

Data Security Analysis in Online Payment Processing



Uriyah Adriel Sam
20-05-2024



Digital Project Management

Project Scenario



Digital Project Management

Section One:

Data Governance



Strategic Data Security Policies

IT Staff should perform a data classification annually, or when there are notable business or technology changes.

Data Security: Regular data classification ensures that all data within the organization is categorized based on sensitivity and value. This helps in applying appropriate security measures to protect sensitive data, reducing the risk of data breaches.

Compliance: Many regulatory frameworks require organizations to classify data to ensure compliance with data protection laws. Regular classification helps in meeting these legal obligations and avoiding potential fines and sanctions.

Risk Management: By identifying and classifying data, IT staff can prioritize security efforts on the most critical and sensitive data, effectively managing risks associated with data loss or exposure.

Operational Efficiency: Clear data classification helps in streamlining data management processes, making it easier for staff to handle data appropriately and efficiently, thus enhancing overall operational productivity.



Strategic Data Security Policies

IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.

Data Security: Classifying applications and critical systems ensures that security measures are tailored to the specific needs and risks associated with different systems. This helps in protecting applications and systems from cyber threats.

Compliance: Certain applications and systems may be subject to specific regulatory requirements. Regular classification ensures that these systems are compliant with relevant regulations, reducing legal and financial risks.

Risk Management: Understanding the criticality of different applications and systems allows IT staff to focus security resources on the most crucial assets, mitigating risks effectively and ensuring business continuity.

Operational Efficiency: By classifying applications and systems, IT staff can optimize resource allocation and support efforts, ensuring that critical systems receive the attention and maintenance they require, thus minimizing downtime and enhancing performance.



Strategic Data Security Policies

IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.

Data Security: Regular regulatory assessments help ensure that security practices align with current legal and regulatory standards, reducing vulnerabilities and enhancing overall data protection.

Compliance: Staying updated with regulatory requirements through annual assessments ensures that the company remains compliant with laws and standards, avoiding potential legal issues and financial penalties.

Risk Management: By identifying regulatory changes and understanding their impact, the organization can proactively manage compliance risks and adjust security measures accordingly to address new threats and vulnerabilities.

Operational Efficiency: Regulatory assessments help streamline compliance processes, ensuring that IT staff are aware of and can efficiently implement necessary changes. This proactive approach reduces the likelihood of reactive, costly compliance efforts and enhances operational stability.



Data Classification

Confidential: Confidential data is highly sensitive information that, if disclosed, could cause significant harm to the company, its employees, or its customers. Access to this data is strictly limited to authorized personnel who require it to perform their duties. Examples include personal identifiable information (PII), financial records, and proprietary information.

Internal: Internal data is information intended for use within the organization. While not as sensitive as confidential data, unauthorized access or disclosure could still have negative impacts on the company. This data is typically shared among employees and departments but is not meant for public release.

Public: Public data is information that is intended for public dissemination and does not require any special protections. This data can be freely shared and accessed by anyone without any potential harm to the company.

Categorize each dataset into one of the three data types

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



Data Regulations

Confidential	<p>General Data Protection Regulation (GDPR):</p> <p>Justification: GDPR applies to the handling of personal data of individuals within the European Union. Confidential data often includes personal identifiable information (PII) of employees and customers, which necessitates compliance with GDPR to protect individual privacy and avoid significant fines and penalties.</p>
Internal	<p>Sarbanes-Oxley Act (SOX):</p> <p>Justification: Internal data such as company emails and technology engineering diagrams may include financial information and internal controls documentation. SOX requires the safeguarding of such internal information to ensure accuracy in financial reporting and adherence to internal control protocols.</p>
Public	<p>Copyright Law</p> <p>Justification: Public data, such as previously published blogs, must adhere to copyright laws to protect intellectual property rights. This ensures that the company respects and protects the intellectual property of others while sharing its own content legally.</p>



Regulatory Compliance

Data Encryption

Policy: All confidential and sensitive data, including personal identifiable information (PII) and payment card information, must be encrypted both at rest and in transit using industry-standard encryption protocols (e.g., AES-256, TLS 1.2 or higher).

Regulation Addressed: GDPR, HIPAA, PCI DSS

Justification: Encryption ensures the protection of sensitive data from unauthorized access and breaches, meeting the requirements of GDPR for data protection, HIPAA for safeguarding health information, and PCI DSS for securing payment card information.

