Section 1: Data Security Program Policy

1.1 Overview

Maintaining data security is critical to the survival of JFin Payments. This policy requires management to financially support and diligently attend to data security efforts.

1.2 Purpose

This policy defines the requirement for a baseline data security program to be developed and implemented by JFin Payments that will describe the process to secure data within IT Systems, Applications and any other mediums from cyber threats.

1.3 Scope

This policy is directed to the IT Management Staff who is accountable to ensure the data security program is developed, implemented and kept up-to-date. This policy is solely to state the requirement to have a data security program, it does not provide requirement around what goes into the plan or sub-plans.

1.4 Policy

4.1.1 Data Security Plan

The following data security elements must be created:

- IT Staff should perform a data classification annually, or when there are notable business or technology changes.
    - This will ensure sensitive data is identified, prioritized, and protected according to its importance and risk level. This helps mitigate security threats and ensures compliance with regulations and industry standards.
- IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.
    - This ensures that IT staff can identify and prioritize applications and systems based on their criticality to the organization. This enables focused security efforts on protecting critical assets, reducing vulnerabilities, and maintaining business continuity.
- IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.
    - This ensures that JFin Payments remains compliant with relevant regulations and standards. This helps mitigate legal and financial risks associated with non-compliance, preserves the organization's reputation, and maintains customer trust

1.4.2 Data Security Requirements Matrix

This matrix is meant to cover some of the most critical areas of protection and answer questions frequently asked by IT Staff like What should be encrypted and what kind of encryption should be used? If someone tries to access a confidential area of the network, after how many failed login attempts should they be denied access? *This is a minor example section and is not meant to cover every single element of data security.*

Data Type	Data Examples	Application Names	Regulations That Apply	Data Encryption Requirement	Recommended Data Storage Zone (High, Mid, Low, or DMZ)	Access Security (After how many login attempts should someone get locked out? For how long?)
Confidential	employee profile data (name, address, phone number, and social security number)	JFinEmpServices App	GDPR PCIDSS\ Federal Privacy Act of 1974 Gramm-Leach-Bliley Act (GLBA) California Consumer Privacy Act (CCPA)	Encryption Algorithm: RSA 2048 Data at rest: Disk, File, Database level encryption Data in transit: TLS, HTTPS, IPSec, SSH, WPA2	High	3 login attempts 10 minutes lockout
	customer profile data (name, email address, and bank and credit card account numbers, company email)	JFinCustomerServices App			DMZ	3 login attempts 30 minutes lockout
Internal	newsletters sent to internal employees	JFinIntNewsletter App	California Consumer Privacy Act (CCPA) GDPR	AES 128 Data at rest: Disk, File, Database level encryption Data in transit: TLS, HTTPS, IPSec, SSH, WPA2	Mid	3 login attempts 5 minutes lockout
Public	blogs previously published on the website	JFinBlogs.com	Copyrights law Digital Millennium Copyright Act (DMCA) e-Commerce Directive	Data in transit: TLS, HTTPS, SSH	Low	

Justification:

- Data Type 1: The data type classified as confidential includes the employee profile data and customer profile data because if there is data loss, this would have a catastrophic impact on the business.

  Regulations that apply: GDPR, Federal Privacy Act of 1974, California Consumer Privacy Act (CCPA) all apply to this data type because JFin Payments have customers in the United Stated and Europe, and they are headquartered at California. JFin is also a payment processing company, hence PCIDSS and the GLBA applies.

  Encryption Requirement: Given the sensitivity of employee and customer profile data, strong encryption (RSA 2048) is necessary to protect against unauthorized access or data breaches.

  Data Storage Zone: High and DMZ security is recommended to ensure that only authorized personnel can access and modify the data.

  Access Security: Implementing a lockout mechanism after 3 login attempts enhances security by preventing brute-force attacks. A 10-minute lockout for employee profile data and a 30-minute lockout for customer profile data.

- Data Type 2: The data type classified as internal includes newsletters sent to internal employees because if this becomes public, there might be impact but it won't be catastrophic to the business.

  The newsletters will be subject to CCPA, GDPR, HIPAA etc. if it contains PII and PHI of employees. AES-128 encryption is recommended because it's less expensive to implement compared to RSA-2048 and it provides strong security while maintaining reasonable performance. The data storage is mid and an access security of 3 login attempts and 5 minute lockout is recommended as the data is internal.

- Data Type 3: The blogs published on the website is classified as public. Blogs published on website are subject to copyright laws e.g. DMCA, subject to GDPR regarding obtaining consent for cookies, subject to EU e-Commerce Directive etc. No encryption is needed as the data is already exposed to the public. The data storage is low as the data is public and no access security policy is needed.

Section 2: Disaster Recovery Policy

2.1 Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives JFin Payments a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2.2 Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by JFin Payments that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

2.3 Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

2.4 Policy

Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Application List: List all the applications provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, where it is saved, and how often the backup is done. It should also describe how that data could be recovered.
    - Data type 1 which contains employee and customer profile data should be fully backed up daily and retained for 180 days. The retention of the daily backup points should be 30 days. Recovery should be tested monthly to ensure the Disaster Recovery Plan works efficiently

  - Data type 2 which contains internal data should be fully backed up weekly and retained for 90 days. The retention of the daily backup points should be 15 days. Recovery should be tested bi-monthly.
  - Data type 3 which contains public data should be backed up incrementally monthly and retained for 45 days. The retention of the weekly backup points should be 2 weeks.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

2.5 Policy Compliance

2.5.0 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2.5.1 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

2.5.2 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.6 Related Standards, Policies and Processes

None.

