

DATA SECURITY ANALYSIS



27/12/2025
Friday

ANSHUL SHUKLA
CBS-0417

Project Scenario

Project Information Slide

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.

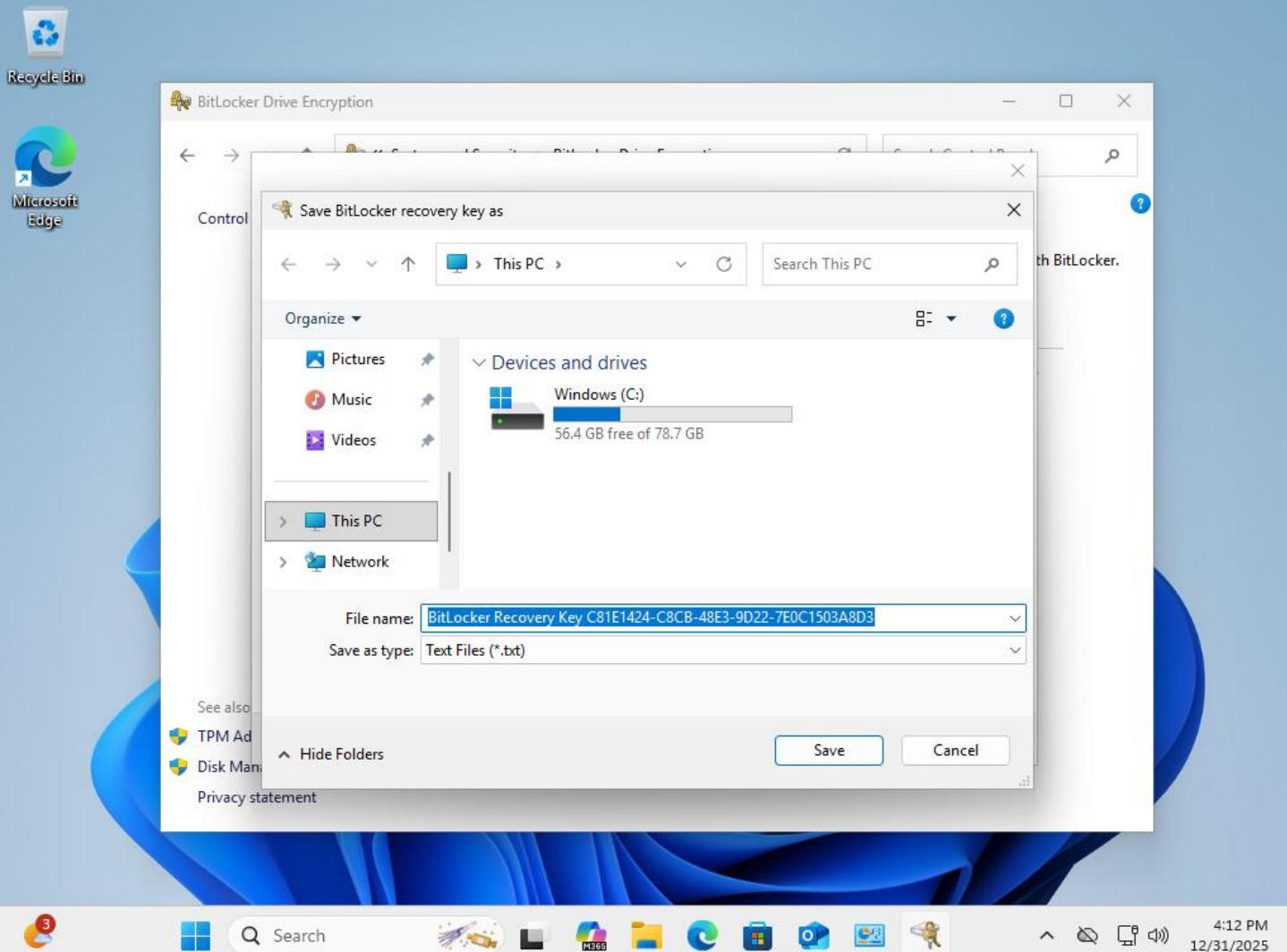
6. Data Breach Notification Policy

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

The screenshot shows the Windows Control Panel interface for BitLocker Drive Encryption. The title bar reads "BitLocker Drive Encryption". The left sidebar has a "Control Panel Home" link. The main content area is titled "BitLocker Drive Encryption" with a sub-section "Operating system drive" under "Windows (C:) BitLocker on". It shows a lock icon and three actions: "Suspend protection", "Back up your recovery key", and "Turn off BitLocker". Below this is a section for "Fixed data drives" and "Removable data drives - BitLocker To Go", both with a note to insert a USB drive. A "See also" sidebar on the left lists "TPM Administration", "Disk Management", and "Privacy statement".

