DATA CLASSIFICATION

DATA

- In general, data is any set of characters that has been gathered and translated for some purpose, usually analysis.
- It can be any character, including text and numbers, pictures, sound, or video.
- Raw data describes the facts and figures that a company processes every day.

DATA CLASSIFICATION

- Data classification is one of the most important steps in data security.
- Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data.
- That’s why it’s important to classify your data based on how sensitive or valuable it is

DATA CLASSIFICATION

- Common data classifications include
  - Highly Confidential
  - Sensitive
  - Internal Use Only
  - Public

HIGHLY CONFIDENTIAL

- This classification applies to the most sensitive business information that is intended strictly for use within your company.
- Its unauthorized disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term.
- It could include credit-card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, etc.

SENSITIVE

- This classification applies to sensitive business information that is intended for use within your company, and information that you would consider to be private should be included in this classification.
- Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.

INTERNAL USE ONLY

- This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company.
- While its unauthorized disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to impact your company, employees, business partners, vendors and the like.

PUBLIC

- Basically any information that requires no special protection or rules for use

CIA

- Confidentiality, Integrity, Availability
- A model designed to guide policies for information security within an organization
- Considered the three most crucial components of security

CONFIDENTIALITY

- Equivalent to privacy
- A set of rules that limits access to information
- Designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it
- i.e. Data Encryption, User ID & Password, Two-Factor Authentication, Biometric lock system

INTEGRITY

- It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people
- i.e. File Permissions, Access Control, Checksums

AVAILABILITY

- A guarantee of reliable access to the information by authorized people whenever required
- Best ensured by maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment
- i.e. Load Balancing, Back-up Servers

AAA

- Concept relating to the people who use that information
  - Authentication
  - Authorization
  - Non-repudiation

AUTHENTICATION

- Authentication is a process of identifying the person before accessing the system.
- It allows user to access the system information only if authentication check got passed.
- Apart from Username & password combination, the authentication can be implemented in different ways like asking secret question and answer, OTP (One Time Password) over SMS, biometric authentication, Token based authentication like RSA Secure ID token etc.

AUTHORIZATION

- Once the Authentication passed the Authorization comes in the picture to limit the user as per the permission set for the user.
- The Authorization is generally implemented on Access control list, user role based, user group based and define the permissions & restrictions to specific user group or granting or revoking the privileges for the users.

ACCESS CONTROL

- Access control is the selective restriction of access to some kind of resource (a folder, a file, and a device).
- There are different types of approaches to access control.
  - DAC
  - MAC
  - RBAC
  - MLS

DAC

- Discretionary Access Control
- Every user can decide who can, with which permission,read his/her files.

MAC

- Mandatory Access Control
- The administrator decides the security policy and all the files in the system will comply

RBAC

- Role Based Access Control
- The permissions are not granted per user, but according to the role
- This allows big organizations to assign permission to roles and roles to users, making it easier to create, modify or delete users.

MLS

- Multi Level Security
- Each user has a trust level and each item has a confidentiality level.
- The administrator is still the one who is in charge or creating the security policy, as in MAC systems, but the system will ensure that each user will only see the items that have a confidentiality level allowed to him based on some system configurations and the user trust level

NON-REPUDIATION/ACCOUNTABILITY

- Tracking who is accessing the systems and which of the requests were denied along with additional details like the Timestamp and the IP address from where the requests came from.
- Means confirmation sent by receiver to sender that the requested services or information was successfully received as Digital confirmation e.g. Digital Certificates, this not only serves as acknowledgement but also helps to validate both sender and receiver is genuine.