2.7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Disaster

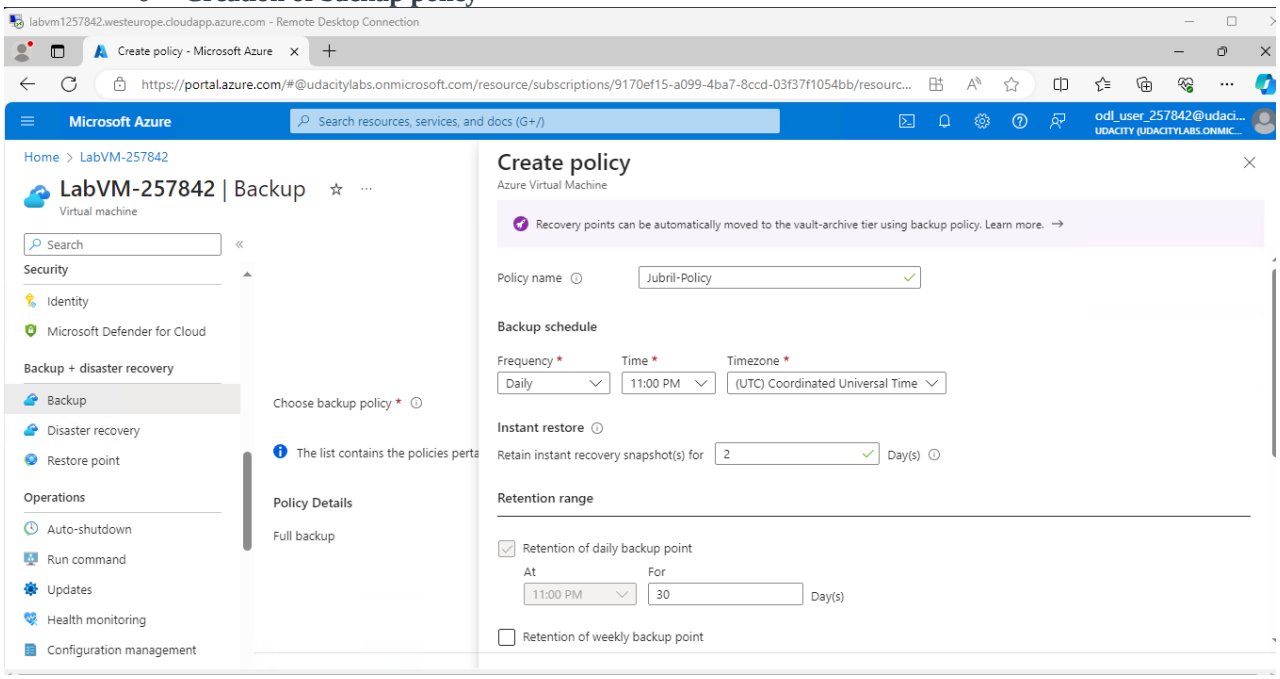
2.8 Revision History

Date of Change	Responsible	Summary of Change
June 2021	IT Management Team	Updated and converted to new format.

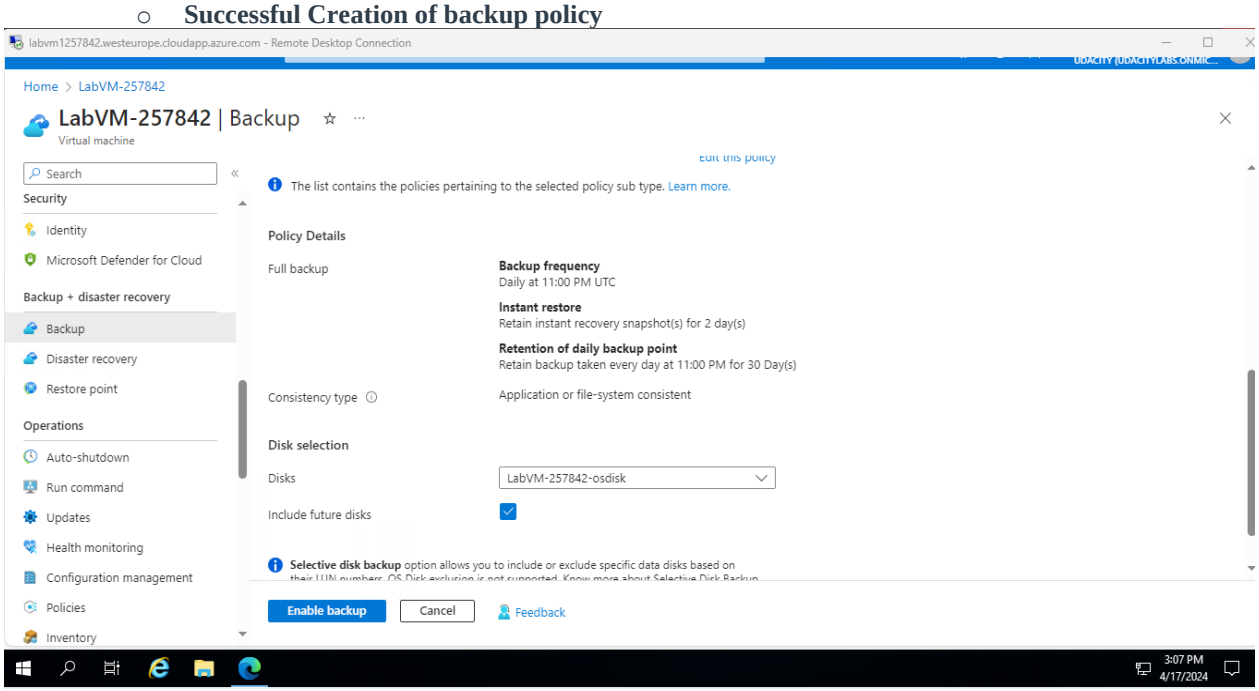
PART 2: IMPLEMENT ENCRYPTION, BACKUP, FILE INTEGRITY MONITORING, ACCESS MANAGEMENT, AND AUDIT