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

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ayysh>cd desktop

C:\Users\ayysh\Desktop>certutil -hashfile public.dll SHA256
SHA256 hash of public.dll:
33f71aa1657c045a00f2ae5efc2ddd018caac1edad04b4ad778ad4a85545c9e
CertUtil: -hashfile command completed successfully.

C:\Users\ayysh\Desktop>
```

The generated SHA256 hash of the downloaded *public.dll* file is **33f71aa1657c045a00f2ae5efc2ddd018caac1edad04b4ad778ad4a85545c9e**. 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

The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security settings, with the 'Password Policy' node selected under 'Account Policies'. The right pane lists various policy settings with their current values.

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Screenshot showing password complexity, length, and expiration settings.

Auditing Security Settings

The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security settings, with 'Account Policies' expanded and 'Account Lockout Policy' selected. The right pane lists four policy settings under 'Policy': 'Account lockout duration' (Security Setting: 10 minutes), 'Account lockout threshold' (Security Setting: 10 invalid logon attempts), 'Allow Administrator account lockout' (Security Setting: Enabled), and 'Reset account lockout counter after' (Security Setting: 10 minutes).

Policy	Security Setting
Account lockout duration	10 minutes
Account lockout threshold	10 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

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

Auditing Security Settings

The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security settings, with 'Audit Policy' selected under 'Local Policies'. The right pane lists audit policies and their current status:

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

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

Auditing Security Settings

Local Security Policy

File Action View Help

Security Settings

- > Account Policies
- > Local Policies
 - > Audit Policy
 - > User Rights Assignment
 - > Security Options**
- > Windows Defender Firewall with Adv...
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Compute...
- > Advanced Audit Policy Configuration

Policy	Security Setting
Accounts: Administrator account status	Disabled
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	Administrator
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	Disabled
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 computer account re-use during d...	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: LDAP server signing requirements Enforc...	Not Defined

Local Security Policy

File Action View Help

Security Settings

- > Account Policies
- > Local Policies
 - > Audit Policy
 - > User Rights Assignment
 - > Security Options**
- > Windows Defender Firewall with Adv...
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Compute...
- > Advanced Audit Policy Configuration

Policy	Security Setting
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: LDAP server signing requirements Enforc...	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain controller: Refuse setting default machine account ...	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	Not Defined
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
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days

Auditing Security Settings

Local Security Policy

File Action View Help

Security Settings

- Account Policies
- Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options**
- Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Microsoft network client: Digitally sign communications (always)	Not Defined
Microsoft network client: Digitally sign communications (if possible)	Enabled
Microsoft network client: Send unencrypted password to this computer	Disabled
Microsoft network server: Amount of idle time required before disconnecting a client	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim	Not Defined
