DATA SECURITY ANALYSIS

27/12/2025
Friday

ANSHUL SHUKLA
CBS-0417

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

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

Regularly reviewing how data is classified helps ensure that information is protected according to its level of sensitivity and importance. As business operations evolve and new technologies or data types are introduced, previously assigned classifications may no longer be accurate. Updating data classification reduces the risk of exposing sensitive information and helps maintain proper access controls. It also supports regulatory compliance and improves overall data handling practices across the organization.

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

Identifying and reviewing critical applications and systems on a regular basis allows the organization to understand which systems are essential for daily operations and security. This process helps IT teams focus protection efforts on high impact systems that handle sensitive data or support core business functions. Keeping classifications up to date improves incident response, minimizes downtime, and ensures that newly introduced or modified systems receive appropriate security controls.

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

Staying aware of applicable laws and regulatory requirements is important for maintaining compliance and avoiding legal issues. Conducting regular regulatory assessments helps the organization adapt to changes in data protection laws or industry standards. This ensures that internal policies and procedures remain aligned with legal expectations. It also helps reduce the risk of penalties, strengthens governance, and builds trust with customers and business partners.

Data Classification

Confidential: Confidential data includes highly sensitive information that, if exposed, could cause serious harm to the company, its employees, or its customers. This type of data requires the highest level of protection and should only be accessed by authorized personnel. Examples include personal information, financial records, and intellectual property.

Internal: Internal data refers to information meant only for use within the organization. While it is not as sensitive as confidential data, unauthorized disclosure could still negatively affect operations or business processes. This data should not be shared outside the company without approval.

Public: Public data includes information that is intended to be shared openly with the public and does not pose a risk if disclosed. This data can be accessed by anyone and does not require special security controls beyond basic integrity protection.

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	GDPR and PCI DSS: These regulations apply because confidential data includes personal, financial, and payment-related information. GDPR requires organizations to protect personal data of individuals and ensure lawful processing, while PCI DSS applies to systems that store or process cardholder data. Both regulations help prevent unauthorized access, data breaches, and misuse of sensitive information.
Internal	GDPR and Internal Security Policies: Internal data may still contain limited personal or employee-related information, which makes GDPR applicable in certain cases. Internal security policies also apply to ensure that this data is accessed only by authorized staff and handled according to company rules, reducing the risk of accidental exposure or misuse.
Public	Copyright and Data Protection Regulations (where applicable): Public data is intended for open access, but it must still comply with copyright laws and data protection rules if any personal information is included. These regulations ensure that published content is lawful, accurate, and does not violate privacy or intellectual property rights.

Regulatory Compliance

1. Data Encryption Policy
All sensitive and confidential data must be encrypted while stored and during transmission to protect it from unauthorized access. Approved encryption standards must be used to meet regulatory and security requirements.

2. Access Control Policy
Access to systems and data must be granted based on job responsibilities and the principle of least privilege. User access should be reviewed regularly and removed immediately when no longer required.

3. Authentication Policy
Strong passwords and multi factor authentication must be enforced to verify user identity. These controls help reduce the risk of unauthorized access and credential based attacks.

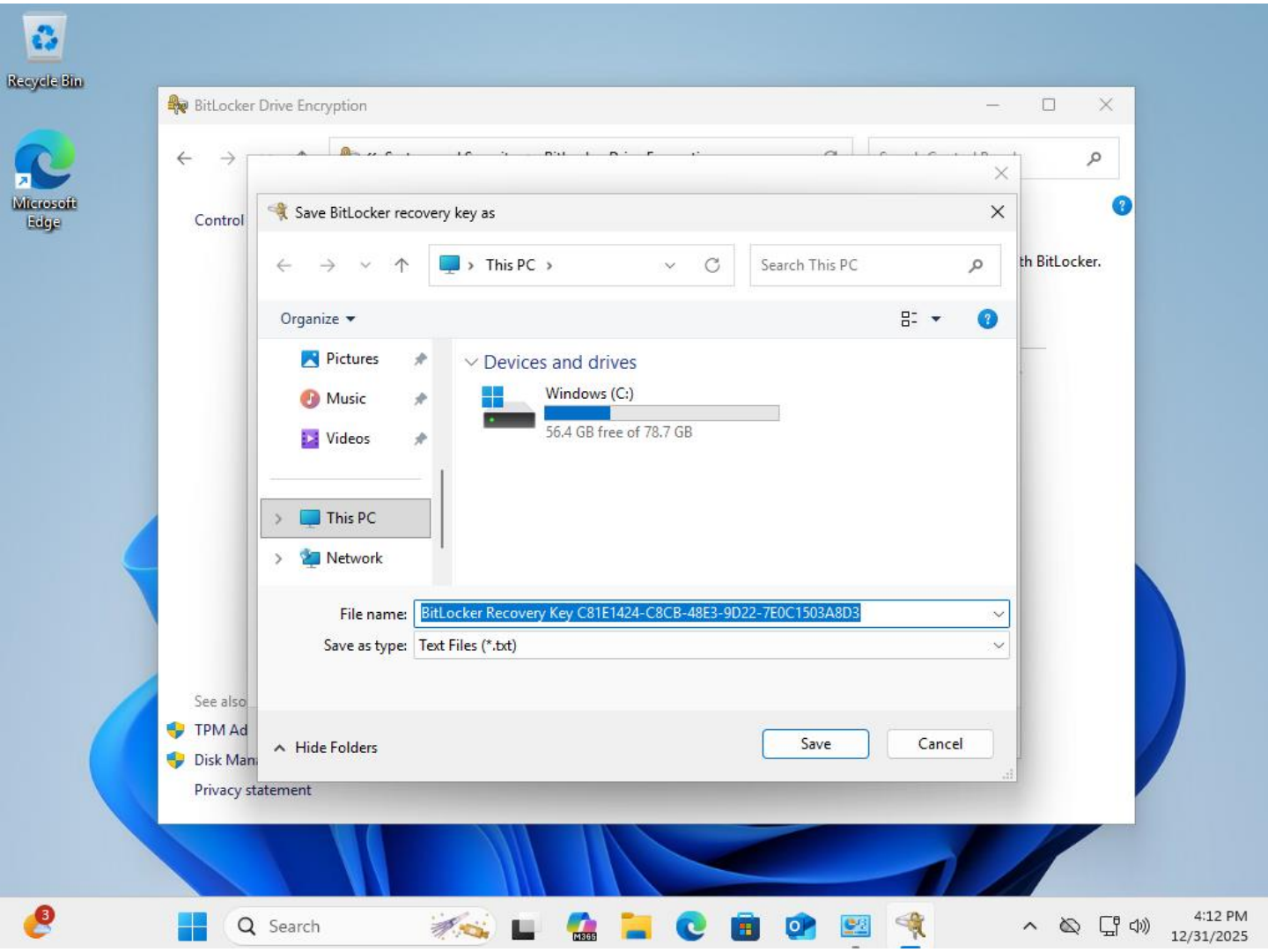
4. Data Retention and Disposal Policy
Data should be retained only for the period required by business needs and regulations. When no longer needed, data must be securely deleted or destroyed to prevent unauthorized recovery.