3.1 Here is an example of the backup process for a critical system:

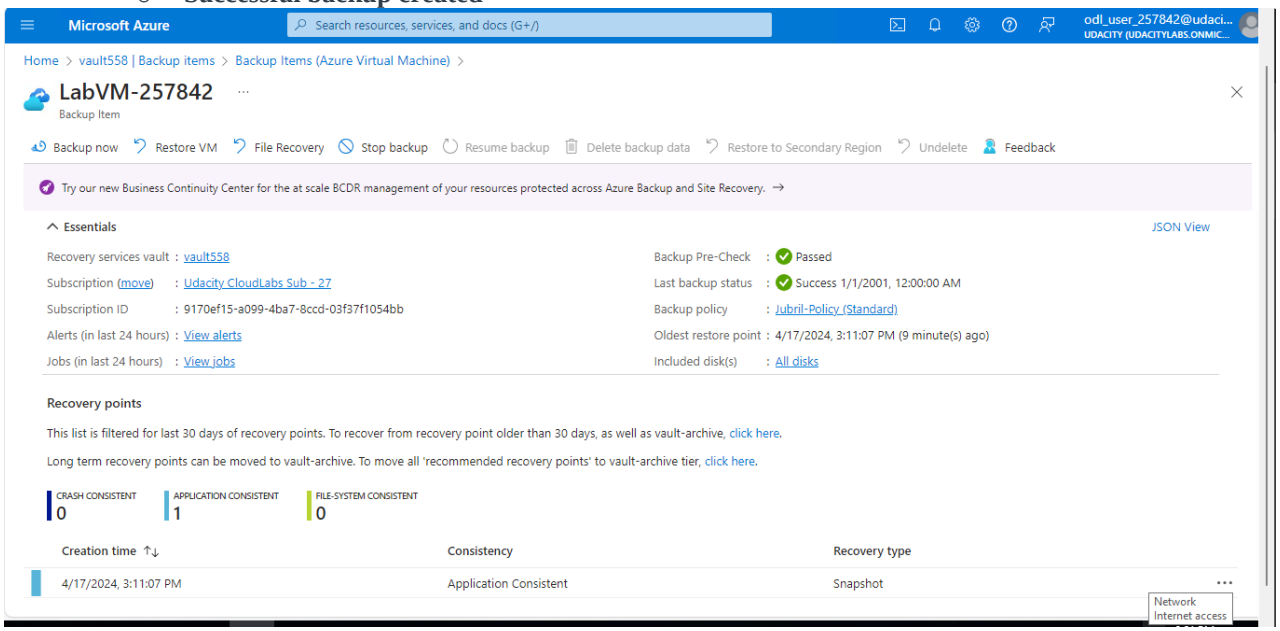
- **Creation of backup policy**



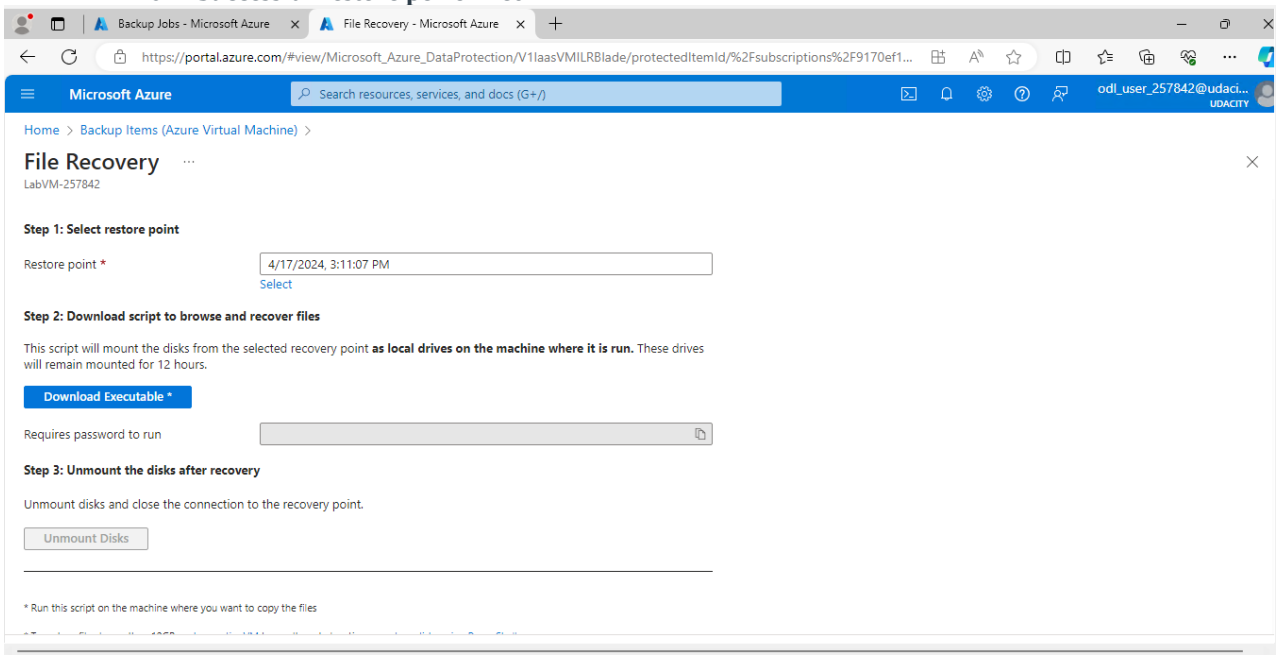
- **Successful Creation of backup policy**