Microsoft network server: Digitally sign communications (always)	Not Defined
Microsoft network server: Digitally sign communications (if possible)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of shares	Enabled
Network access: Do not allow anonymous enumeration of users	Disabled
Network access: Do not allow storage of passwords and credentials	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	System\CurrentControlSet\Control\Network\NamedPipes\AllowAnonymousAccess
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\Network\RemotelyAccessiblePaths
Network access: Remotely accessible registry paths and subkeys	System\CurrentControlSet\Control\Network\RemotelyAccessibleSubkeys
Network access: Restrict anonymous access to Named Pipes	Enabled
Network access: Restrict clients allowed to make remote calls	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate on the server
Network security: Allow Local System to use computer identifier	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined

Local Security Policy

File Action View Help

Security Settings

- Account Policies
- Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options**
- Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to the computer	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client encryption requirements	Negotiate sealing
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP	Require 128-bit encryption
Network security: Minimum session security for NTLM SSP	Require 128-bit encryption
Network security: Restrict NTLM: Add remote server exceptions in the list	Not Defined
Network security: Restrict NTLM: Add server exceptions in the list	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication requests	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in the list	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to the list	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives	Disabled
Shutdown: Allow system to be shut down without having to log off	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption	Disabled
System objects: Require case insensitivity for non-Windows objects	Enabled

Auditing Security Settings

The screenshot shows the 'Local Security Policy' snap-in window. The title bar reads 'Local Security Policy'. The menu bar includes 'File', 'Action', 'View', and 'Help'. Below the menu is a toolbar with icons for back, forward, search, and other actions. The left pane is a tree view of policy settings:

- Security Settings
 - Account Policies
 - Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options** (selected)
 - Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - Public Key Policies
 - Software Restriction Policies
 - Application Control Policies
 - IP Security Policies on Local Computer
 - Advanced Audit Policy Configuration

The right pane displays a list of security policies with their current settings:

Policy	Security Setting
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executabl...	Disabled
User Account Control: Admin Approval Mode for the Built-i...	Not Defined
User Account Control: Allow UIAccess applications to prom...	Disabled
User Account Control: Behavior of the elevation prompt for ...	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials o...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials
User Account Control: Configure type of Admin Approval M...	Legacy Admin Approval...
User Account Control: Detect application installations and p...	Enabled
User Account Control: Only elevate executables that are sign...	Disabled
User Account Control: Only elevate UIAccess applications th...	Enabled
User Account Control: Run all administrators in Admin Appr...	Enabled
User Account Control: Switch to the secure desktop when pr...	Enabled
User Account Control: Virtualize file and registry write failure...	Enabled

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

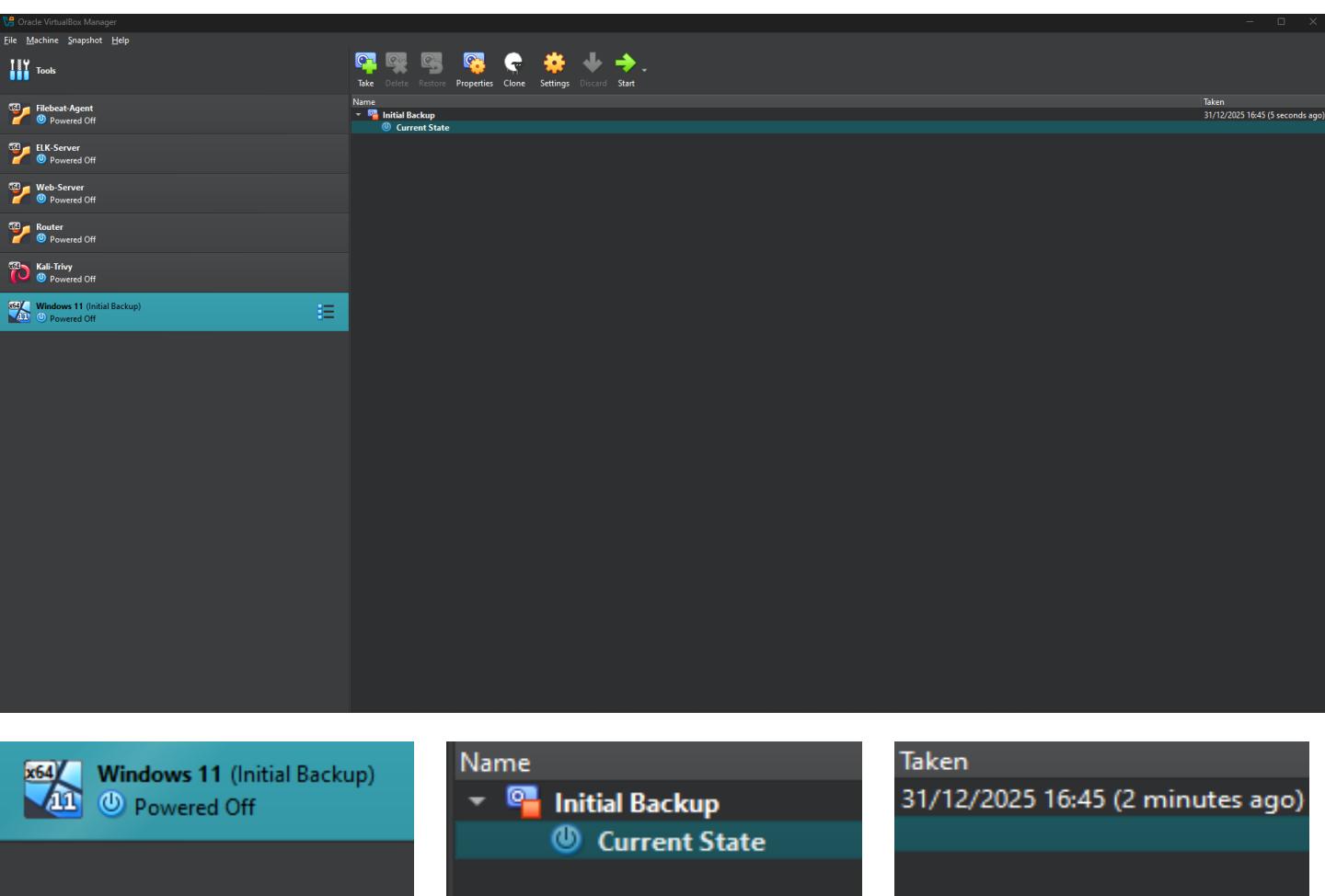
Public Data

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.