Access Control

Policy: Access to confidential and sensitive data must be restricted based on the principle of least privilege, ensuring that only authorized personnel with a legitimate business need have access to such data. Multi-factor authentication (MFA) must be used for accessing critical systems.

Regulation Addressed: GDPR, SOX, PCI DSS

Justification: Limiting access to sensitive data helps prevent unauthorized access and potential data breaches, complying with GDPR's data protection principles, SOX's internal control requirements, and PCI DSS's access control mandates.

Data Disposal

Policy: All confidential and sensitive data must be securely disposed of when no longer needed, using methods such as shredding, degaussing, or secure wiping to ensure data is irrecoverable.

Regulation Addressed: GDPR, HIPAA, PCI DSS

Justification: Proper data disposal methods are essential to prevent data leaks and unauthorized recovery, ensuring compliance with GDPR's data minimization and retention principles, HIPAA's requirements for PHI disposal, and PCI DSS's data protection standards.



Regulatory Compliance

Breach Notification

Policy: In the event of a data breach involving confidential or sensitive data, the incident must be reported to the relevant regulatory authorities and affected individuals within 72 hours of discovery. A comprehensive incident response plan must be in place to manage and mitigate data breaches.

Regulation Addressed: GDPR, HIPAA

Justification: Timely breach notification is crucial for regulatory compliance and for mitigating the impact of data breaches. GDPR mandates reporting within 72 hours, and HIPAA requires prompt notification of breaches involving PHI.

Regular Audits and Assessments

Policy: Conduct regular audits and assessments, including annual regulatory assessments and security audits, to ensure ongoing compliance with applicable data regulations and to identify and address potential security vulnerabilities.

Regulation Addressed: SOX, PCI DSS, GDPR

Justification: Regular audits help ensure continuous compliance with regulatory requirements and identify security gaps, as required by SOX for internal controls, PCI DSS for payment card data security, and GDPR for data protection.

Data Minimization and Retention

Policy: Only collect and retain the minimum amount of personal data necessary for business operations, and establish clear data retention schedules to ensure data is only kept as long as needed for regulatory or business purposes.

Regulation Addressed: GDPR, SOX

Justification: Data minimization reduces the risk of data breaches and ensures compliance with GDPR's principle of data minimization and SOX's requirements for maintaining accurate and necessary financial records.



Digital Project Management

Section Two: Data Confidentiality



Securing Disks

Place the screenshot from the Keys page of the Key Vault you created, with the generated key.

Microsoft Azure

Search resources, services, and docs (G+)

Home > MyVault22 | Overview > MyVault22

MyVault22 | Keys ☆ ...

Key vault

Search

+ Generate/Import Refresh Restore Backup Manage deleted keys

The key 'UriyahKey' has been successfully created.