5. Monitoring and Audit Policy
System and user activities must be logged and monitored to detect suspicious behavior. Audit logs should be protected and reviewed regularly to support compliance and incident investigations.

6. Data Breach Notification Policy
Any suspected or confirmed data breach must be reported immediately to the security team. Appropriate actions and notifications must be completed within required legal timeframes to reduce impact.

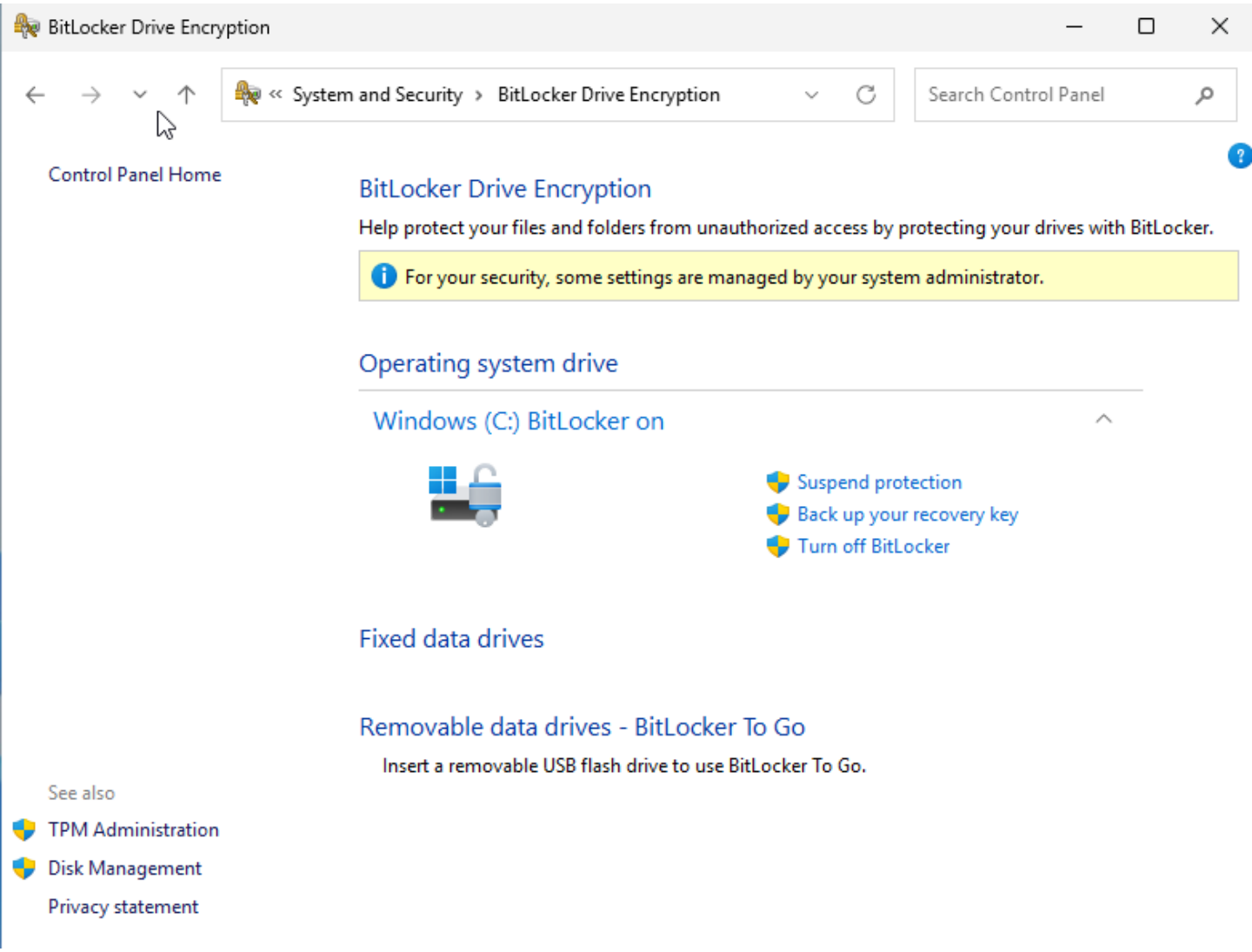
Section 2:
Data Confidentiality

Securing Disks



This screenshot shows the BitLocker recovery key generation process. The recovery key is created to allow access to the encrypted disk in case authentication fails or system recovery is required, ensuring secure key management for encrypted data.

