Data or information within an organization often includes valuable assets that must be protected from security threats. From the moment data is created to the time it is destroyed, the life cycle of data is a broad topic within information security. Careful planning and design is essential to protect the data throughout its entire life cycle.

# Instructions

For this assignment, prepare a strategic plan to manage data within financial databases throughout its data life cycle. Your plan should include the following stages:

1. Collect
2. Store
3. Process
4. Share
5. Archive
6. Destroy

For each stage, outline and provide a detailed explanation of the important considerations, the security threats, the strategy used and the expected results from the strategy.

**Collect**

**Important Considerations:**

* Is the data sensitive?
* Should the data be accessible to the public?
* Can the data be verified?
* Is the data collected withing legal boundaries?

**Security Threats**

* If the data is sensitive or if it shouldn’t be accessible to the public, where/how should it be stored?
* What damages can occur if the data is compromised?

**Strategy**

To collect data, one must first ensure compliance with laws and regulations within the legal boundaries they are operating under. Personal data must be collected fairly and only used for the purposes that have been authorised by the owner.

**Expected Results**

If you follow the steps outlined above, then there should not be any issues with the collection of data.

**Store**

**Important Considerations**

* What performance requirements are required for reading and writing the data?
* What type of storage system is required (SSD or HDD)?
* How much data is being stored?

**Security Threats**

* Is the data properly stored to prevent theft?

**Strategy**

First one must consider what type of storage system is required, an SSD would be the superior option but if the requirements are low then an HDD would be the cheaper option. Next you must consider the scale and get an appropriate amount of storage to accommodate expected demands. Finally one should consider what kind of encryption/security is going to be placed on the data, based on the sensitivity of said data.

**Expected Results**

If you considered all your needs, then you should be able to store your data effectively and securely.

**Process**

**Important Considerations**

* What is the quality of data being processed?
* Quality Control
* Quality Assurance

**Security Threats**

* Is the person handling the data qualified/authorized to do so?

**Strategy**

First one must assess the quality of the data to be processed. Ensure that the data is accurate, relevant, precise, reliable, current, complete, and timely. If all these standards are met, then one must ensure that quality control and assurance are upheld. To make sure all these standards are being followed then the person handling the data must be qualified and authorised to do so.

**Expected Results**

If all these standards are upheld, then there will be no complaints with the processing of the data.

**Share**

**Important Considerations**

* What is/should be the policy regarding the sharing of data?
* Who needs access to the data?
* How is the data secured when it is being accessed or shared?

**Security Threats**

* Is the data custodian qualified?
* What kind of authentication is in place to protect against imposters?

**Strategy**

First one must consider who will require access to the data, and how to verify them when they request it. Next the data should be encrypted and stored in a secure location to prevent data theft. The data custodian should be qualified to handle the data.

**Expected Results**

If you followed this advice then you should encounter no issues when sharing your data.

**Archive  
Important Considerations**

* What is the policy on data backup?
* How often is data recovered from the archive?
* How long is the retention period?

**Security Threats**

* Is the data archived securely?

**Strategy**

First it is recommended to archive the data in an offsite facility to ensure that the data is retained even in the even of a natural disaster. Next one must set the policy on data backup, which can vary greatly depending on need. Ensure that the data is secured safely behind encryption and physical security. Make note of the how long the data needs to be kept for via legal guidelines.

**Expected Results**

You should be able to securely archive your data if you follow these guidelines.

**Destroy**

**Important Considerations**

* How sensitive is the data that needs to be destroyed?
* What is the proper disposal method for the data and data storage?

**Security Threats**

* Can the data be recovered after it is destroyed?

**Strategy**

Once it has been determined that the data is sensitive and it must be destroyed, there are three recommended methods to do so. Overwriting data over and over, Degaussing by using electric current to de-magnetize hard drives, and to physically shred the drive into small pieces.

**Expected Results**

If you did all that, you should be good to go.