Name	Status	Expiration date
UriyahKey	✓ Enabled	5/21/2026

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Events

Objects

Keys

Secrets

Certificates

Settings

Access configuration

Networking

Microsoft Defender for Cloud

Properties



Securing Disks

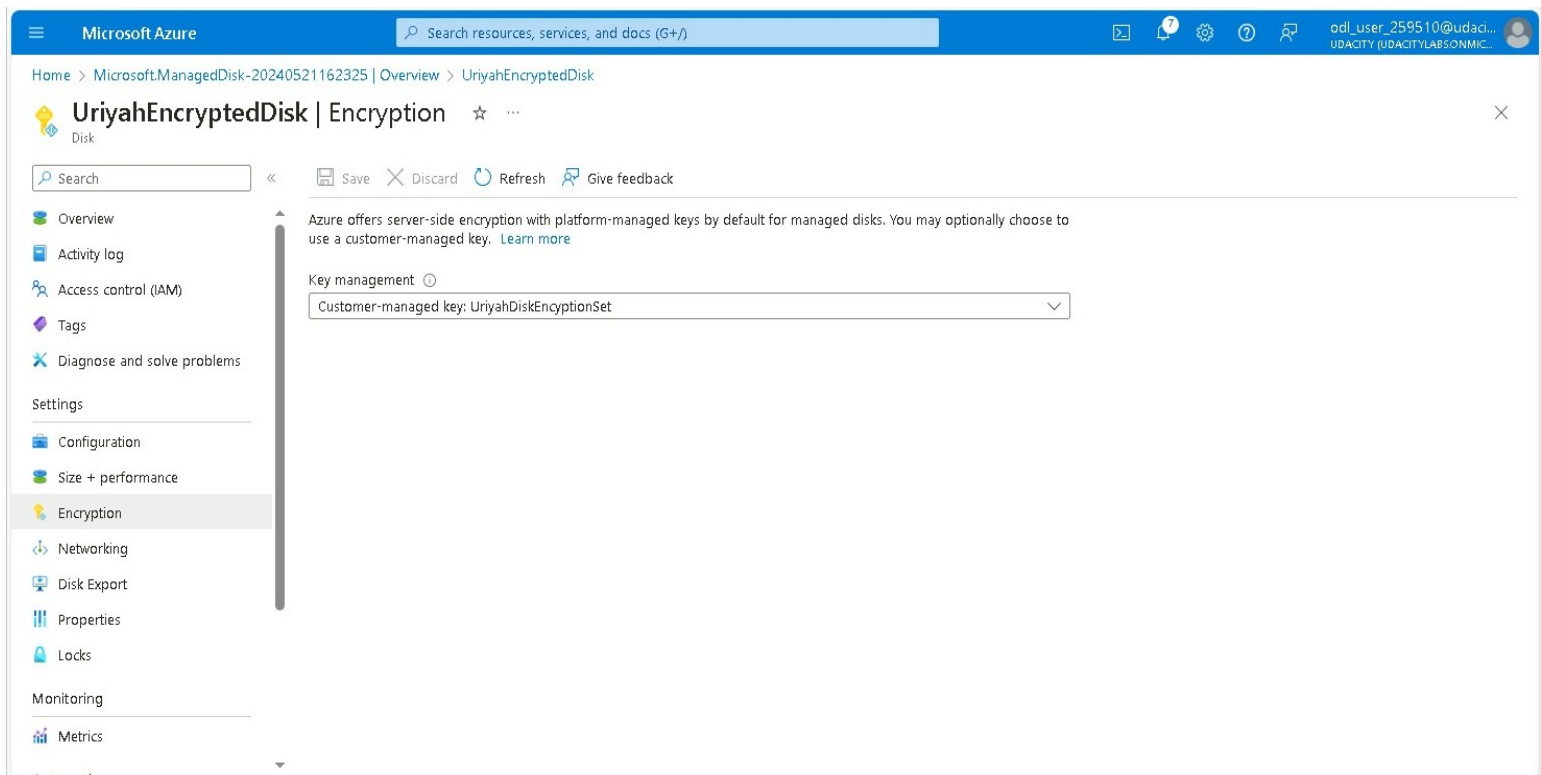
Place the screenshot from Key page of the Disk Encryption Set you created

The screenshot shows the Microsoft Azure portal interface for managing a Disk Encryption Set. The breadcrumb navigation indicates the path: Home > Microsoft.DiskEncryptionSet-20240521161729 | Overview > UriyahDiskEncryptionSet. The page title is 'UriyahDiskEncryptionSet | Key'. The left sidebar contains a navigation menu with options: Overview, Activity log, Access control (IAM), Tags, Settings, Resources, Key (selected), Properties, Locks, Automation, CLI / PS, Tasks (preview), Export template, and Help. The main content area shows instructions to 'Select a key vault and a key in the same subscription and region as the disk encryption set to replace the current key in your encryption set.' The 'Current key' field displays a URL: 'https://MyVault22.vault.azure.net/keys/UriyahKey/9966974641aa4ced925d9...'. Below this is a 'Change key' button. There are three settings: 'Auto key rotation' (unchecked), 'User-assigned identity' (with a 'Select an identity' link), and 'Multi-tenant application' (with a 'Select an application' link). A warning icon and message state: 'You are required to select the user-assigned managed identity first.'



