DATA SECURITY ANALYSIS

[YOUR NAME]
[ROLL NO]

HOW TO USE THIS TEMPLATE

- We have provided these slides as a guide to ensure you submit all the required components to complete your project successfully.
- When presenting your project, remember that these slides are merely a guide. We strongly encourage you to embrace your creative freedom and make changes that reflect your unique vision as long as the required information is present.
- You can add slides to the template when your answers or screenshots do not fit on the previously provided pages.
- Delete this and all other project instruction slides before submitting your project.
- **Remember to add your name and the date to the cover page.**

Project Scenario

Overview

You have recently joined JFin Payments, a rapidly growing online payment processing firm based in Los Angeles, California, as a Data Security Analyst. With over 100,000 **customers across the United States and Europe**, JFin Payments handles a diverse range of sensitive data, including employee and customer profiles, financial information, company communications, and intellectual property.

As a key member of the data security team, your primary responsibility is to ensure the confidentiality, integrity, and availability of the company's data assets. To achieve this, you will collaborate with the data warehouse and application and infrastructure security teams to develop and implement robust data security policies, procedures, and controls.

Throughout the project, you will leverage your expertise in data security, regulatory compliance, and risk management to fortify JFin Payments' data security posture. Your insights and recommendations will play a crucial role in safeguarding sensitive information, maintaining customer trust, and supporting the company's continued growth in the competitive online payment processing industry.

Section 1:
Data Governance

Strategic Data Security Policies

In the rapidly evolving digital landscape, the security of sensitive information remains a cornerstone of JFin Payments' operations. The diversity of data managed—from customer financial details to internal communications and intellectual property—presents a complex challenge in maintaining confidentiality, integrity, and availability. Your role involves contributing to the safeguarding of this information by understanding and evaluating the benefits of key data security program policies provided by the company.

- Review the policy items provided on the next slide.
- For each item, write a brief explanation of its benefits. Consider aspects such as data security, compliance, risk management, and operational efficiency.

Strategic Data Security Policies

IT Staff should perform a data classification annually, or when there are notable business or technology changes.
[Explain the benefits of including this guidance in the Data Security Policy]
IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.
[Explain the benefits of including this guidance in the Data Security Policy]
IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.
[Explain the benefits of including this guidance in the Data Security Policy]

Data Classification

As a Data Security Analyst at JFin Payments, one of your primary responsibilities is to ensure the confidentiality, integrity, and availability of the company's data assets. To effectively protect sensitive information, it is crucial to establish a data classification system that categorizes data based on its sensitivity and criticality. In this task, you will define three data types (confidential, internal, and public) and classify the datasets provided by the data warehouse team accordingly.

- Define each of the three data types: confidential, internal, and public
- Categorize each dataset provided by the data warehouse team into one of the three data types

Data Classification

Confidential: [Write a clear definition of the data type]
Internal: [Write a clear definition of the data type]
Public: [Write a clear definition of the data type]

Categorize each dataset into one of the three data types

Dataset	Data Type
Employee profile data	
Customer profile data	
Company email	
Repository of previously published blogs	
Internal employee newsletters	
Technology engineering diagrams	
Intellectual property	

Data Regulations

It is essential to understand the regulatory landscape surrounding the company's data assets. Different data types may be subject to various regulations, depending on their sensitivity and the nature of the information they contain. In this task, you will identify the regulations that apply to each data type (confidential, internal, and public) and provide a justification for why each regulation applies.

- For each data type (confidential, internal, and public), identify the relevant data regulations (if any)
- Provide a justification for why each identified regulation applies to the specific data type

Data Regulations

Confidential	[Applicable Regulation]: [Write the justification here]
Internal	
Public	

Regulatory Compliance

Your responsibilities include recommending and implementing security controls that ensure compliance with applicable data regulations. By establishing clear security policies and procedures, you can help the company meet its regulatory obligations and protect sensitive data from unauthorized access, use, or disclosure. In this task, you will design six security policy items that address the requirements of the identified regulations relevant to JFin Payments' data.