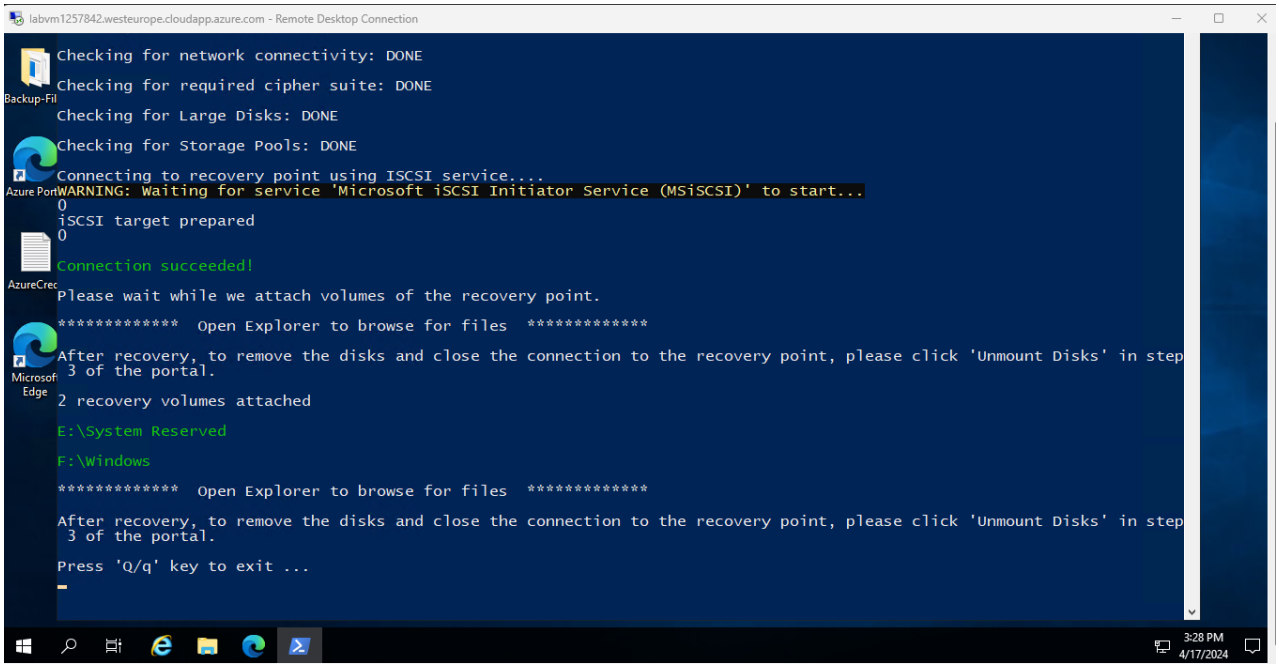


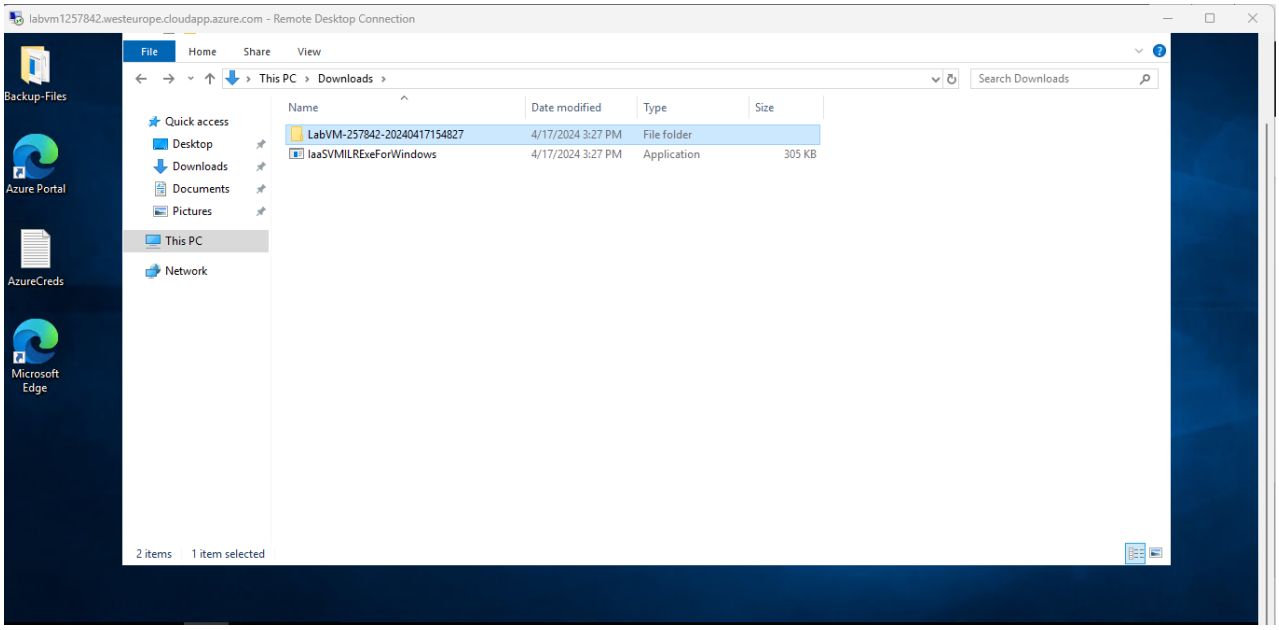
- **Successful backup created**



- **Successful restore performed**

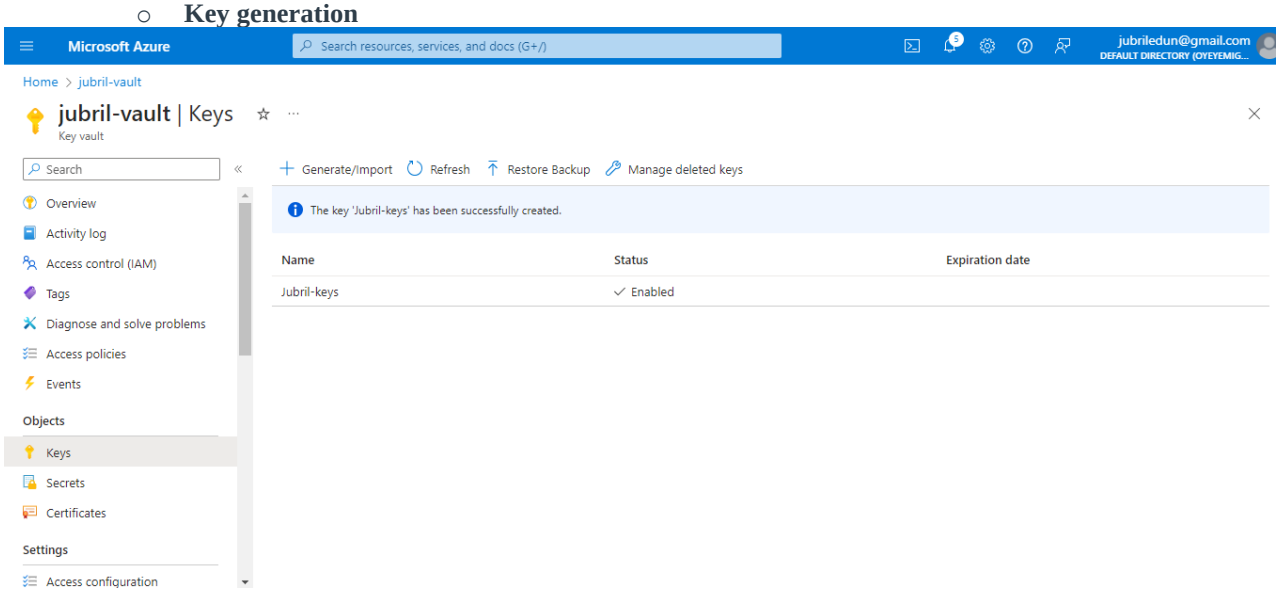