Securing Disks

Place the screenshot from the Encryption page of the Disk you created





Digital Project Management

Section Three: Data Integrity



File Integrity Verification

The original DSysLaunch2pm.dll hash:

B029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE3251184D4

The original SSysLaunch9am.dll hash:

76A586439464553482A529108A0BAD0FECDA3F9337BAE2098697F170026B6733

The file "DsysLaunchpm.dll" has been modified, as evidenced by a discrepancy in its hash value. Conversely, the file "SSysLaunch9am.dll" remains unaltered, given that its hash value has not changed

```
PS C:\Users\demouser> Get-FileHash C:\Users\demouser\Documents\Esnd-4\DSysLaunch2pm.dll -Algorithm SHA256
```

Algorithm	Hash	Path
SHA256	A029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE32511F56E	C:\Users\demouser\Documents...

```
PS C:\Users\demouser> Get-FileHash C:\Users\demouser\Documents\Esnd-4\SSysLaunch9am.dll -Algorithm SHA256
```

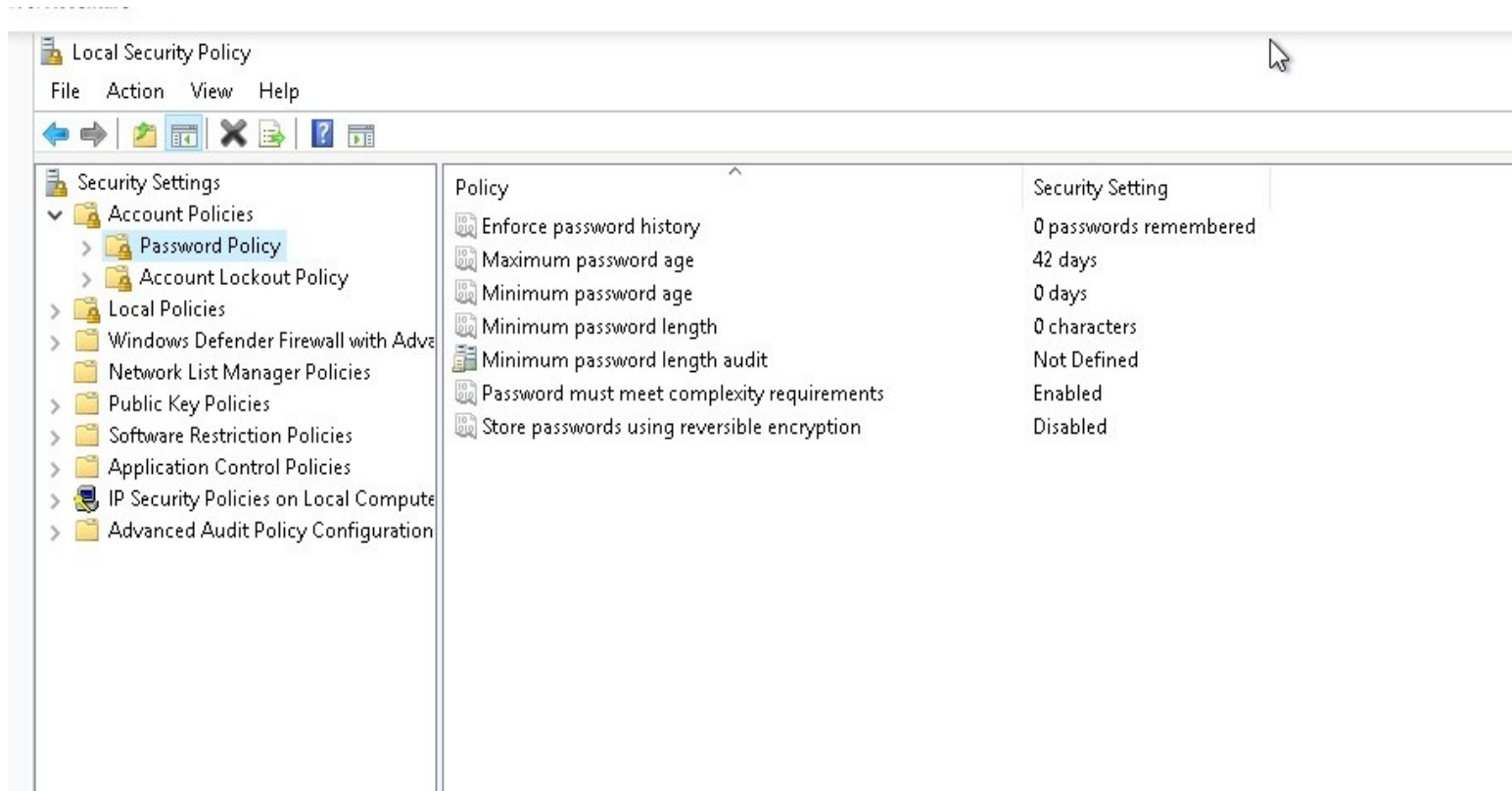
Algorithm	Hash	Path
SHA256	76A586439464553482A529108A0BAD0FECDA3F9337BAE2098697F170026B6733	C:\Users\demouser\Documents...

```
PS C:\Users\demouser>
```