- Write six security policy items that address the requirements of the applicable data regulations
- Each policy item should be written in clear, concise language and follow the provided format
- The policy items should cover various aspects of data security, such as data encryption, access control, data disposal, and breach notification

Regulatory Compliance

[Write a security policy item that addresses the requirements of any of the applicable data regulations]
[Write a security policy item that addresses the requirements of any of the applicable data regulations]
[Write a security policy item that addresses the requirements of any of the applicable data regulations]
[Write a security policy item that addresses the requirements of any of the applicable data regulations]
[Write a security policy item that addresses the requirements of any of the applicable data regulations]
[Write a security policy item that addresses the requirements of any of the applicable data regulations]

Section 2:
Data Confidentiality

Securing Disks

As a Data Security Analyst at JFin Payments, one of your responsibilities is to ensure the confidentiality and integrity of data stored on virtual disks. Implementing disk encryption using strong cryptographic keys is an effective way to protect sensitive data from unauthorized access. In this task, you will generate an RSA key (2048 bits) and leverage it to enable encryption on a disk, providing evidence of successful implementation through screenshots.

- Generate an RSA key (2048 bits) for disk encryption
- Create a disk encryption set using the generated RSA key
- Create a disk and encrypt it with the disk encryption set
- Provide the following screenshots as evidence of successful implementation:
  - Screenshot 1: Successful key generation page
  - Screenshot 2: Successful creation of disk encryption set page
  - Screenshot 3: Successful disk encryption page

Securing Disks

Place the screenshot of the generated key.

Securing Disks

Place the screenshot from configuration Page after you have encrypted the Virtual Disk Image of the VM

Section 3:
Data Integrity

File Integrity Verification

ensuring the integrity of critical files is essential to maintain the security and reliability of the company's systems. One common method for verifying file integrity is by generating and comparing cryptographic hashes, such as SHA256. In this task, you will generate SHA256 hashes for public files Additionally, you will submit a screenshot of the generated hashes as part of your evidence.

- Go to https://drive.google.com/file/d/1XT0Uc1Q4FWtRAxhfX1m9DsXhU599ytv0/view?usp=drive_link
- Generate SHA256 hashes
- Compare the generated hashes with the original hashes on the next slide and explain what your findings mean in terms of file integrity
- Submit a screenshot of the generated hashes

File Integrity Verification

Download public.dll from dll-files.com and verify Hash.

Version 14.0.0.130
The original public.dll hash: f7761cd21b7461fd126ecbac1fa7e516138349fb

[Explain your findings here (e.g., whether the files have been modified or remain unchanged)]

Place the screenshot of the generated hashes here

Auditing Security Settings

It is crucial to ensure that the company's virtual machines (VMs) are properly configured to maintain the security and integrity of the systems and data they host. Auditing the security settings of VMs helps identify potential vulnerabilities and ensures compliance with industry best practices and regulatory requirements. In this task, you will access the audit settings on a VM and provide screenshots as evidence of the password policy, account lockout policy, audit policy, and security options configurations.

- Navigate to the password policy screen and take a screenshot
- Navigate to the account lockout policy screen and take a screenshot
- Navigate to the audit policy screen and take a screenshot
- Navigate to the security options screen and take a screenshot
- Ensure that all screenshots are clear, legible, and capture the relevant information