Securing Disks

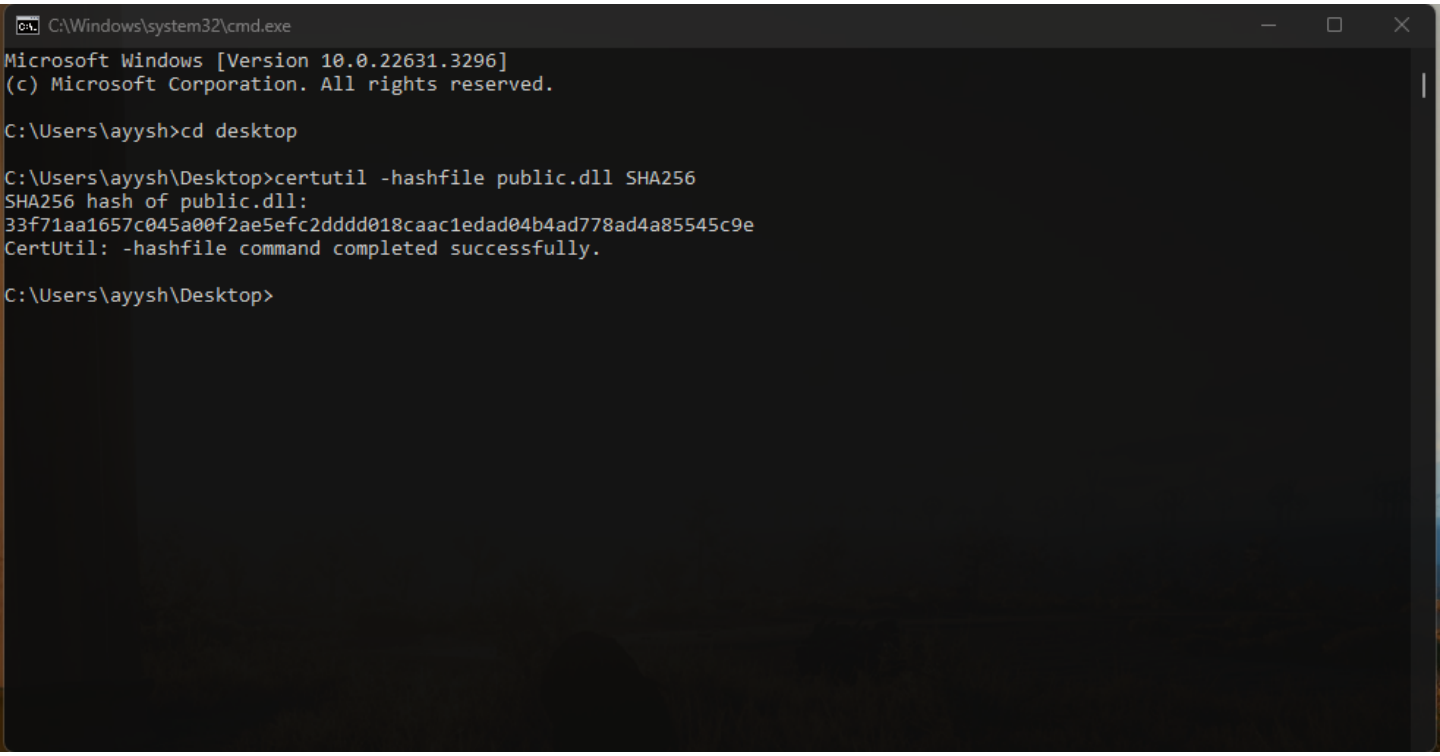


This screenshot shows the BitLocker configuration page after encryption has been successfully enabled on the virtual machine. The operating system drive (C:) is protected, confirming that disk-level encryption has been applied to secure data stored on the virtual disk.

Section 3:
Data Integrity

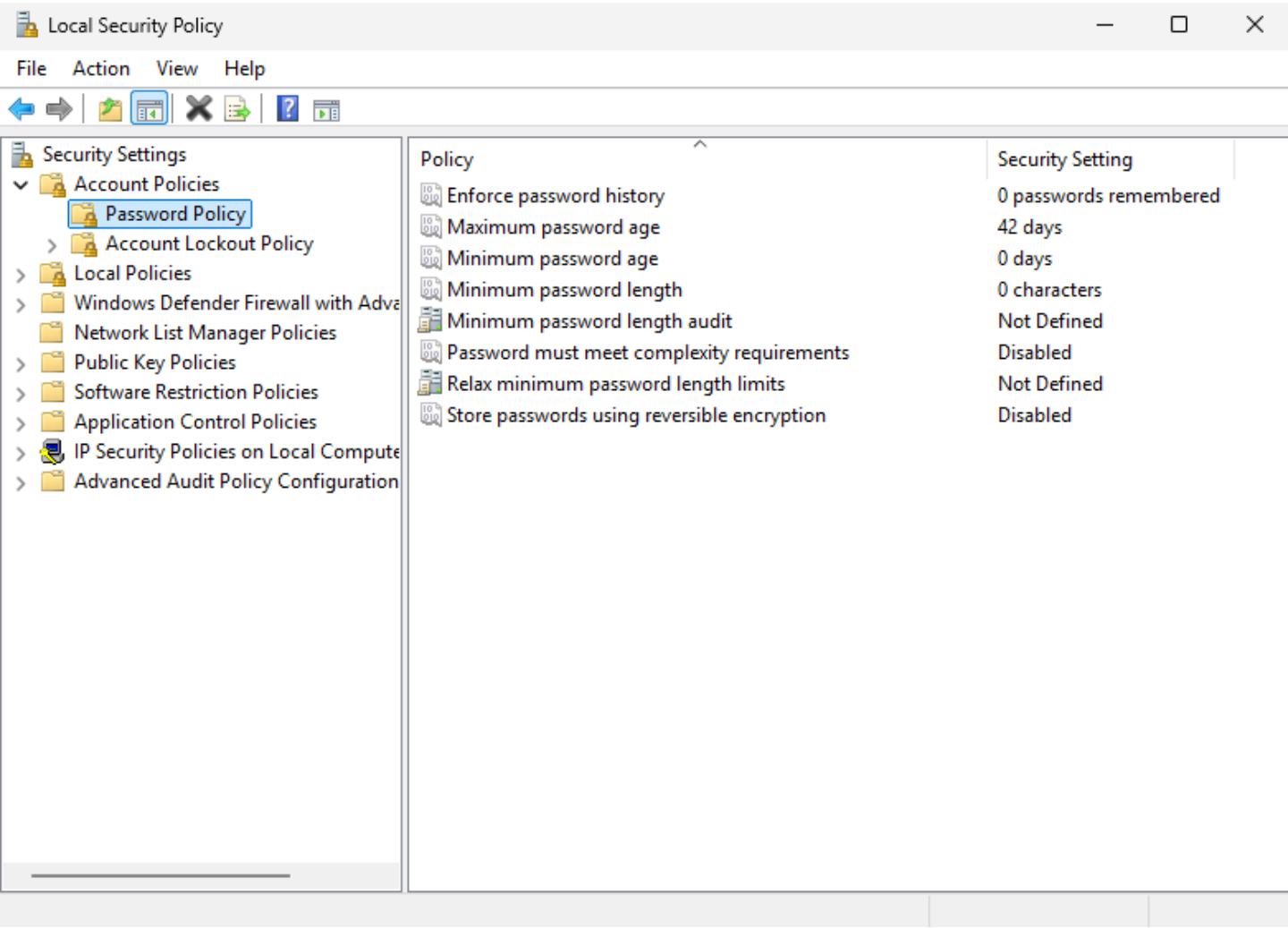
File Integrity Verification

Version 14.0.0.130
The original public.dll hash: f7761cd21b7461fd126ecbac1fa7e516138349fb