Auditing Security Settings

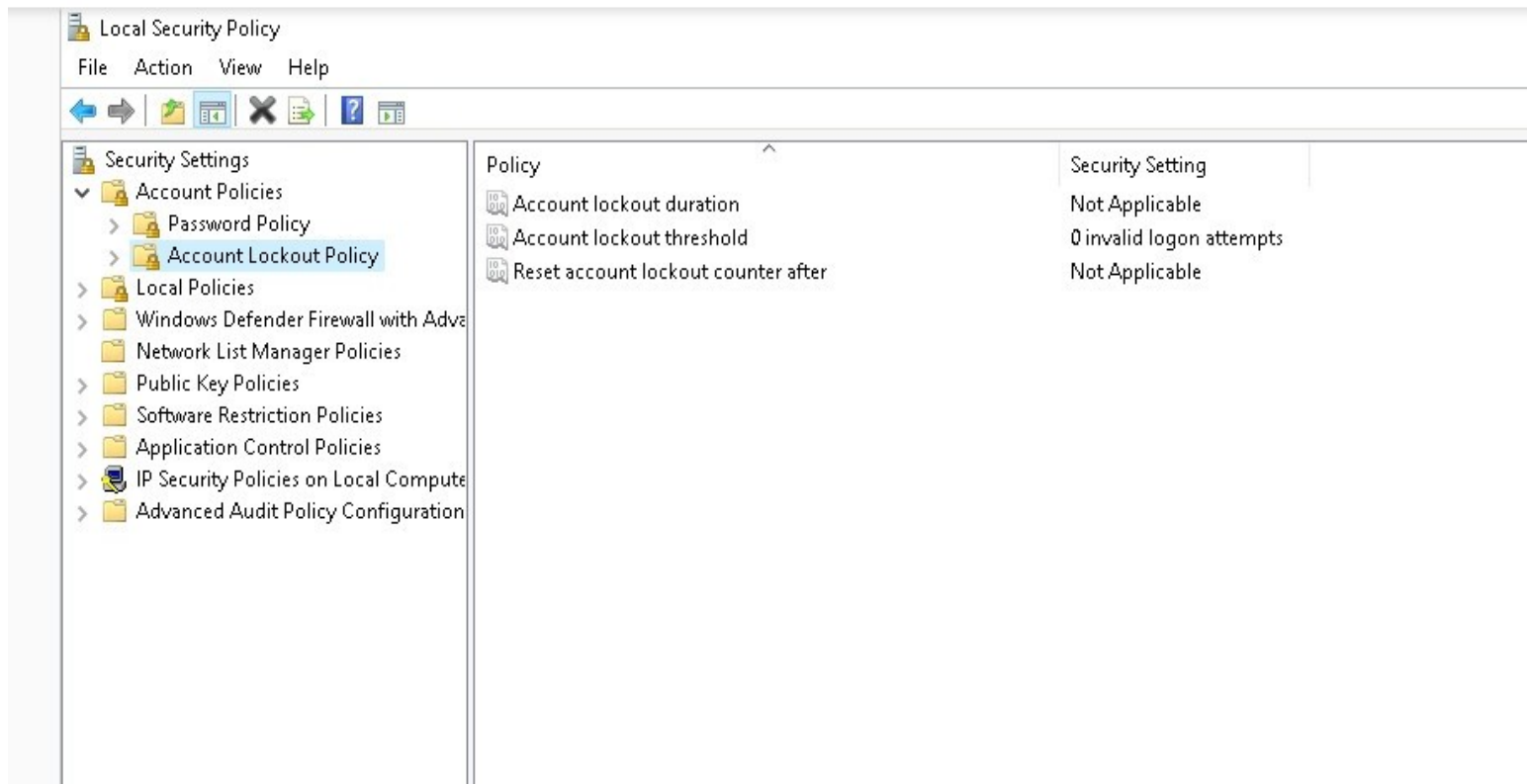
Place the screenshot of the password policy screen here





