

Data Security Analysis in Online Payment Processing



Lakshya Sharma
08/05/2024



Project Scenario

Project Scenario

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 One:

Data Governance



Strategic Data Security Policies

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

Benefits of including this guidance in the Data Security Policy:

Maintaining Relevance and Accuracy:

1. Regular data classification ensures that the categorization of data assets remains up-to-date and accurately reflects the evolving nature of my organization's information landscape.

2. Adapting to Changing Needs:

Business and technology changes can introduce new data sources, storage locations, or processing requirements, which may necessitate updates to the data classification scheme

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

Benefits of including this guidance in the Data Security Policy:

1. Comprehensive Risk Management:

Application and critical system classification allows my organization to identify and prioritize the security needs of its most vital information assets and supporting infrastructure.

2. Efficient Resource Allocation:

The classification of applications and critical systems enables my organization to prioritize its security efforts and resources, ensuring that the most sensitive and business-critical assets receive the highest level of protection.

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

Benefits of including this guidance in the Data Security Policy:

1. Adapting to Evolving Regulations:

By mandating periodic regulatory assessments, the policy enables my organization to stay informed and responsive to these changes, ensuring that its data security controls and procedures remain compliant.

2. Continuous Improvement:

The regulatory assessment process provides valuable insights into my organization's data security program, highlighting areas for improvement and opportunities to enhance its effectiveness.



Data Classification

Confidential data refers to the most sensitive information within my organization, which if disclosed, could cause significant harm to my company, its employees, or our customers. This includes, but is not limited to, financial records, customer payment details, employee personally identifiable information (PII), and intellectual property.

Internal data refers to information that is intended for use within my organization and should not be shared publicly. This includes business plans, operational procedures, internal communications, and other non-public data that is critical to my organization's operations.

Public data is information that is intended for external distribution and does not contain any sensitive or confidential details. This includes marketing materials, publicly available product information, and other data that the organization has explicitly designated as suitable for public access.

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	Confidential
Intellectual property	Confidential



Data Regulations

Confidential	<p>General Data Protection Regulation (GDPR) The GDPR applies to confidential data as it contains personally identifiable information (PII) of EU citizens, such as customer financial records and employee PII. The GDPR mandates strict requirements for the processing, storage, and protection of personal data to ensure the privacy and rights of data subjects.</p> <p>Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. PCI DSS was designed to prevent cybersecurity breaches of sensitive data and reduce the risk of fraud for organizations that handle payment card information.</p>
Internal	<p>ISO/IEC 27001 is an information security management system (ISMS) standard that provides a framework for establishing, implementing, maintaining, and continually improving my organization's information security practices. This standard is applicable to my organization's internal data that is not classified as confidential or public, such as our proprietary business information, internal communications, and employee records.</p>
Public	<p>Americans with Disabilities Act (ADA) The ADA requires that public-facing websites and digital content be accessible to individuals with disabilities, including those with visual, auditory, or cognitive impairments.</p>



Regulatory Compliance

1. Disaster Recovery and Business Continuity:

My company must develop and maintain a comprehensive disaster recovery and business continuity plan to ensure the availability of critical systems and data in the event of a disruption.

The disaster recovery plan must be regularly tested and updated to address evolving threats and business requirements.

2. Backup Storage and Retention:

Backup data must be stored in both on-site and off-site locations to ensure redundancy and protection against local disasters or facility-level incidents.

Backup data must be retained for a period determined by applicable regulations, such as the GDPR's requirement to maintain personal data for no longer than necessary.

3. Backup Testing and Restoration:

My company must regularly test the integrity and recoverability of backup data, including the ability to restore data from backups.

Restoration procedures must be documented, and employees with authorized access must be trained on the backup and restoration processes.

4. Backup Requirements:

All confidential data, including customer financial records, employee PII, and intellectual property, must be backed up on a regular basis.

Backup frequency must be determined based on the sensitivity and criticality of the data, with more frequent backups for highly sensitive information.

5. Access Provisioning and Review:

All requests for access to confidential data, including customer financial records, employee PII, and intellectual property, must be reviewed and approved by the designated data owners or security team.

Access privileges must be granted based on the principle of least privilege, where users are assigned the minimum necessary permissions to perform their job functions.

