Sensitive Data

Salalila, John Carlo & Santos Beah (BSIS 3C)

What is Sensitive Data?

Sensitive data is any information that is personal, confidential, or otherwise potentially compromising if it were to be accessed or disclosed without permission. This can include things like passwords, financial information, medical records, or personally identifiable information (PII) such as name, address, and social security number. It is important to protect sensitive data and handle it with care, as unauthorized access or disclosure of this information can have serious consequences for individuals and organizations.

Who has access to the sensitive data, and what level of access do they have?

The individuals who have access to sensitive data, and the level of access they have, will depend on the specific context and the requirements of the particular application. In general, it is important to carefully control and limit access to sensitive data to only those individuals who need it for legitimate business purposes.

The level of access that individuals have to sensitive data may also vary depending on their role and responsibilities. For example, an administrator may have full access to all data, while a regular user may only have access to a limited subset of data.
It is important to carefully evaluate and control access to sensitive data to ensure that it is protected from unauthorized access or disclosure.

What is the potential impact of unauthorized access or disclosure?

The potential impact of unauthorized access or disclosure of sensitive data can vary depending on the nature of the data and the circumstances of the access or disclosure. In general, unauthorized access or disclosure of sensitive data can have serious consequences for individuals and organizations.

Overall, it is important to carefully evaluate the nature of sensitive data and the potential impact of unauthorized access or disclosure in order to ensure that it is properly protected and handled with care.

How is the sensitive data backed up and recovered in case of a data loss event?

In general, it is important to have a plan in place for backing up and recovering sensitive data in case of a data loss event, such as a hardware failure, cyber attack, or natural disaster. This may include regularly creating backups of the data and storing them in a secure location, such as on a separate server or in the cloud.

When recovering data, it is important to ensure that the data is restored accurately and securely, and that the integrity of the data is maintained. This may involve testing the restored data to ensure that it is complete and correct, and taking steps to secure the data and prevent unauthorized access during the recovery process.

Examples of Sensitive Data

It is important to protect this information and handle it with care, as unauthorized access or disclosure can have serious consequences.

01 Personal identification information (PII), such as name, address, social security number, and date of birth.

02 Financial information, such as bank account numbers, credit card numbers, and investment records.

03 Passwords and login credentials for online accounts.

04 Government-issued identification numbers, such as passport numbers or driver's license numbers.

05 Personal communication records, such as emails and text messages.

Ways to protect Sensitive Data

By following these best practices and being vigilant about protecting sensitive data, you can help to ensure that it stays secure.

USE STRONG AND UNIQUE PASSWORDS

Use complex passwords that are difficult to guess or crack, and avoid using the same password for multiple accounts.

ENCRYPT DATA

Encrypting data makes it unreadable to anyone who does not have the necessary decryption key. This can be especially important for protecting data in transit, such as when it is being sent over the internet.

USE SECURE NETWORKS

Use secure networks and connections whenever possible, and avoid using public WiFi networks for sensitive activities.

Ways to protect Sensitive Data

By following these best practices and being vigilant about protecting sensitive data, you can help to ensure that it stays secure.

KEEP SOFTWARE AND SECURITY PROTOCOLS UP TO DATE

Make sure to keep all software and security protocols up to date to ensure that you are protected against the latest threats.

LIMIT ACCESS TO SENSITIVE DATA

Only grant access to sensitive data to individuals who need it for legitimate business purposes, and make sure to revoke access when it is no longer needed.

USE TWO-FACTOR AUTHENTICATION

Two-factor authentication adds an extra layer of security by requiring a second form of verification, such as a code sent to a phone or an authentication app.

Ways to protect Sensitive Data

By following these best practices and being vigilant about protecting sensitive data, you can help to ensure that it stays secure.

USE SECURITY TOOLS

Use security tools such as firewalls, antivirus software, and intrusion detection systems to protect against cyber threats.

REGULARLY MONITOR AND REVIEW SECURITY

Regularly monitor and review your security measures to ensure that they are effective and up to date.

Questions

01 In your own understanding, what is sensitive data?

02 How do you protect your sensitive data? Such as password, personal information, etc.

03 What do you think are the repercussions of not taking extra measures to protect it?

04 Give Atleast one sensitive data types.

05 How should we implement this sensitive types?