Auditing Security Settings

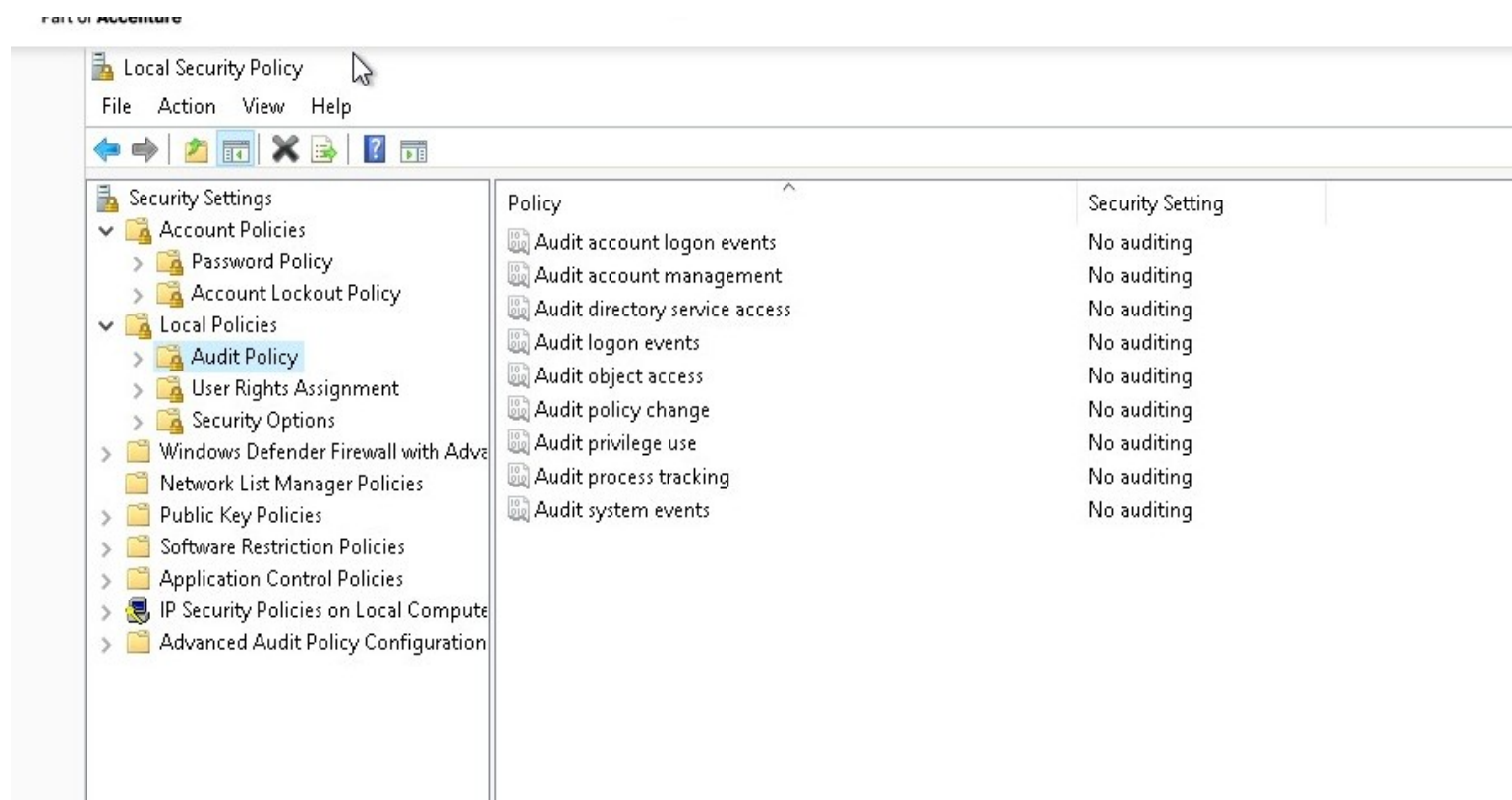
Place the screenshot of account lockout policy screen here