6. Third-Party Access Management:


Access granted to third-party vendors, contractors, or partners must be carefully reviewed and approved, with clear documentation of the scope and duration of the access.

Third-party access must be monitored and regularly reviewed to ensure that it remains necessary and appropriate, and access must be promptly revoked when



Section Two: Data Confidentiality

[Home](#) > [JFin-Payment | Overview](#) > [JFin-Payment](#)



JFin-Payment | Keys

☆ ...

Key vault


[+ Generate/Import](#)
[↻ Refresh](#)
[↑ Restore Backup](#)
[🔑 Manage deleted keys](#)

	Name	Status	Expiration date
	JFin-Payments-Key	✓ Enabled	5/21/2026

Overview

Access policies

✓ Objects

 Keys



Securing Disks

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

Home / Disk Encryption Set / DiskEncryptionSet



DiskEncryptionSet | Key



Disk Encryption Set



Save



Discard



Give feedback



Overview



Activity log



Access control (IAM)



Tags

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. [Learn more](#)

Current key

<https://fin-payments-key-vault.vault.azure.net/keys/Fin-Payments-Key/4ab...>

[Change key](#)



Securing Disks

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

The screenshot shows the Microsoft Azure portal interface for the 'EncryptedDisk' resource. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information. The left sidebar lists various services, with 'EncryptedDisk' selected. The main content area displays the 'Encryption' settings for the disk. It includes a 'Key management' dropdown menu set to 'Customer-managed key: DiskEncryptionSet'. The page also features a 'Search' bar, 'Save', 'Discard', 'Refresh', and 'Give feedback' buttons. The 'Encryption' section is highlighted in the sidebar, and the main content area shows the 'Key management' dropdown menu.

Microsoft Azure

Search resources, services, and docs (G+)

odl_user_259487@udaci... UDACITY

All services > EncryptedDisk

EncryptedDisk | Encryption ☆ ...

Search

Save Discard Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Size + performance

Encryption

Networking

Disk Export

Properties

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Key management ⓘ

Customer-managed key: DiskEncryptionSet



Section Three: Data Integrity

File Integrity Verification



The original DSysLaunch2pm.dll hash:
A029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE32511
Generated DSysLaunch2pm - Copy.dll hash:
A029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE32511

The original SSysLaunch9am.dll hash:
76A586439464553482A529168A0BAD0FECDA3F9337BAE2098697F170026B6733
Generated SSysLaunch9am - Copy.dll hash:
76A586439464553482A529168A0BAD0FECDA3F9337BAE2098697F170026B6733

Comparism:

The generated hash for the copy DSysLaunch2pm.dll file matches the original hash. This indicates that the DSysLaunch2pm. file remains intact and has not been modified. The generated hash for the copy SSysLaunch9am.dll file matches the original hash. This indicates that the SSysLaunch9am.dll file remains intact and has not been modified. Hence the DSysLaunch2pm.dll file has not been modified or corrupted, as the generated hash matches the original hash. The SSysLaunch9am.dll file remains intact, as the generated hash matches the original hash.

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

Algorithm Hash
-----
SHA256 A029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE32511...

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

Algorithm Hash Path
-----
SHA256 76A586439464553482A529168A0BAD0FECDA3F9337BAE2098697F170026B6733 C:\Users\demouser\Do...

PS C:\Users\demouser> Get-FileHash 'C:\Users\demouser\Documents\Esnd-4\DSysLaunch2pm - Copy.dll'

Algorithm Hash Path
-----
SHA256 A029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE32511F56E C:\Users\demouser\Do...

PS C:\Users\demouser> Get-FileHash 'C:\Users\demouser\Documents\Esnd-4\SSysLaunch9am - Copy.dll'