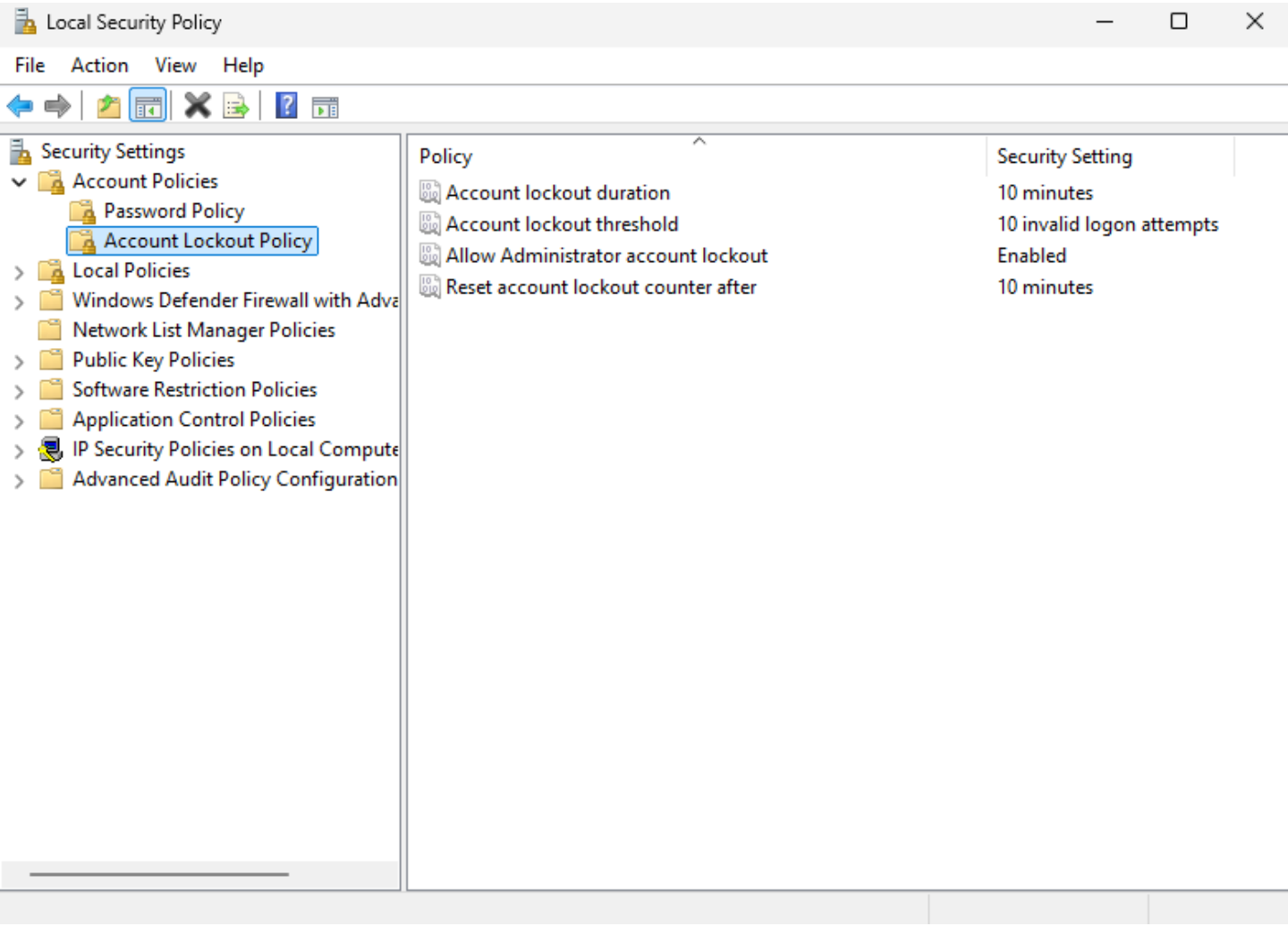
The generated SHA256 hash of the downloaded *public.dll* file is **33f71aa1657c045a00f2ae5efc2dddd018caac1edad04b4ad778ad4a85545c9e**. This value does not match the original hash provided, which indicates that the file is not identical to the reference version. The difference suggests that the file may be a different version or has been modified. Since cryptographic hash values change even with the smallest alteration, this mismatch confirms that the file integrity cannot be verified against the original hash.

Auditing Security Settings



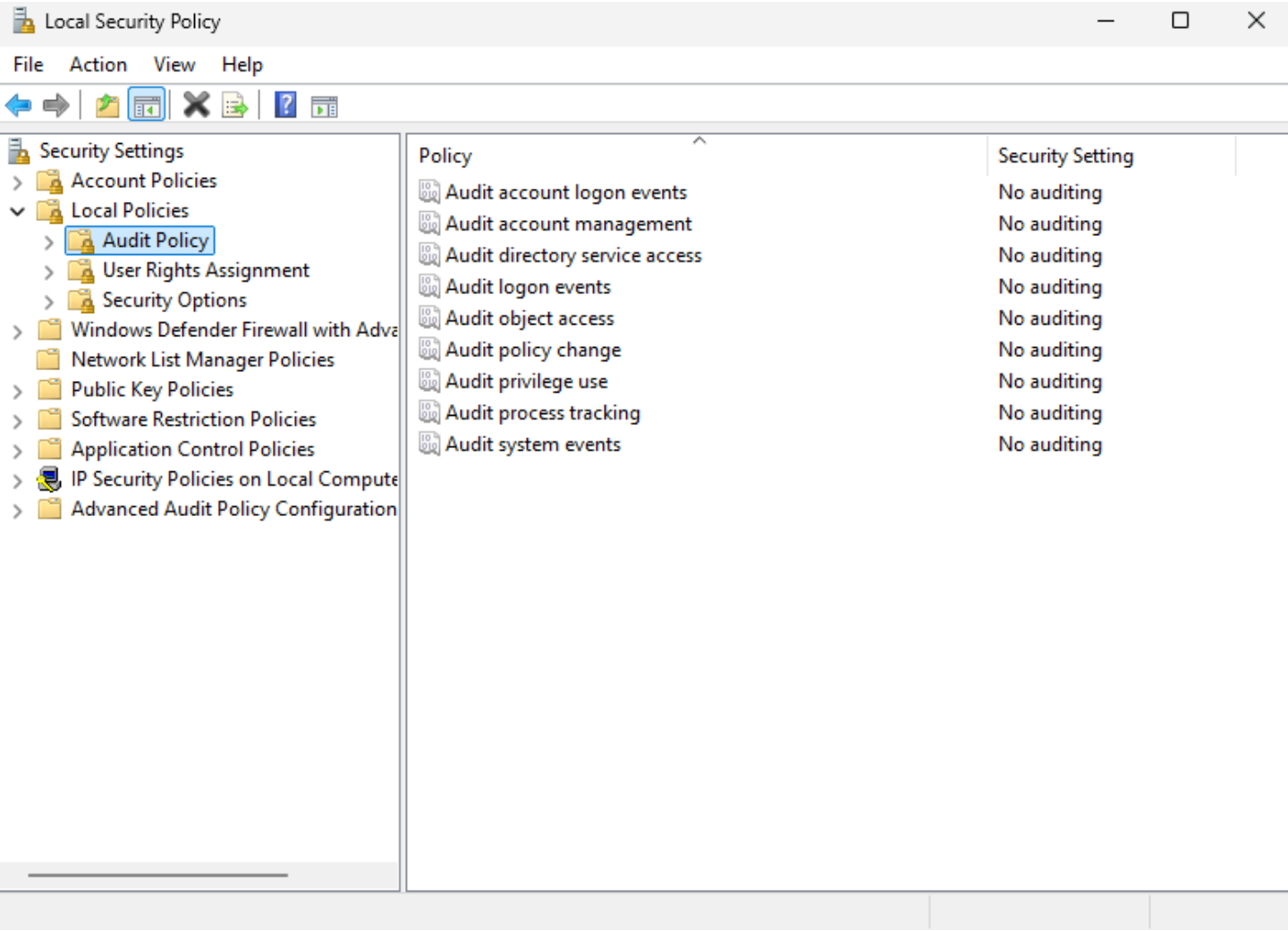
Screenshot showing password complexity, length, and expiration settings.

