Data Protection

- *data protection* involves data integrity, data security, and data privacy
- *data integrity* – ensuring that the data is correct, relevant, up-to-date
- *data security* – preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information
  - about protecting data from malicious threats
- *data privacy* – having control over what data is collected about you and how it is used
  - about using data responsibly

Data Protection

- these aspects reflect the elements of the *CIA triad* –
  - *confidentiality* – information is not made available or disclosed to unauthorized parties or processes
  - *integrity* – ensuring accuracy and completeness of the information over its full lifecycle
  - *availability* – ensuring information can be accessed when needed
    - requires proper functioning of the DB system and its security controls
    - includes prevention of service disruptions such as power outages, hardware failures, system upgrades, and denial-of-service attacks

 https://en.wikipedia.org/wiki/Information_security

Data Protection

- data integrity can involve policies but is also supported through implementing constraints in the database
- privacy is about policies
- security supports the policies by preventing improper access

Data Privacy

- there are many laws and regulations governing data e.g.

US federal –
- Family Educational Rights and Privacy Act (FERPA) – governs student information
- Health Insurance Portability and Accountability Act (HIPAA) – governs health information
- Gramm-Leach-Bliley Act – governs personal information collected by banks and financial institutions
- Fair Credit Reporting Act – governs collection and use of credit information

US state – (20 states have comprehensive laws, 6 have narrow laws, 10 have introduced laws 2023-24)
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) – governs personal information collected from CA residents
  - requires a privacy policy
  - requires informing data subjects about collection
  - requires giving data subjects the ability to access, correct, delete info
- New York SHIELD Act – requires safeguards to protect personal information collected from NY residents

European –
- EU General Data Protection Regulation (GDPR) – governs personal information collected from EU residents
  - requires consent before personal info is collected
  - requires notification of data breaches within 72 hours
  - defines rights of data subjects with regards to their personal info – to be informed about collection and use, to access their data, to ask for errors to be corrected, to request deletion, to restrict processing, to object to how info is used

Obligations

- businesses are expected to operate according to sound business principles and in a legal and ethical manner
  - including with respect to data assurance and security
- *due care* and *due diligence*
  - have taken the necessary steps to protect data, and can demonstrate having taken responsibility for data security
  - ongoing activities to make sure protection mechanisms remain up-to-date and operational
  - *due diligence* refers to having a plan or policy – having structures in place to protect the organization's interests
    - e.g. establishing and reviewing policies for data handling, ensuring compliance with legal requirements, auditing database security settings and user permissions to ensure compliance with organizational policies, conducting risk assessment and evaluating vendors
  - *due care* refers to the actions taken in the moment to follow and implement the policies
    - e.g. setting up strong authentication mechanisms to prevent unauthorized access, performing regular backups, applying security patches, monitoring to detect security breaches

Security – Access Control

There are three parts to access control –

- *identification* – asserting identity
  - e.g. providing a username
- *authentication* – identifying the user
  - by something (only) the user knows (e.g. PIN, password, mother's maiden name, pet's name)
  - by something (only) the user has (e.g. driver's license, magnetic swipe card)
  - by something (only) the user is (e.g. palm prints, fingerprints, voice prints, retina scans)
- *authorization* – determining if the user is allowed access to a resource
  - involves *policies* to determine who can access what and under what circumstances and *access control mechanisms* to enforce the policies

MySQL Identification and Authentication

- identity is user@host
  - username (provided by the user) and the host the user is connecting from
- authentication is via password

MySQL Privileges

User accounts are granted privileges specifying what operations they can execute in the DB.

Three levels of privileges:

- admin – deal with management of DB server
  - global
- database – apply to particular databases
  - can be granted for specific DB or globally for all DBs
- database object – apply to particular database objects (tables, indexes, views, stored routines)
  - can apply to a single object, all objects of that type in a specific DB, or globally for all objects of that type

views and stored routines allow for access to specific rows, columns, operations

Privilege	Column	Context
CREATE	Create_priv	databases, tables, or indexes
DROP	Drop_priv	databases, tables, or views
GRANT OPTION	Grant_priv	databases, tables, or stored routines
LOCK TABLES	Lock_tables_priv	databases
REFERENCES	References_priv	databases or tables
EVENT	Event_priv	databases
ALTER	Alter_priv	tables
DELETE	Delete_priv	tables
INDEX	Index_priv	tables
INSERT	Insert_priv	tables or columns
SELECT	Select_priv	tables or columns
UPDATE	Update_priv	tables or columns
CREATE TEMPORARY TABLES	Create_tmp_table_priv	tables
TRIGGER	Trigger_priv	tables
CREATE VIEW	Create_view_priv	views
SHOW VIEW	Show_view_priv	views
ALTER ROUTINE	Alter_routine_priv	stored routines
CREATE ROUTINE	Create_routine_priv	stored routines
EXECUTE	Execute_priv	stored routines
FILE	File_priv	file access on server host
CREATE TABLESPACE	Create_tablespace_priv	server administration
CREATE USER	Create_user_priv	server administration
PROCESS	Process_priv	server administration
PROXY	see proxies_priv table	server administration
RELOAD	Reload_priv	server administration
REPLICATION CLIENT	Repl_client_priv	server administration
REPLICATION SLAVE	Repl_slave_priv	server administration
SHOW DATABASES	Show_db_priv	server administration
SHUTDOWN	Shutdown_priv	server administration
SUPER	Super_priv	server administration
ALL [PRIVILEGES]		server administration
USAGE		server administration

allows holder to grant or revoke privileges they have for other users

ability to import from or export to files located on the server host

confers no privileges


```
GRANT
    priv_type [(column_list)]
      [, priv_type [(column_list)]] ...
    ON [object_type] priv_level
    TO user_specification [, user_specification] ...
    [REQUIRE {NONE | ssl_option [[AND] ssl_option] ...}]
    [WITH with_option ...]

object_type:
    TABLE
  | FUNCTION
  | PROCEDURE

priv_level:
    *
  | *.*
  | db_name.*
  | db_name.tbl_name
  | tbl_name
  | db_name.routine_name

user_specification:
    user
    [
        IDENTIFIED BY [PASSWORD] 'password'
      | IDENTIFIED WITH auth_plugin [AS 'auth_string']
    ]
```

of the form 'username'@'host'

GRANT can also be used to create user accounts

```
REVOKE
    priv_type [(column_list)]
      [, priv_type [(column_list)]] ...
    ON [object_type] priv_level
    FROM user [, user] ...

REVOKE ALL PRIVILEGES, GRANT OPTION
    FROM user [, user] ...
```


Guidelines

- Do not grant more privileges than necessary to a user.
  - especially if the user is not a human (and thus the password needs to be stored in plaintext somewhere)
  - *need-to-know principle* – users should be granted the fewest privileges possible to allow them to do their jobs
- Never grant privileges to all hosts.
- Do not grant certain privileges to non-admin users.
  - PROCESS allows display of information which includes statements currently being executed
  - SUPER allows server configuration and control, including termination of other sessions
  - SHUTDOWN allows server shutdown
  - GRANT OPTION allows users to give their privileges to other users

Guidelines

- Use caution with other privileges.
  - FILE allows import of files from the server host into tables, which can then be accessed using SELECT
  - ALTER allows renaming of tables, which can be used to subvert the privilege system

Questions

Are these privileges coded into the database as it is built or put in after by a different system?

- privileges can be granted to users at any time, but typically defined initially as part of DB implementation
- SQL provides GRANT and REVOKE statements for managing privileges
- Workbench provides a GUI front end

Questions

How to implement proper password handling between our application and MySQL?

- photo album exercises address this
- "one big application" model – application manages user accounts
  - database contains a table with usernames and (encrypted) passwords
  - `INSERT INTO USER(username,password) VALUES ('arthur',SHA('tea'))`
  - to check password, query the database for the row of the user table matching the username and encrypted password
  - if a row is found, application stores that the login was successful
    - checks if there has been a successful login before doing operations that are limited to certain users

Questions

More generally, how to handle security in our projects?

- application will manage user accounts similar to the photo album
- there will be two accounts for application access to the DB
  - guest – SELECT, EXECUTE
  - admin – SELECT, INSERT, UPDATE, DELETE, EXECUTE
- use views and stored routines to limit access to sensitive tables
  - e.g. USER table