Auditing Security Settings

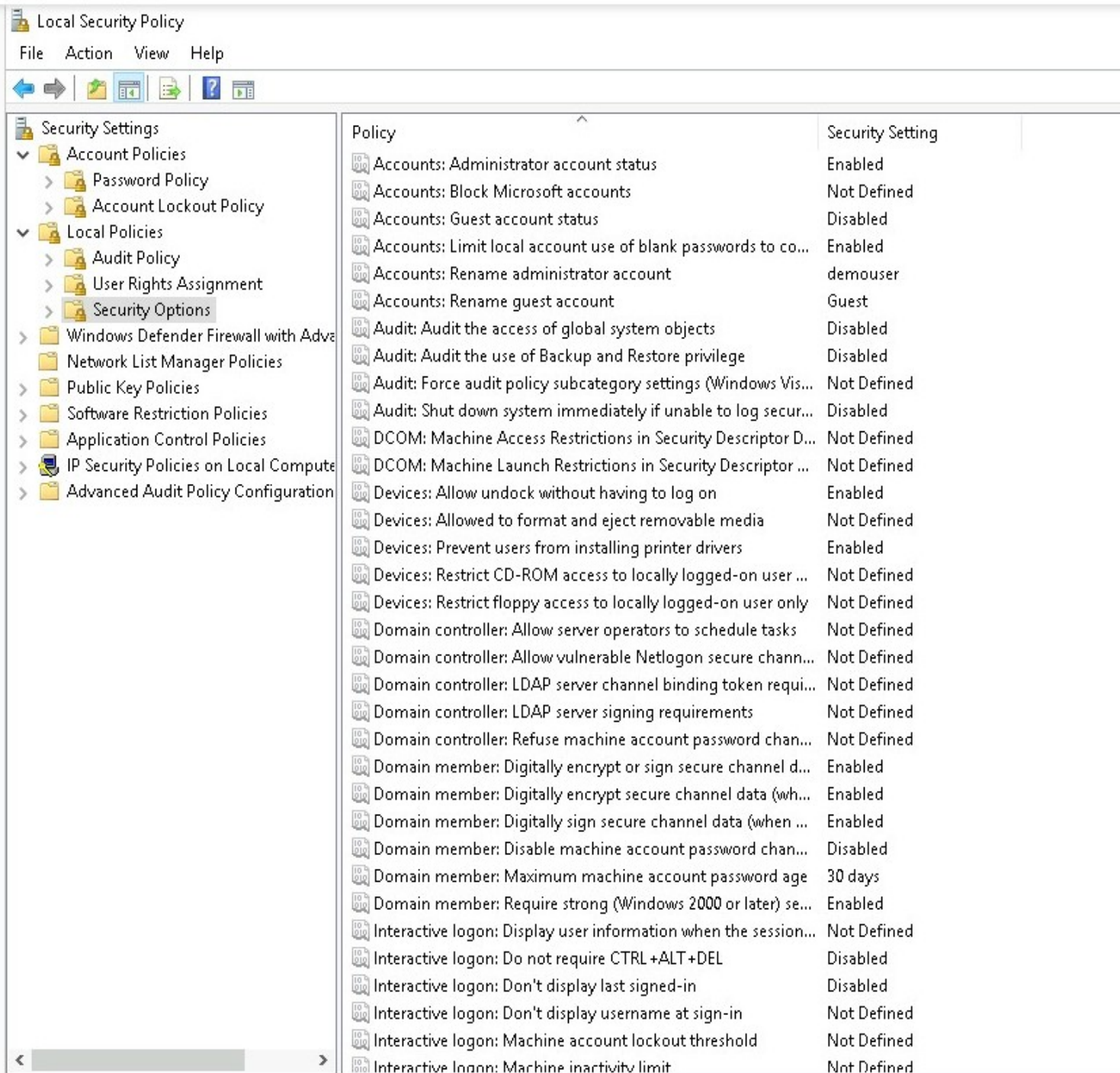
Place the screenshot of the audit policy screen here





Auditing Security Settings

Place the screenshot of the security options screen here



The screenshot displays the 'Local Security Policy' window. The left-hand navigation pane shows a tree structure under 'Security Settings', with 'Local Policies' expanded and 'Security Options' selected. The main pane on the right contains a table of security policies and their current status.

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	demouser
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive Logon: Machine inactivity limit	Not Defined



Enhancing VM Security

1. Enforce Strong Password Policy

Strong passwords significantly reduce the risk of unauthorized access by making it more difficult for attackers to guess or crack passwords. Regular password changes and complexity requirements ensure that compromised passwords are not in use for extended periods, aligning with best practices and security standards.