Auditing Security Settings



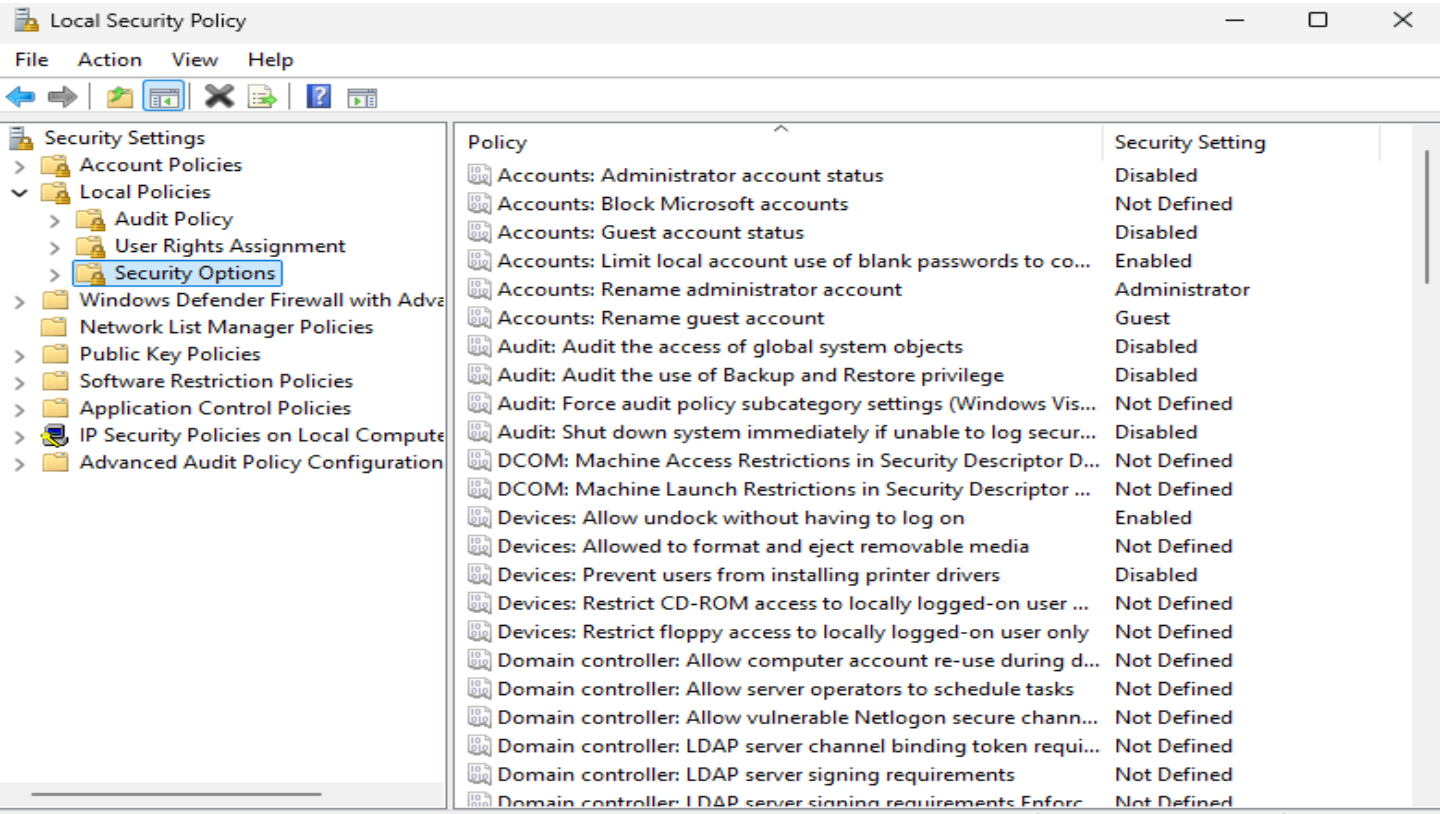
Screenshot showing account lockout configuration to protect against brute-force attacks.