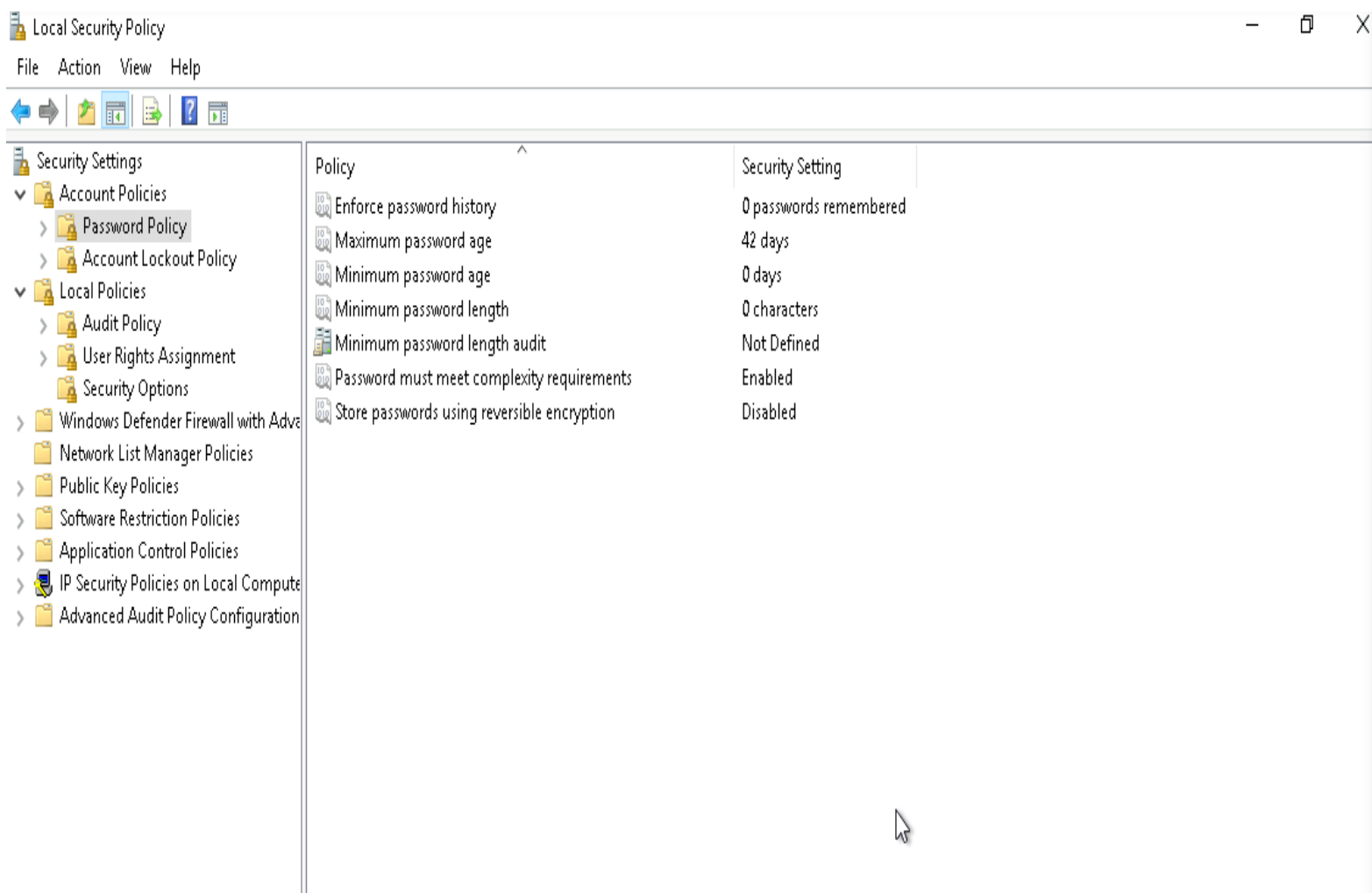
Algorithm Hash Path
-----
SHA256 76A586439464553482A529168A0BAD0FECDA3F9337BAE2098697F170026B6733 C:\Users\demouser\Do...
```

Place the screenshot of the generated hashes here



Auditing Security Settings

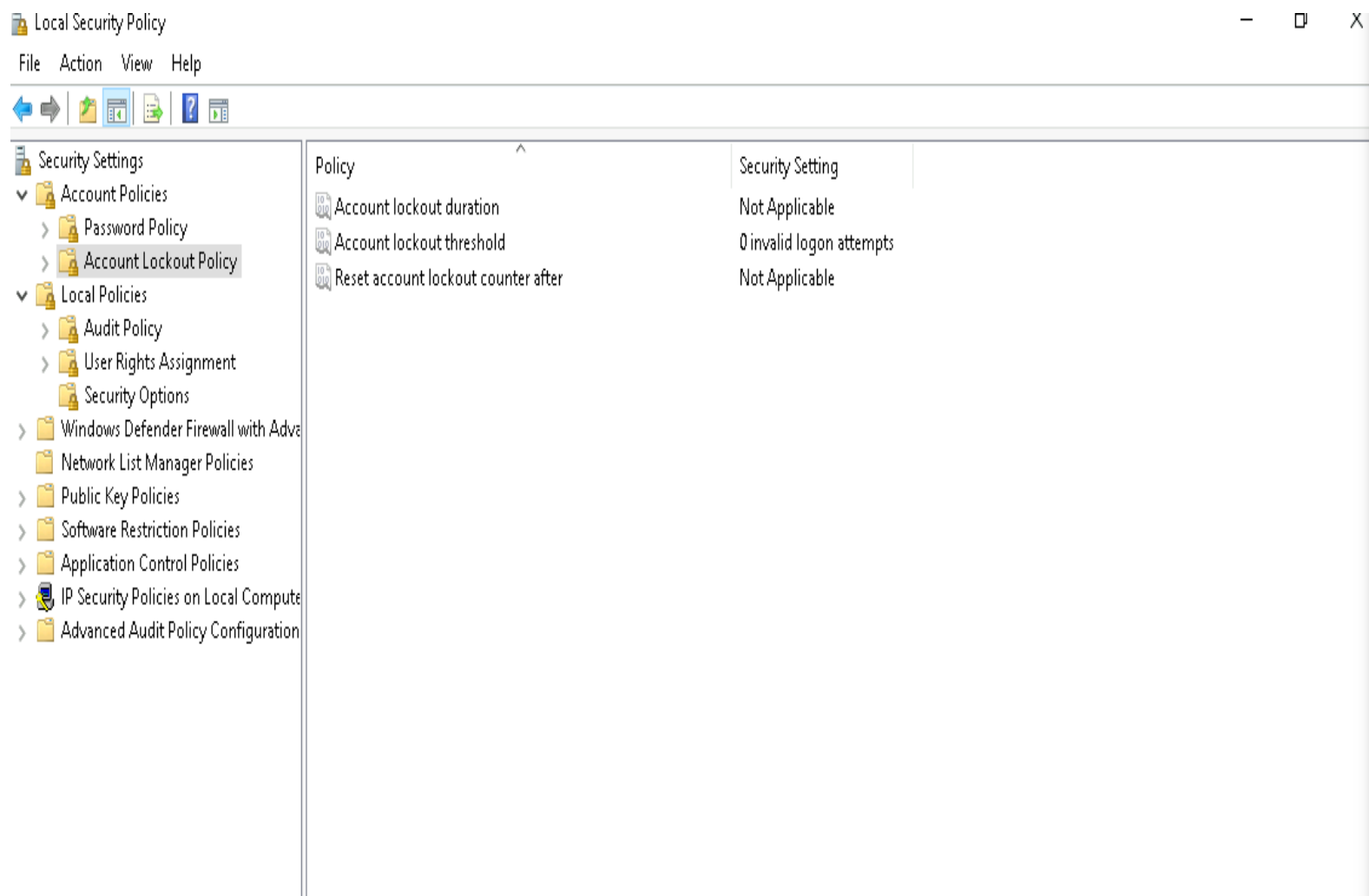
Place the screenshot of the password policy screen here





Auditing Security Settings

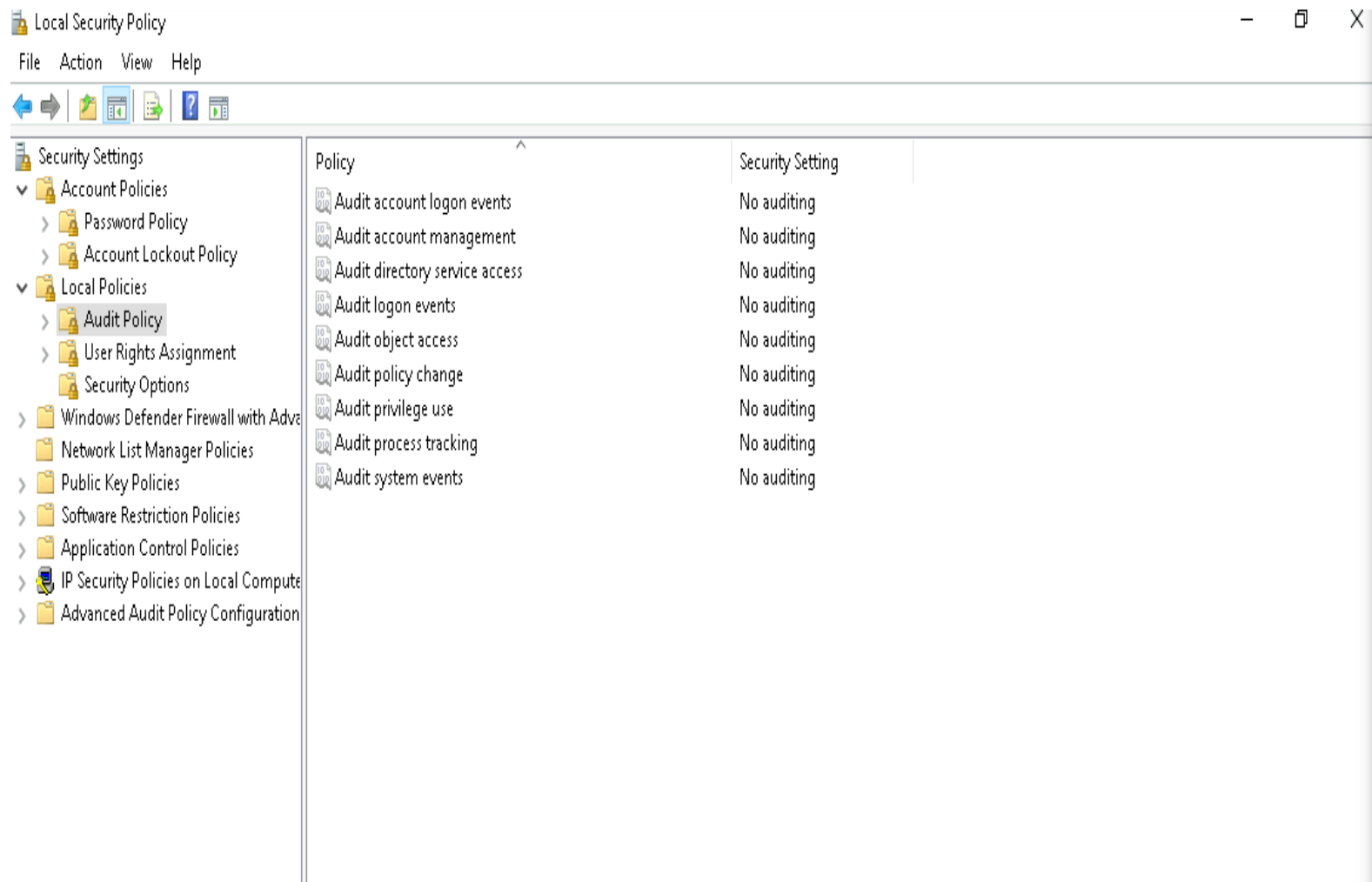
Place the screenshot of account lockout policy screen here





Auditing Security Settings

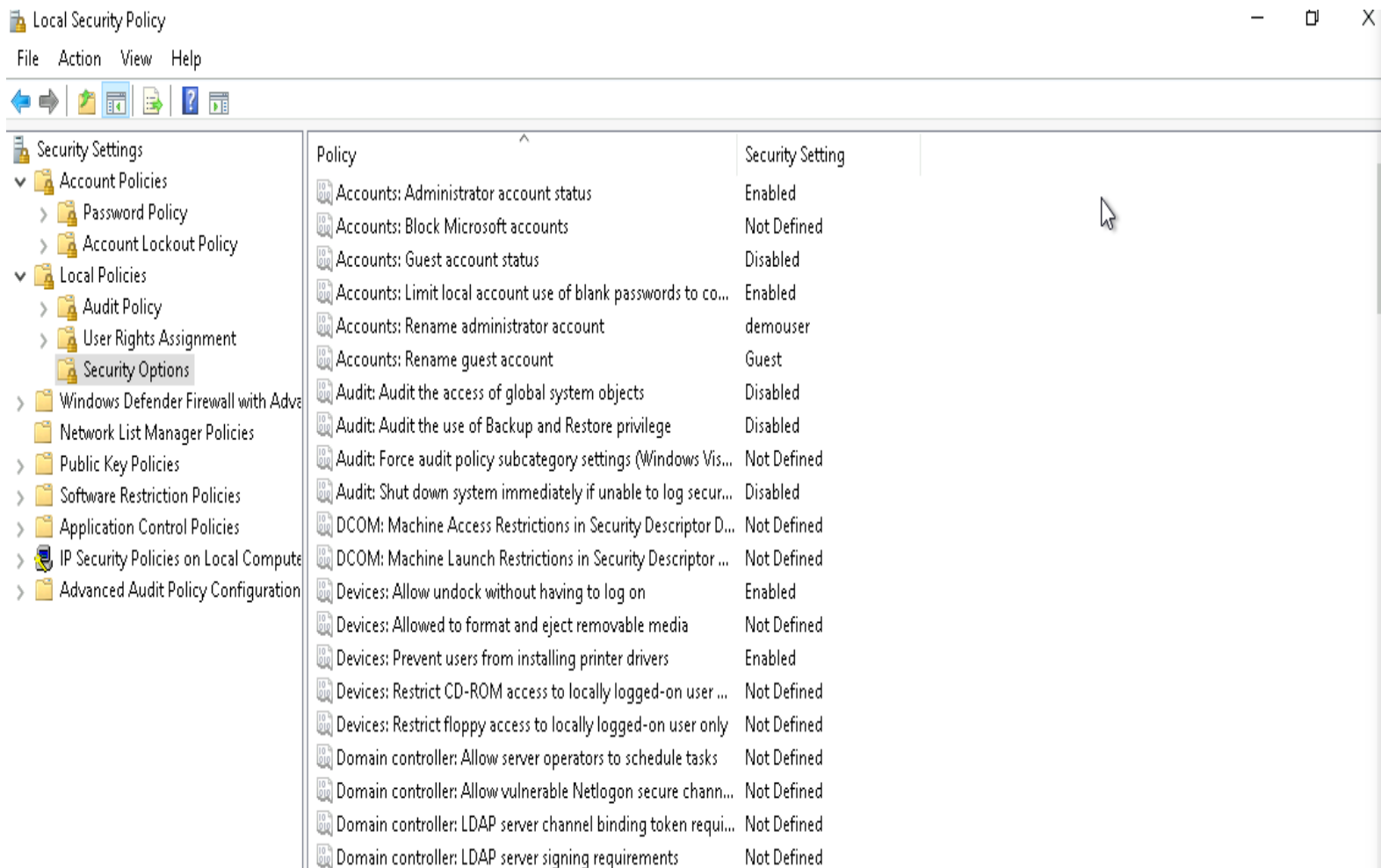
Place the screenshot of the audit policy screen here





Auditing Security Settings

Place the screenshot of the security options screen here





Enhancing VM Security

1. Configure the audit policy to log all successful and failed events for account logon, account management, and privilege use activities.

Extensive auditing and logging of security-relevant events are essential for detecting and investigating security incidents, as well as for demonstrating compliance with regulations such as GDPR and the NIST Cybersecurity Framework. Reviewing audit logs can help identify potential threats or misuse of the system.

2. Disable the "Network security: Allow LocalSystem null session fallback" and "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security options.

These security options, if left enabled, can potentially introduce vulnerabilities and weaknesses that can be exploited by attackers. Disabling unnecessary security options helps reduce the attack surface and aligns with the principle of least privilege, as recommended by security frameworks like the CIS Benchmarks.