Steps to get Local Security Policy

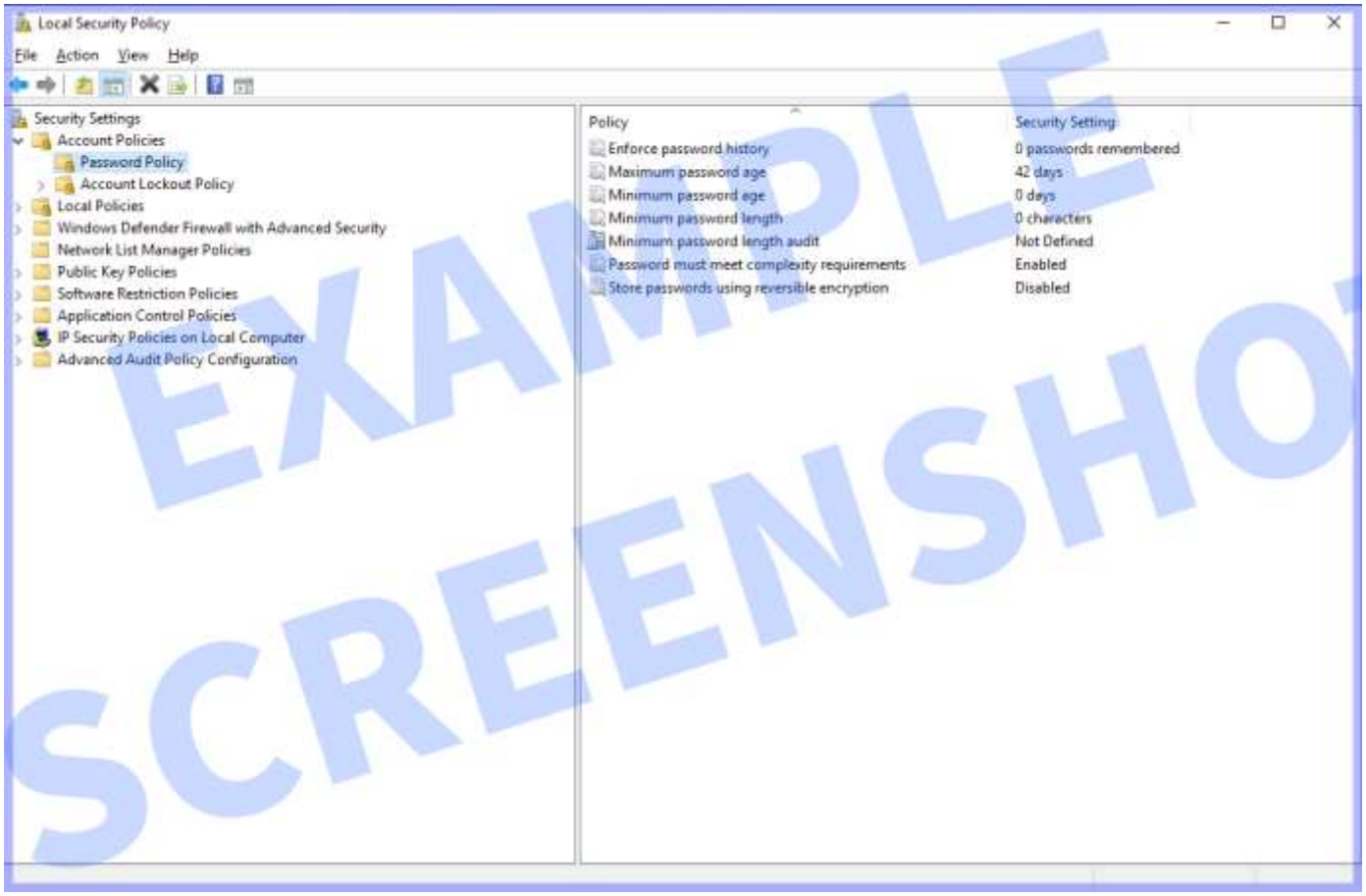
```
@echo off
pushd "%~dp0"

dir /b %SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~3*.mum >List.txt
dir /b %SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-Package~3*.mum >>List.txt

for /f %%i in ('findstr /i . List.txt 2^>nul') do dism /online /norestart /add-package:"%SystemRoot%\servicing\Packages\%%i"
pause
```