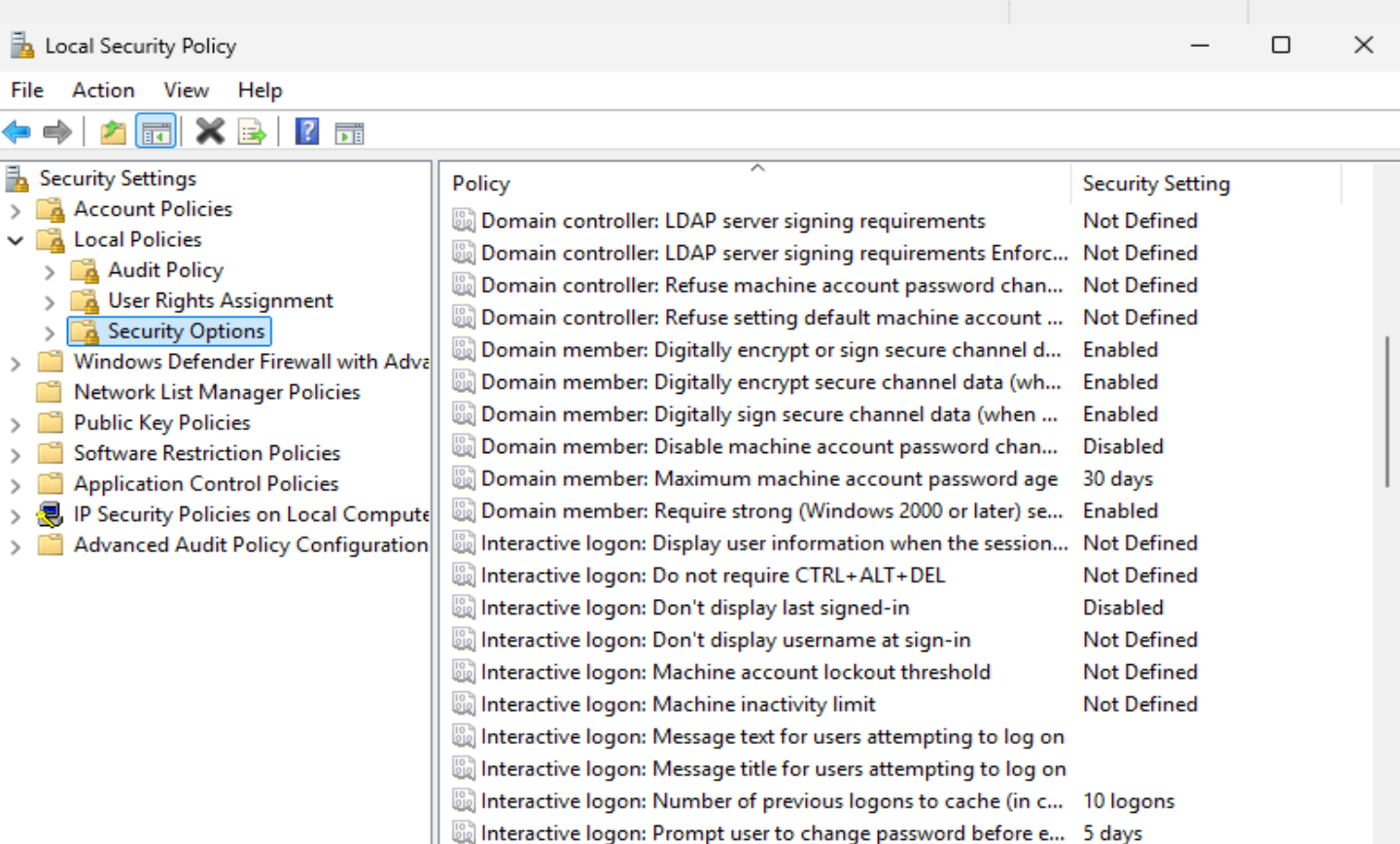
Auditing Security Settings



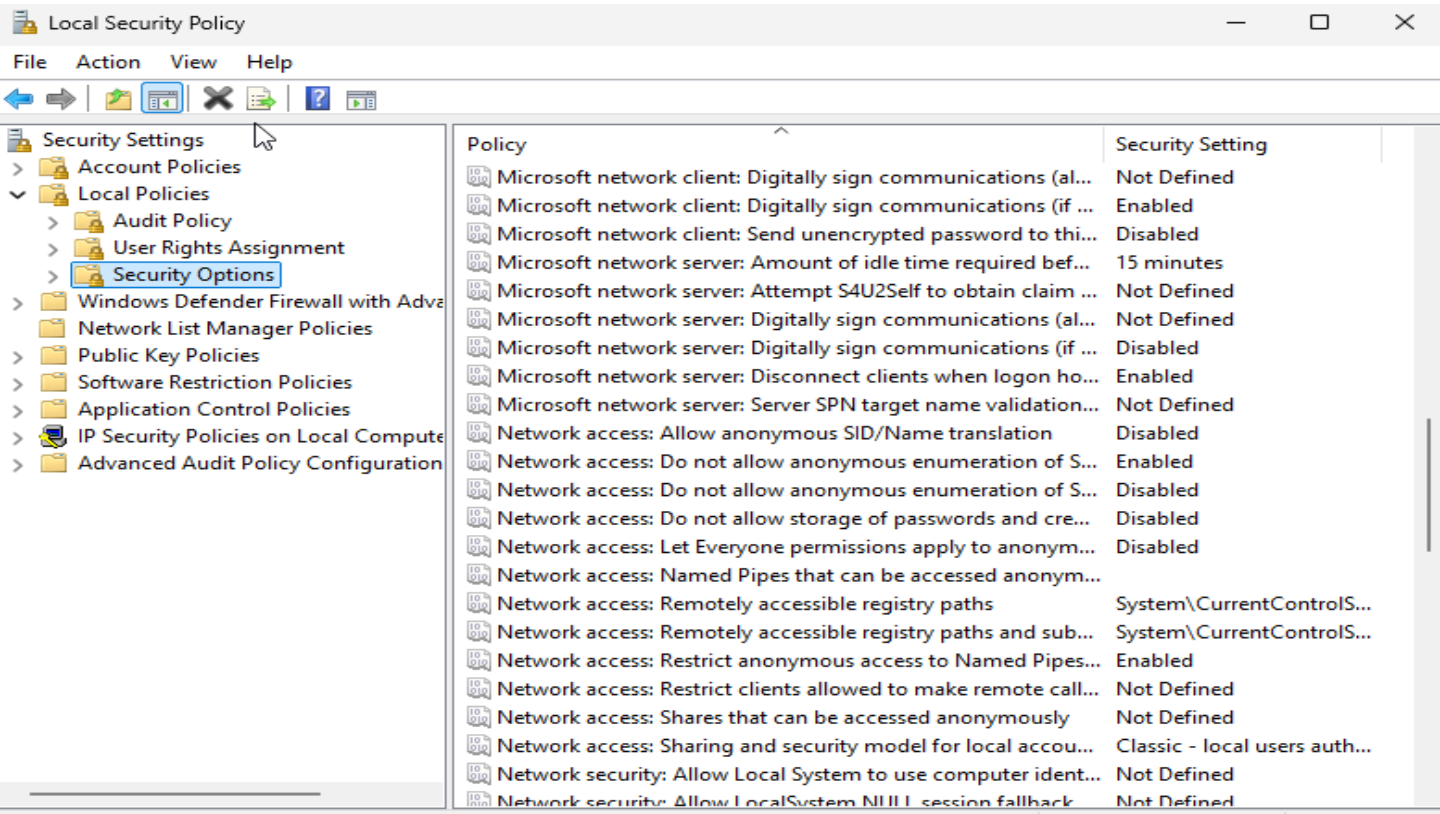
Screenshot showing audit settings used to log and monitor security events.

