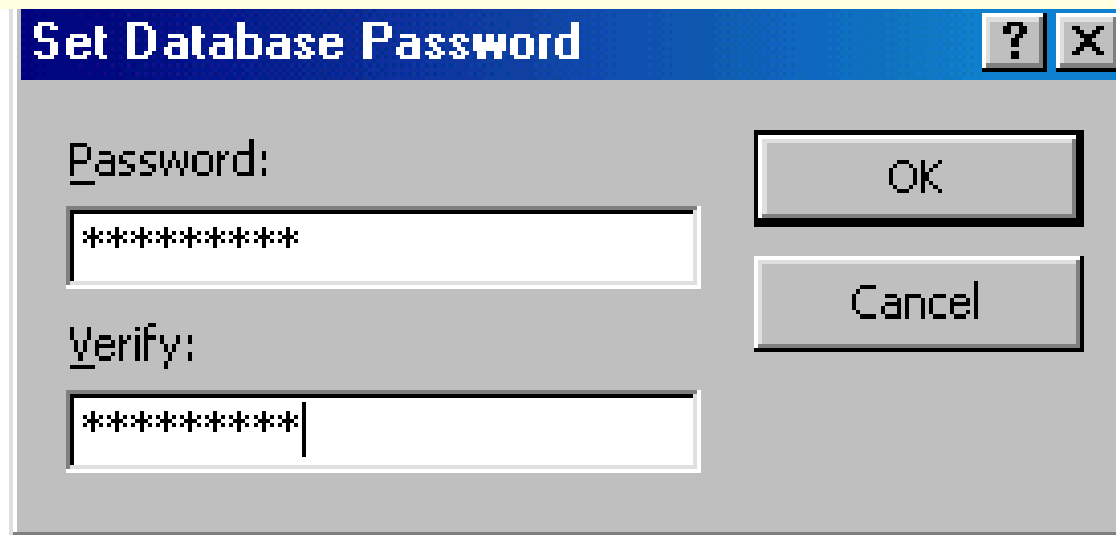
- Pengamanan PC

Resiko yang dihadapi PC adalah terinfeksi virus, untuk itu di dalam *Security policy* harus terdapat prosedur yang harus diikuti pada saat suatu software ditransfer ke sistem.

# Pengamanan PC

## Security in MS. Access

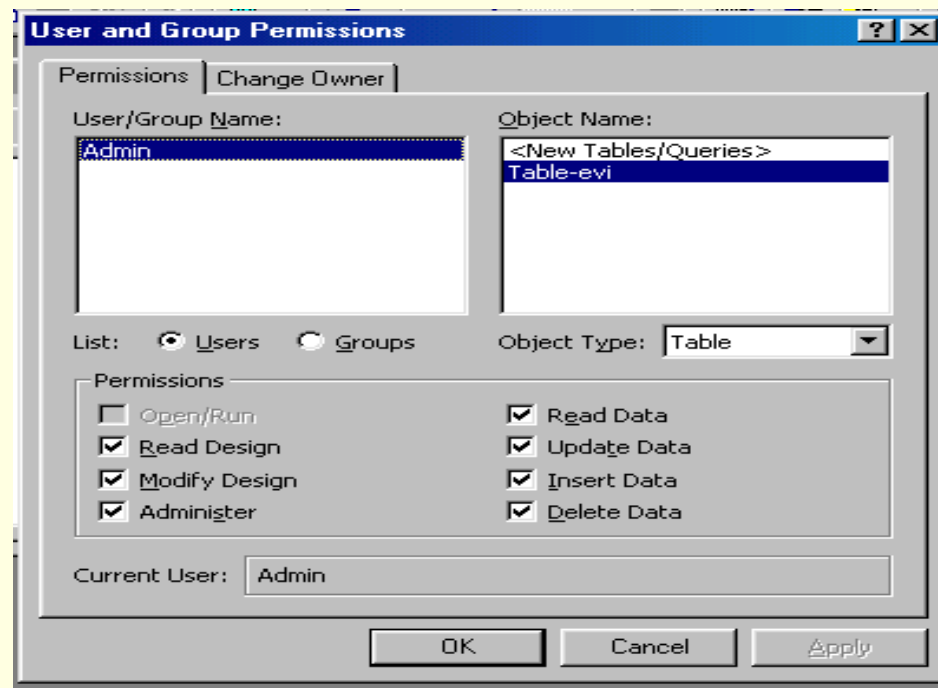
1. Setting a password for opening a database





# Pengamanan PC

2. User-level security which can be used to limit the part of the database that a user can read or update.



# Pengamanan PC