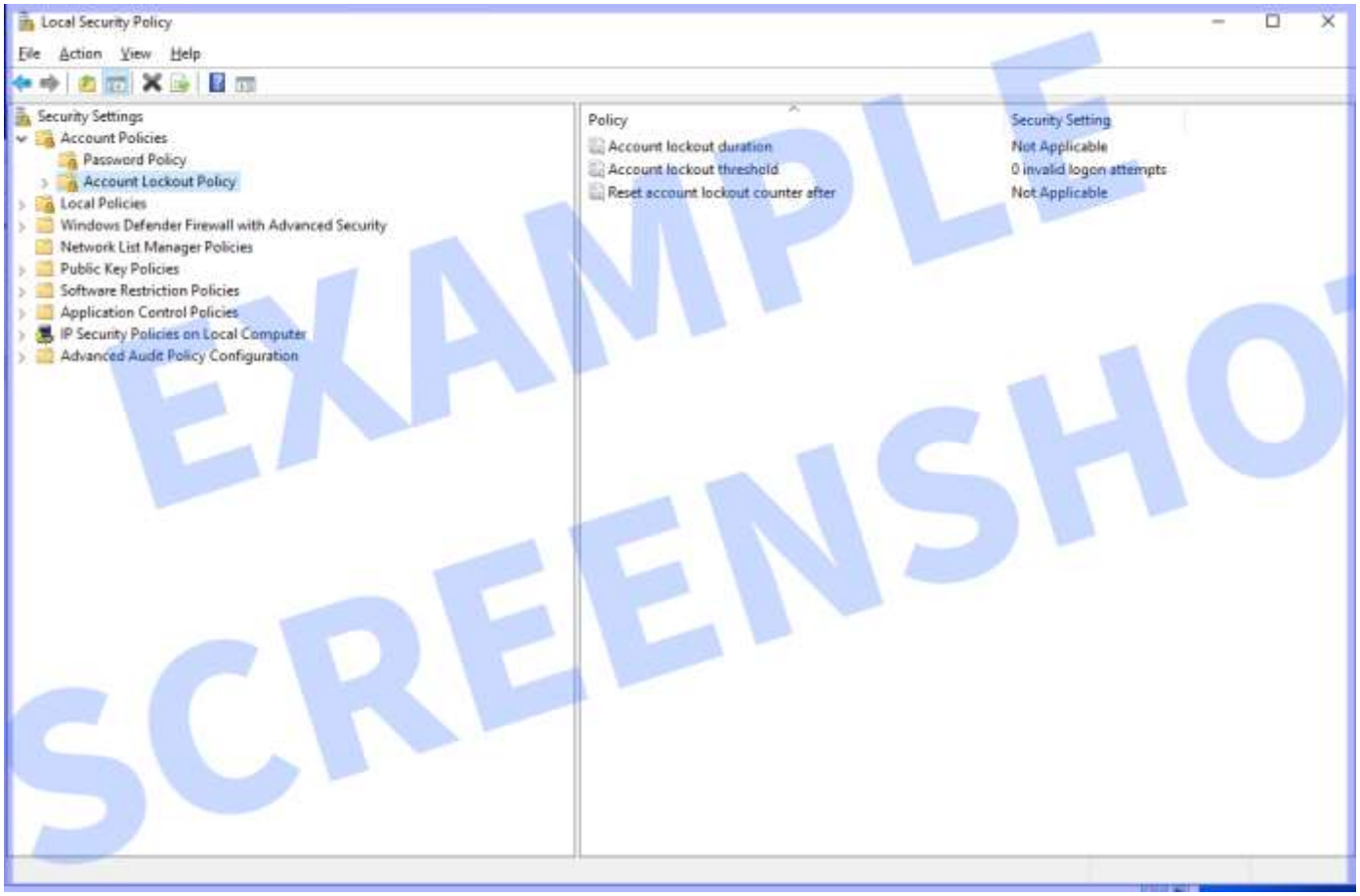
Auditing Security Settings

Place the screenshot of the password policy screen here



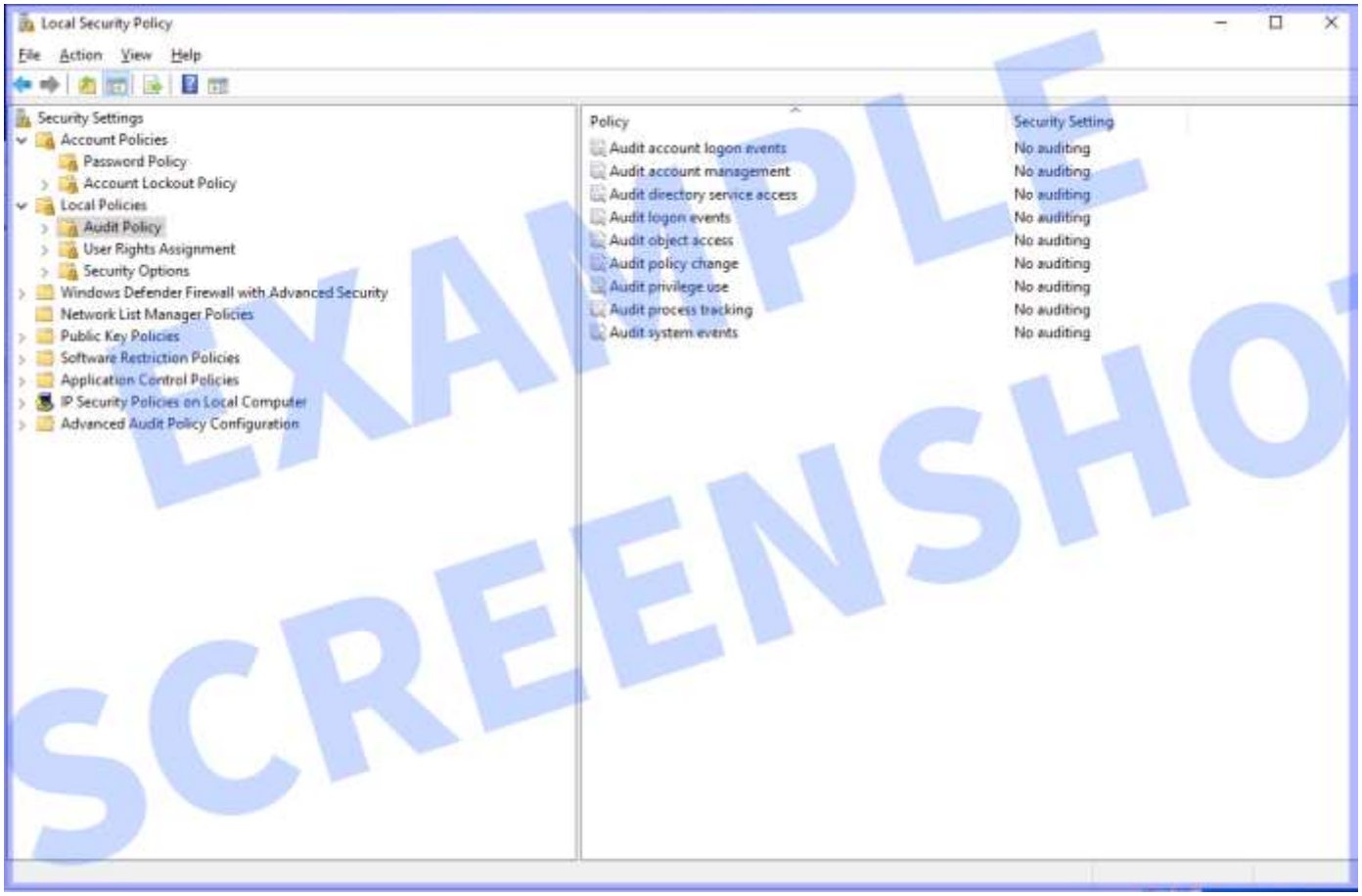
Auditing Security Settings

Place the screenshot of account lockout policy screen here



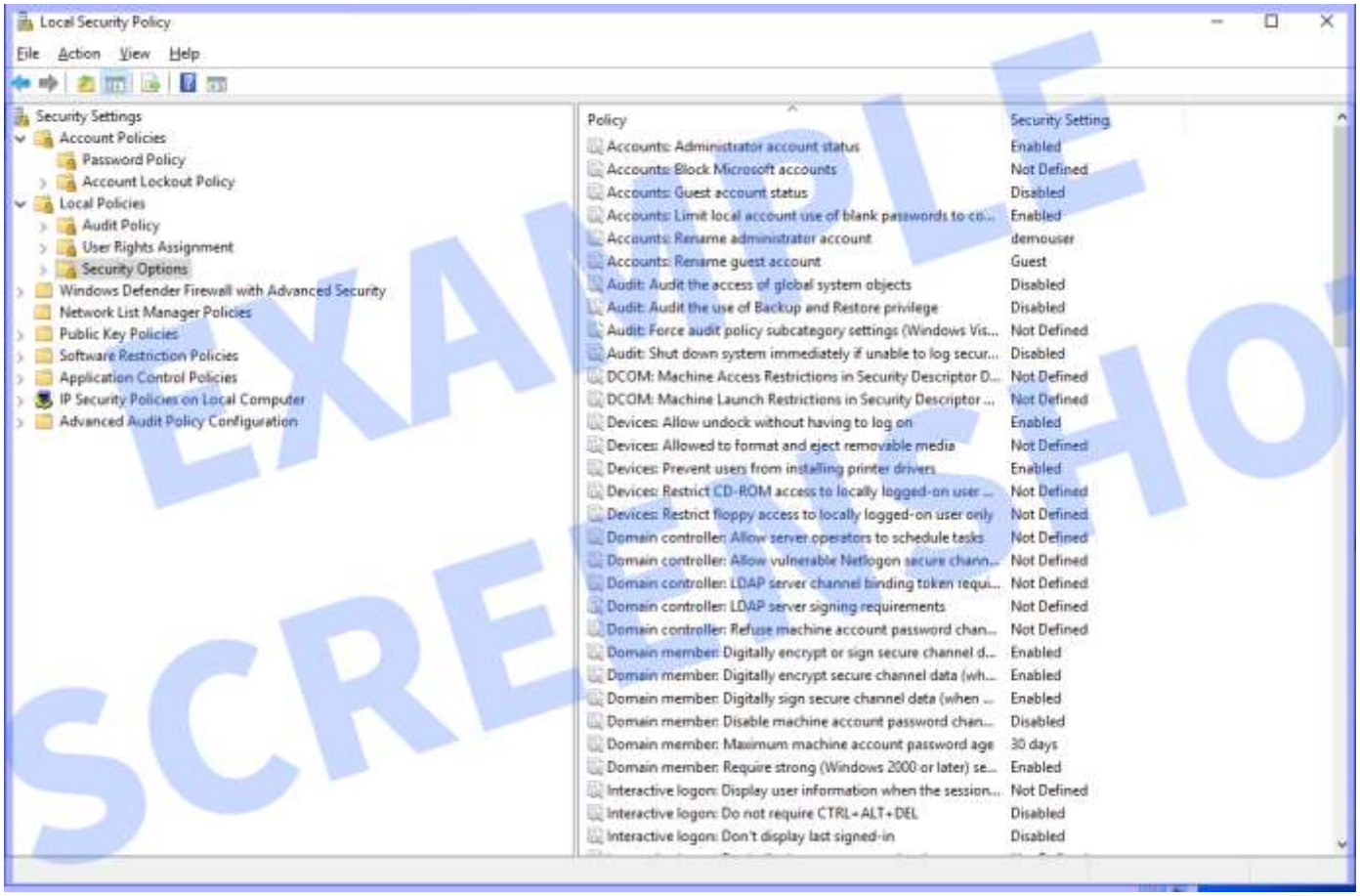
Auditing Security Settings

Place the screenshot of the audit policy screen here



Auditing Security Settings

Place the screenshot of the security options screen here



Enhancing VM Security

The next step is to provide actionable recommendations based on your findings. Review the existing security policies and options on the VM and provide 4 specific security recommendations that the company should implement on the machine to strengthen its overall security posture and comply with industry best practices and regulatory requirements. You do not need to implement any of this.

- Review the password policy, account lockout policy, audit policy, and security options of the VM
- Identify areas where security improvements can be made based on industry best practices and security standards
- Provide 4 specific security recommendations that the company should set on the machine
- For each recommendation, include a brief justification explaining the benefits and importance of the proposed setting

Enhancing VM Security