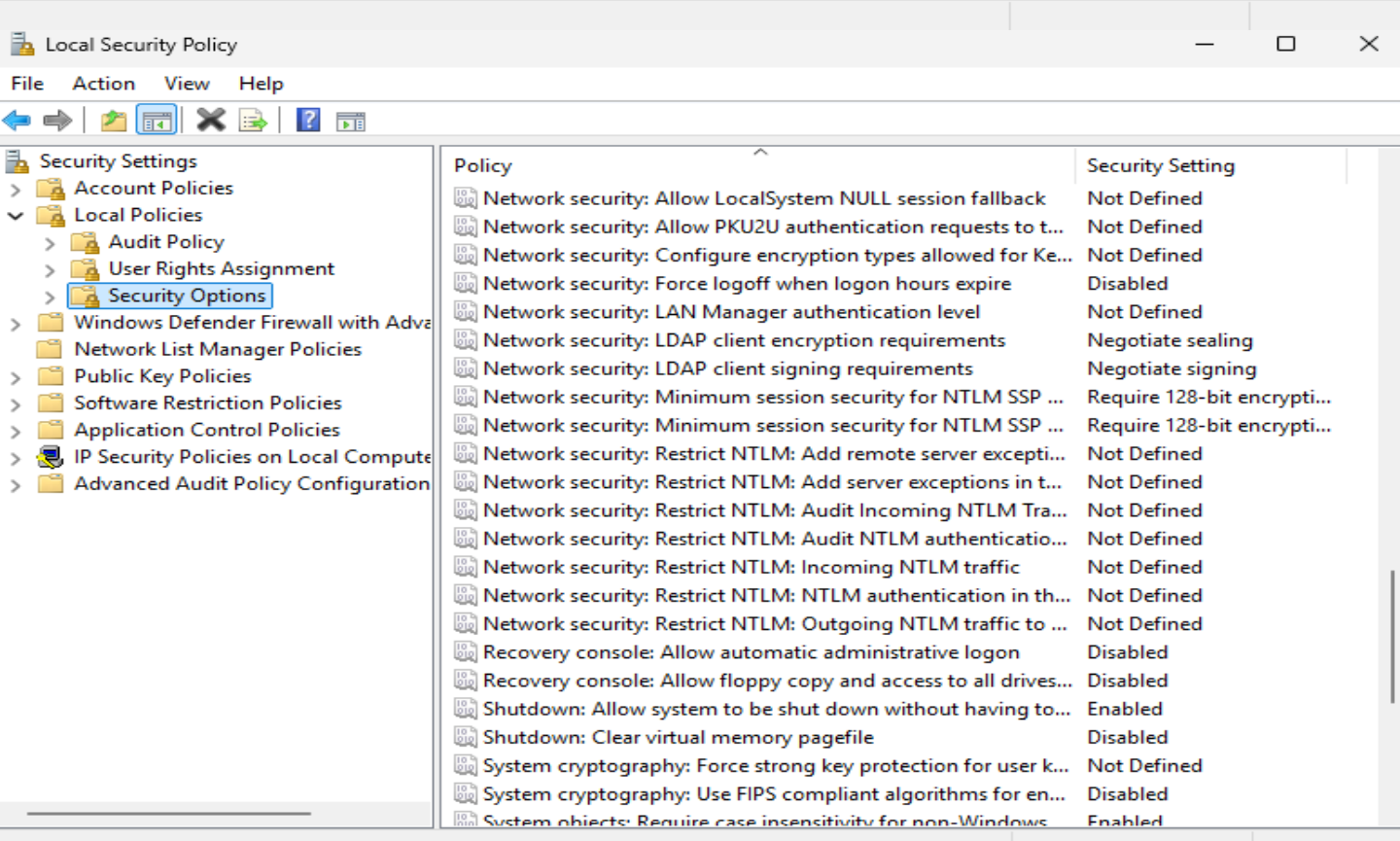
Auditing Security Settings



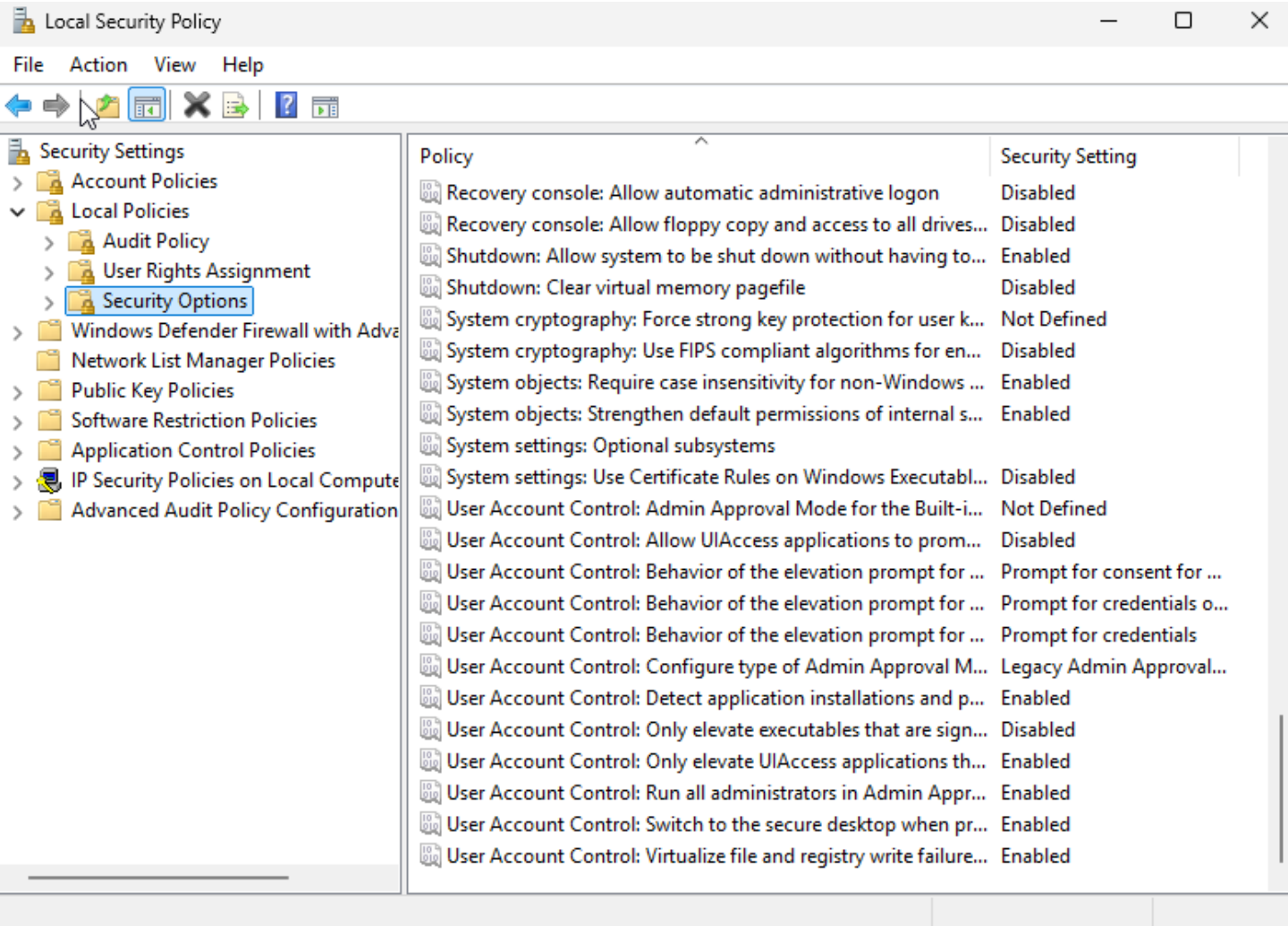


Auditing Security Settings





Auditing Security Settings



Screenshot showing system-wide security configuration options for access control and protection.

Enhancing VM Security

1. Enforce Strong Password Complexity and Length

The current password policy does not enforce complexity or a minimum length, which increases the risk of weak passwords. Enabling password complexity requirements and setting a minimum length (such as 10–12 characters) helps protect against brute-force and password-guessing attacks, improving overall account security.