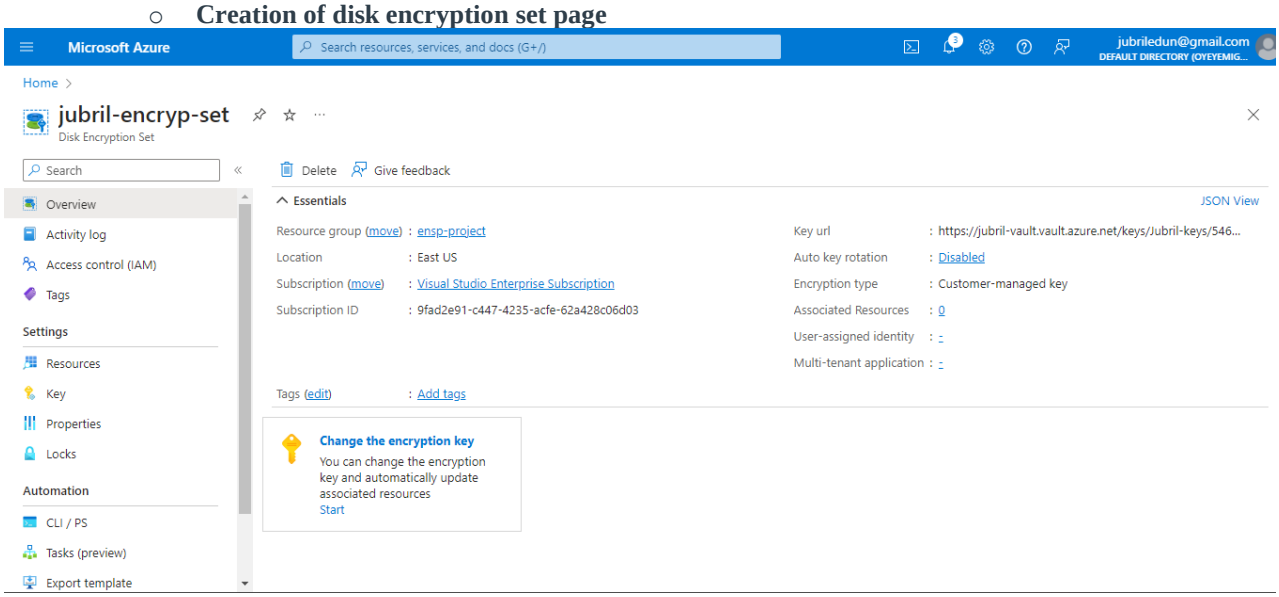


3.2 Here is an example of the encryption process for a critical system:

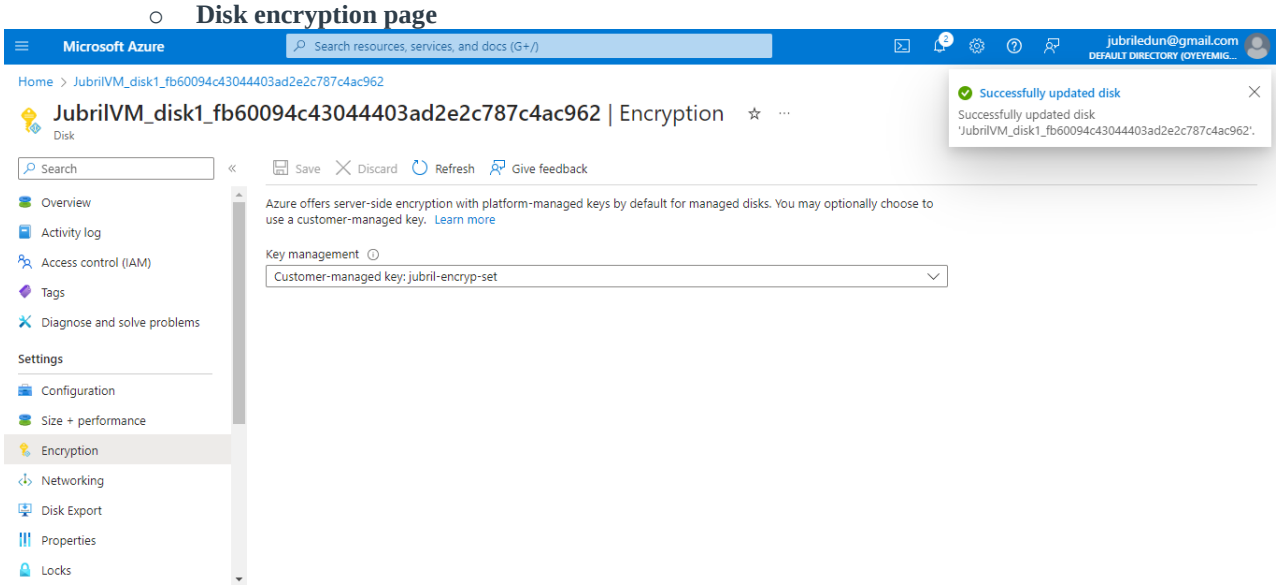