3. Set the account lockout threshold to 5 invalid login attempts and the lockout duration to 15 minutes.

Locking out user accounts after a limited number of failed login attempts helps mitigate the risk of brute-force attacks and limits the potential damage from credential-based attacks. The recommended settings strike a balance between security and usability, in accordance with industry standards like the CIS Benchmarks.

4. Increase the minimum password length to at least 12 characters and require the use of complex passwords that include a combination of uppercase, lowercase, numeric, and special characters.

Longer and more complex passwords are significantly more difficult for attackers to guess or crack, providing stronger protection against unauthorized access to the system. This aligns with industry best practices and regulatory standards, such as NIST SP 800-63B, which recommends password lengths of at least 8 characters with complexity requirements.



Section Four: Data Availability



Developing a Data Backup Strategy

Confidential Data	
Backup Frequency:	Real-time/Continuous
Retention Period:	1 year
<p>Real-time/Continuous backups ensure that any changes or updates to the confidential data are immediately captured and protected, minimizing the risk of data loss. This high level of data protection is crucial for safeguarding the confidentiality, integrity, and availability of sensitive information that is critical to my organization's operations and regulatory compliance.</p> <p>Industry best practices, as outlined in frameworks like NIST SP 800-171 and ISO 27001, emphasize the importance of frequent backups and real-time data protection for sensitive data.</p>	
Internal Data	
Backup Frequency:	Daily
Retention Period:	90 days
<p>Daily backups provide a reasonable level of protection against data loss or corruption, ensuring that any changes or updates to the internal data are captured in a timely manner. This backup frequency allows my organization to restore data from recent periods, minimizing the potential impact of data loss or system failures.</p> <p>Industry best practices, as outlined in frameworks such as the NIST Cybersecurity Framework and the CIS Benchmarks, recommend daily or frequent backups for critical business data that is necessary for ongoing operations.</p>	



Developing a Data Backup Strategy

Public Data	
Backup Frequency:	Weekly
Retention Period:	30 days
<p>The 30-day retention period is appropriate for public data, as it allows for the retrieval and restoration of recent versions while minimizing storage requirements. Public data is generally considered low-risk and less critical to the organization's core operations, as it is intended for external consumption and does not contain sensitive or confidential information.