2. Strengthen Account Lockout Policy Settings

Although account lockout is enabled, adjusting stricter thresholds (such as fewer allowed failed attempts and longer lockout duration) can further reduce the risk of brute-force login attacks. This helps prevent unauthorized access attempts and improves system resilience against credential abuse.

3. Enable Audit Policies for Security and Logon Events

Audit policies are currently set to “No auditing,” which limits visibility into system activity. Enabling auditing for logon events, account management, and policy changes allows administrators to detect suspicious behavior, investigate incidents, and meet compliance and monitoring requirements.

4. Harden Security Options and Account Settings

Several security options, such as restricting blank passwords, controlling administrator account usage, and limiting device access, should be reviewed and enforced. Strengthening these settings reduces privilege misuse, prevents unauthorized access, and aligns the system with industry security best practices.

Section 4:
Data Availability

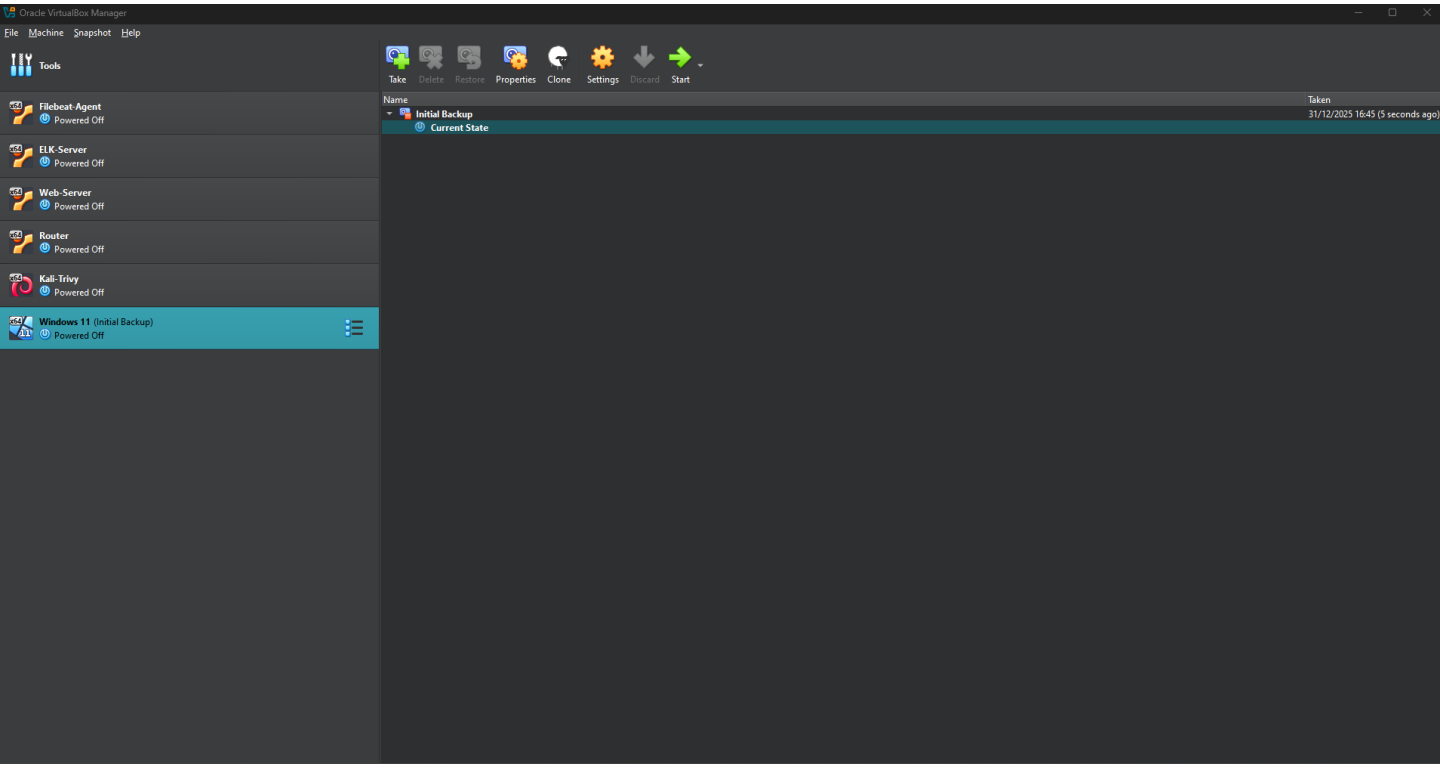
Developing a Data Backup Strategy

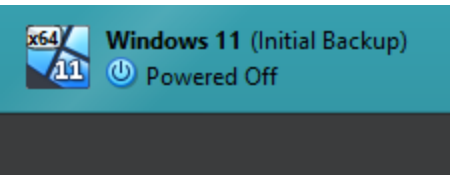
Confidential Data	
Backup Frequency:	**Daily (with continuous or near real-time backups where possible)**
Retention Period:	**1 Year**
Confidential data includes sensitive customer and employee information that is critical to business operations and regulatory compliance. Daily backups ensure minimal data loss in case of system failure, cyberattacks, or accidental deletion. A retention period of one year supports regulatory requirements, auditing needs, and incident investigations while balancing storage costs and data management best practices.	
Internal Data	
Backup Frequency:	**Weekly**
Retention Period:	**90 Days**
Internal data supports day-to-day operations but is less sensitive than confidential data. Weekly backups provide sufficient protection against accidental loss or corruption while avoiding unnecessary storage overhead. A 90-day retention period allows recovery from recent issues and supports internal review or troubleshooting when needed.	

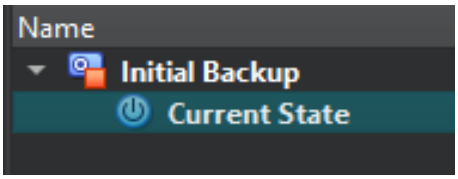
Developing a Data Backup Strategy

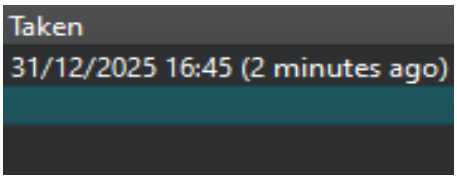
Public Data	
Backup Frequency:	**As needed (or weekly)**
Retention Period:	**30 Days**
Public data is intended for open access and does not contain sensitive information, so it requires less frequent backups. Backups are mainly needed to protect against accidental deletion or system errors. A 30-day retention period is sufficient to restore content if required while keeping storage usage minimal.	

Creating a Backup









Screenshots showing the creation of a virtual machine snapshot used as a backup. This snapshot serves as a restore point that allows the system to be recovered in case of data loss, misconfiguration, or system failure.