1. [Recommendation]
[A brief justification]
2. [Recommendation]
[A brief justification]
3. [Recommendation]
[A brief justification]
4. [Recommendation]
[A brief justification]

Section 4:
Data Availability

Developing a Data Backup Strategy

In the previous task, you categorized JFin Payments' data into confidential, internal, and public data types and identified the applicable regulations for each category. Building upon this foundation, it is essential to establish a robust data backup strategy to ensure data availability, integrity, and compliance with regulatory requirements. In this task, you will recommend a backup frequency and retention period for each data type, providing justifications for your recommendations based on industry best practices and regulatory obligations. Although multiple different backups are needed for each data type, **only recommend the shortest amount of time appropriate between backups for the data type**.

- Recommend a backup frequency for each data type, specifying at least how often a backup should be run (e.g., real-time, daily, weekly, as needed)
- Propose a retention period for each data type, indicating how long the backups should be kept (e.g., 30 days, 90 days, 1 year)
- Provide justifications for your recommended backup frequency, considering factors such as data criticality, regulatory requirements, and industry best practices

Developing a Data Backup Strategy

Confidential Data	
Backup Frequency:	[Write the backup frequency here]
Retention Period:	[Write the retention period here]
[Write the justification for your recommended backup frequency here]	
Internal Data	
Backup Frequency:	[Write the backup frequency here]
Retention Period:	[Write the retention period here]
[Write the justification for your recommended backup frequency here]	

Developing a Data Backup Strategy

Public Data	
Backup Frequency:	[Write the backup frequency here]
Retention Period:	[Write the retention period here]
[Write the justification for your recommended backup frequency here]	

Creating a Backup

Continuing our focus on data protection and disaster recovery, creating regular backups of critical systems is essential to ensure data availability and minimize downtime in case of incidents or failures. In this task, you will create a backup of the LabVM and provide a screenshot of the LabVM Backup screen as proof of initiation.

- Start the backup process for the VM in VirtualBox
- Take a screenshot of the VM Backup screen, clearly showing the initiated backup process
- You do not need to wait until the backup process is finished

Creating a Backup

Place the screenshot of the VM Backup screen here