- **Key generation**



- **Creation of disk encryption set page**

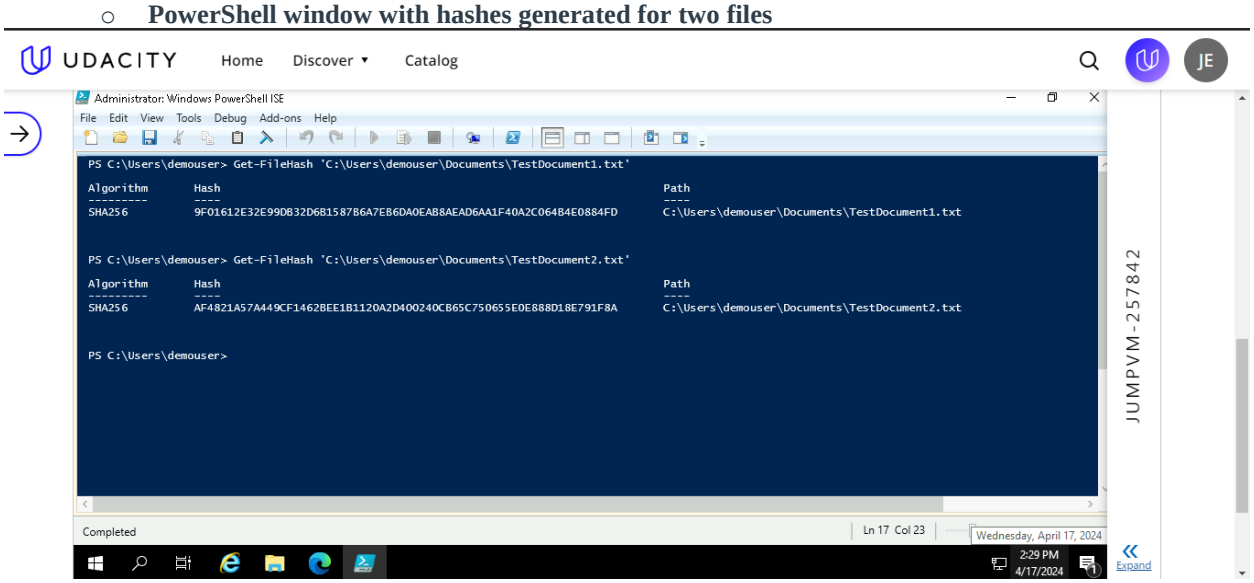


- **Disk encryption page**



3.3 Here is an example of the file integrity monitoring