</p> <p>This retention period provides my organization with the ability to access and restore public data as needed, supporting various business functions, such as content management and website maintenance. The 30-day timeframe ensures that my organization can fulfill any short-term data recovery or compliance needs related to its public-facing data.</p> <p>Industry frameworks, such as the NIST Cybersecurity Framework, often recommend retention periods in the range of 30 to 90 days for data that is considered less critical or sensitive. The 30-day retention period proposed for JFin Payments' public data aligns with these industry standards and best practices.</p>	



Creating a Backup

Place the screenshot of the LabVM Backup screen here

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar shows 'Microsoft Azure' and a search bar. The user is logged in as 'odl_user_259513@udaci...'. The main content area is titled 'LabVM-259513 | Backup' and includes a sidebar with navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Bastion, Windows Admin Center, Networking, Network settings, and Load balancing. The main panel shows the backup configuration for the virtual machine 'LabVM-259513'. It includes a 'Backup now' button and a 'Restore VM' button. The 'Essentials' section provides key information: Recovery services vault is 'vault970', Subscription is 'Udacity CloudLabs Sub - 36', Subscription ID is '887ccff6-d0cb-4640-90df-b155cab350a0', Alerts (in last 24 hours) are 'View alerts', Jobs (in last 24 hours) are 'View jobs', Backup Pre-Check is 'Passed', Last backup status is 'Warning (Initial backup pending)', Backup