2. Implement Account Lockout Policy

An account lockout policy helps protect against brute force attacks by temporarily disabling accounts after multiple failed login attempts. This reduces the likelihood of unauthorized access through repeated guessing of passwords while still allowing legitimate users to regain access after a short period.

3. Enable Audit Policy

Auditing is crucial for detecting and responding to security incidents. By logging and reviewing critical activities, the organization can identify potential security breaches, monitor compliance with security policies, and take corrective actions promptly. This also supports forensic investigations in the event of a security incident.

4. Configure Security Options

Enhancing security options helps protect the system from unauthorized changes, reduces the attack surface by disabling unnecessary services, and ensures that only trusted software is loaded during the boot process. This combination of settings strengthens overall system security and mitigates various vulnerabilities.



Digital Project Management

Section Four: Data Availability



Developing a Data Backup Strategy

Confidential Data

Backup Frequency:	Daily
Retention Period:	1 Year

Confidential data, such as employee profile data, customer profile data, and intellectual property, is highly sensitive and critical to the operations and security of JFin Payments. Daily backups ensure that any changes or additions to this data are captured regularly, minimizing the risk of data loss. Retaining these backups for 1 year aligns with regulatory requirements and industry best practices for financial and personal data protection, ensuring that the company can recover data in the event of data corruption, loss, or a security breach. Longer retention periods help in meeting compliance with regulations such as GDPR, CCPA, and PCI DSS, which may mandate extended retention of financial and personal data for audit and legal purposes.



Developing a Data Backup Strategy

Internal Data	
Backup Frequency:	Weekly
Retention Period:	90 Days
<p>Internal data, including company emails, internal employee newsletters, and technology engineering diagrams, is important for the company's operational efficiency and internal communications but does not typically require the same level of immediacy as confidential data. Weekly backups strike a balance between data protection and resource utilization, ensuring that significant changes are captured without excessive redundancy. A 90-day retention period is sufficient to meet operational needs and internal policies, providing a reasonable timeframe for recovering from accidental deletions or modifications while not excessively burdening storage resources. This practice aligns with internal data management standards and ensures business continuity without unnecessary data hoarding.</p>	



Developing a Data Backup Strategy

Public Data	
Backup Frequency:	Monthly
Retention Period:	30 Days
<p>Public data, such as the repository of previously published blogs, is less critical since it is already available in the public domain and can often be recreated or sourced from the web if necessary. Monthly backups are adequate to capture any updates or changes while minimizing storage and processing overhead. A 30-day retention period is practical for this data type, ensuring that any recent updates can be recovered without long-term storage of redundant public data. This approach conserves storage resources while maintaining the ability to restore public-facing content if needed, following a cost-effective and efficient data management strategy.</p>	



Creating a Backup

Place the screenshot of the LabVM Backup screen here

The screenshot displays the Microsoft Azure portal interface for managing a virtual machine named 'LabVM-259510'. The left-hand navigation pane lists various management options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Bastion, Windows Admin Center, and Networking. The main content area is titled 'LabVM-259510 | Backup' and includes a search bar and a set of action buttons: Backup now, Restore VM, File Recovery, Stop backup, Resume backup, Delete backup data, Restore to Secondary Region, and Undelete. A banner promotes the Business Continuity Center. Below this, the 'Essentials' section provides key backup details: Recovery services vault (vault599), Subscription (Udacity CloudLabs Sub - 35), Subscription ID (20bd5839-016e-4d9f-9805-63a5953c-b007), Alerts (in last 24 hours), Jobs (in last 24 hours), Backup Pre-Check (Passed), Last backup status (Warning: Initial backup pending), Backup policy (EnhancedPolicy-7egydki2 (Enhanced)), Oldest restore point, and Included disk(s) (All disks). A 'Recovery points' section explains the filtering for the last 30 days and provides links for vault-archive. At the bottom, three bar charts show consistency levels: CRASH CONSISTENT (0), APPLICATION CONSISTENT (0), and FILE-SYSTEM CONSISTENT (0). The table below these charts has columns for Creation time, Consistency, and Recovery type, but currently shows 'No restore points available'.

Creation time	Consistency	Recovery type
No restore points available.		