process for a critical system:

- **PowerShell window with hashes generated for two files**

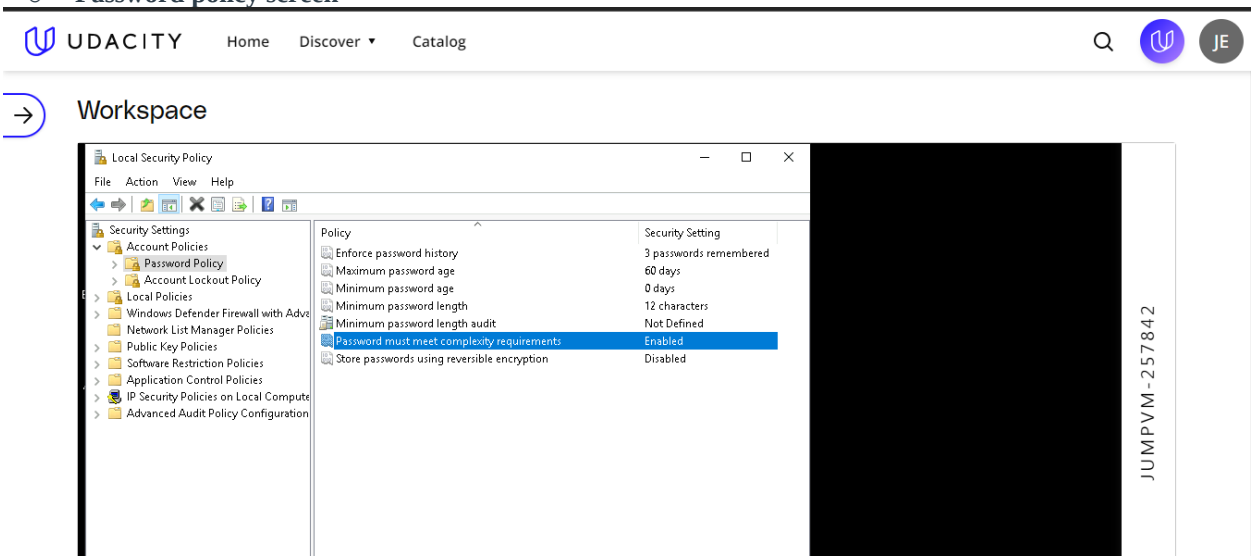


- Recommendations to improve data integrity:

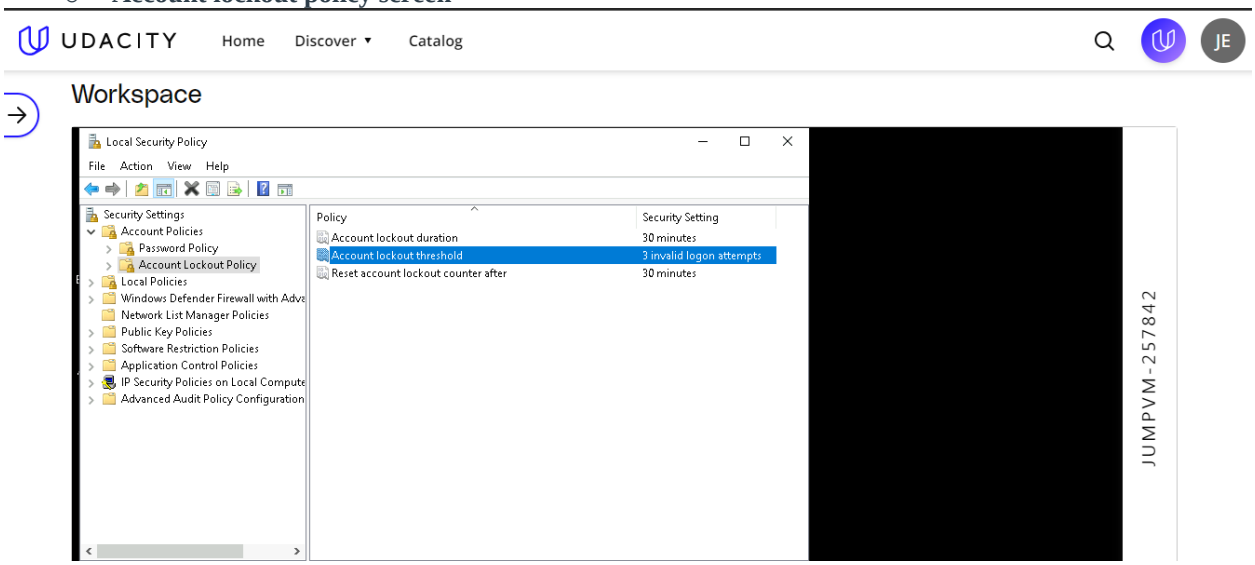
  - Grant read permissions to authorized users or groups who need access to the files for legitimate purposes. This allows them to view the contents of the files without being able to modify them e.g. regular employees
  - If the files are executable or contain scripts that need to be run, grant execute permissions to users or groups who require this functionality e.g. developers, system administrators etc.
  - Deny write permissions to all users except for authorized administrators or designated personnel responsible for file management. This prevents unauthorized modifications or tampering with the files.
  - Deny delete permissions to all users except for administrators or designated personnel responsible for file management. This ensures that the files cannot be accidentally or maliciously deleted.
  - Deny permissions to modify the access control lists (ACLs) of the files to prevent unauthorized changes to the permissions themselves.

3.4 Here is an example of the access review process for a critical system:

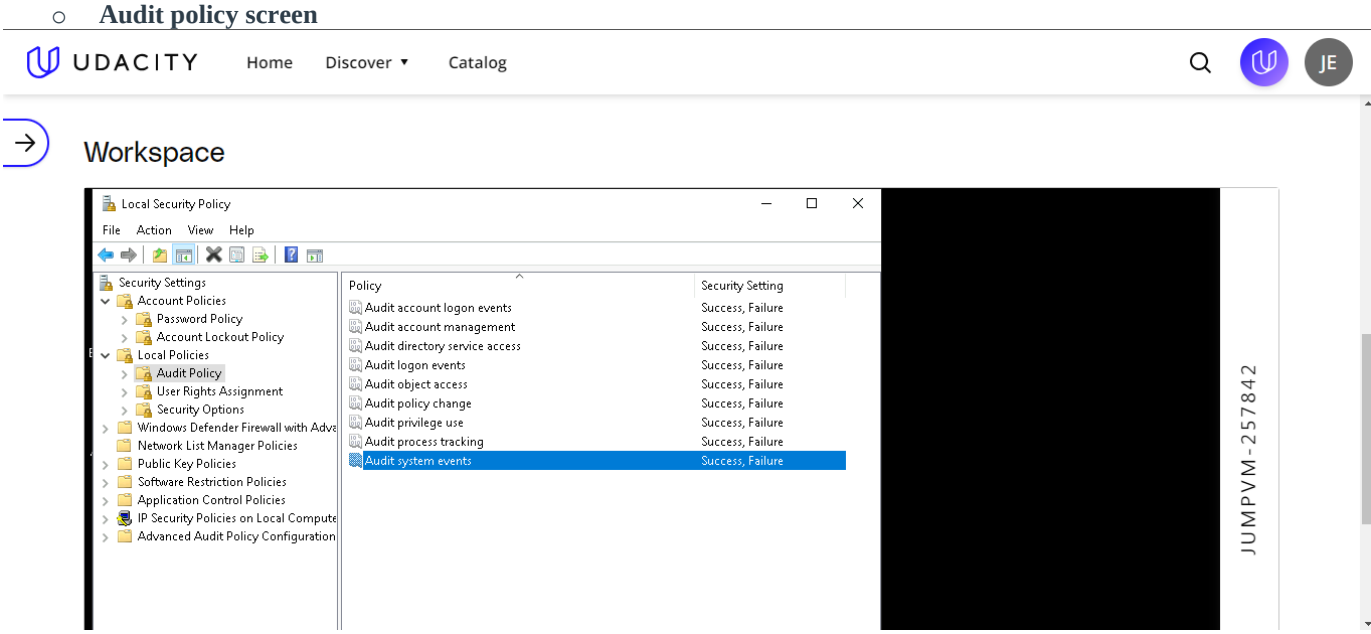
- **Password policy screen**



- **Account lockout policy screen**



- **Audit policy screen**



- **Security options screen**