policy is 'DailyPolicy-lwgm1lt3 (Standard)', Oldest restore point is '-', and Included disk(s) are 'All disks'. The 'Recovery points' section indicates that the list is filtered for the last 30 days and provides links for vault-archive and long-term recovery points. At the bottom, there are three bars representing consistency: CRASH CONSISTENT (0), APPLICATION CONSISTENT (0), and FILE-SYSTEM CONSISTENT (0).

Microsoft Azure

Search resources, services, and docs (G+/I)

odl_user_259513@udaci... UDACITY

Home > LabVM-259513

LabVM-259513 | Backup ☆ ...

Virtual machine

Search

Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data Restore to Secondary Region Undelete ...

Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →

Essentials JSON View

Recovery services vault : [vault970](#)

Subscription (move) : [Udacity CloudLabs Sub - 36](#)

Subscription ID : 887ccff6-d0cb-4640-90df-b155cab350a0

Alerts (in last 24 hours) : [View alerts](#)

Jobs (in last 24 hours) : [View jobs](#)

Backup Pre-Check : ✓ Passed

Last backup status : ⚠ Warning (Initial backup pending)

Backup policy : [DailyPolicy-lwgm1lt3 \(Standard\)](#)

Oldest restore point : -

Included disk(s) : [All disks](#)

Recovery points

This list is filtered for last 30 days of recovery points. To recover from recovery point older than 30 days, as well as vault-archive, [click here](#).

Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, [click here](#).

CRASH CONSISTENT 0 APPLICATION CONSISTENT 0 FILE-SYSTEM CONSISTENT 0