Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

Time on Task:	Progress:
13 hours, 39 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:41 PM

Guided Exercises

Part 1: Update the Information Security Policy Document

3. **Recommend** and **explain** four properties and any associated values.

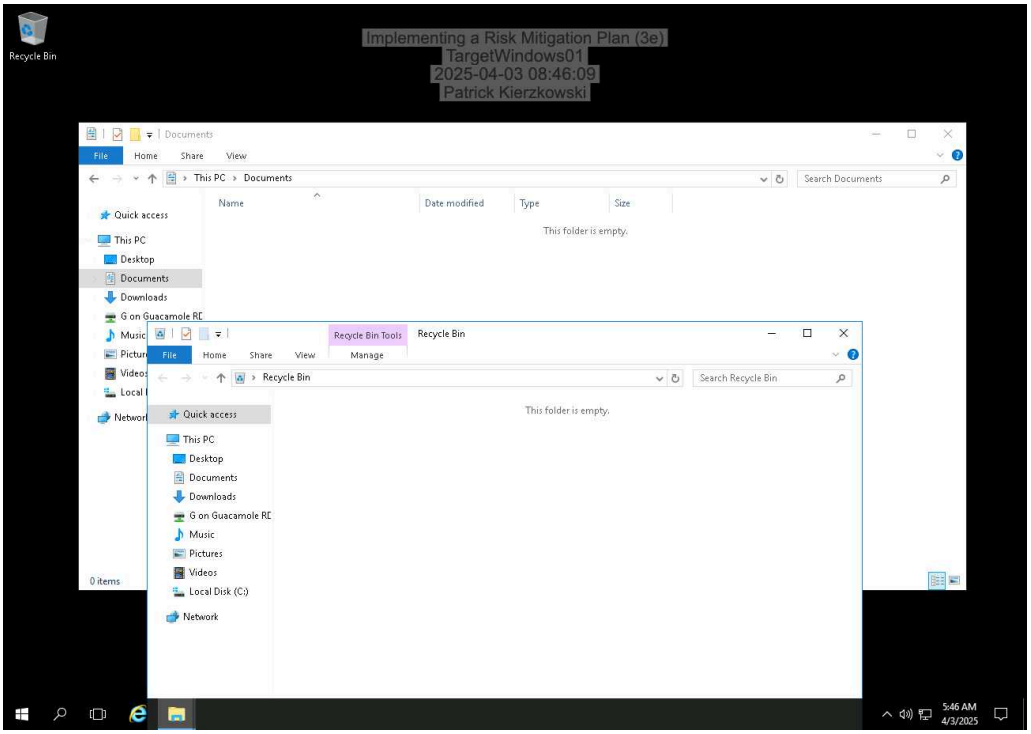
The first property of a strong password is ensuring its long enough. It should be at least 12 characters, as longer passwords are harder to crack. The second property is to use things like special characters, uppercase/lowercase letters, and numbers as it makes the password more complex. A third property is that you should have a different password for every account, just incase a breach occurs on one of those platforms. If you're password gets leaked it won't compromise other accounts. The last property is to avoid common words or phrases, such as using Password as you're password.

4. **Update** the existing password policy with an additional statement for each property.

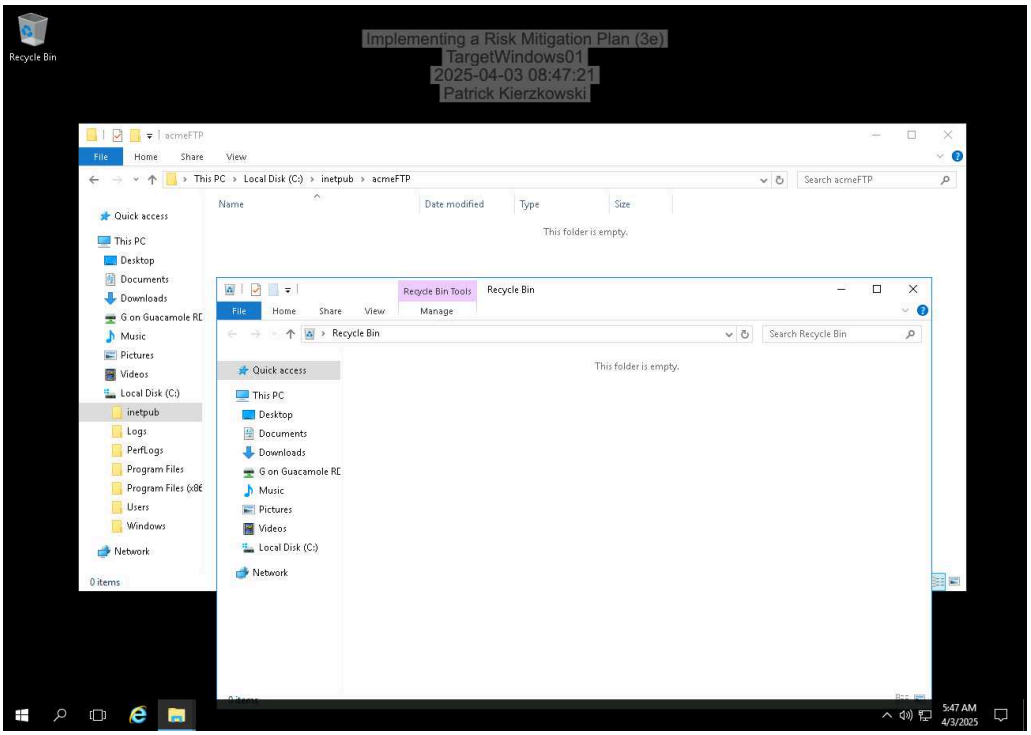
2.2.1 - All employees shall have a password for information services and computers they have been using. Passwords must be 12 characters long, and include letters, symbols and numbers. 2.2.2 - Employees shall not share their passwords with other employees. If a password is leaked or stolen, report it right away2.2.3 - Employees shall not write their passwords on paper. If you think you will forget your password, store it in a secure password manager. 2.2.4 - Employees shall not use their personal password in the computer and services of the Acme. Your work password should be unique from your personal passwords, for our safety and yours.

Part 2: Sanitize a Windows Server

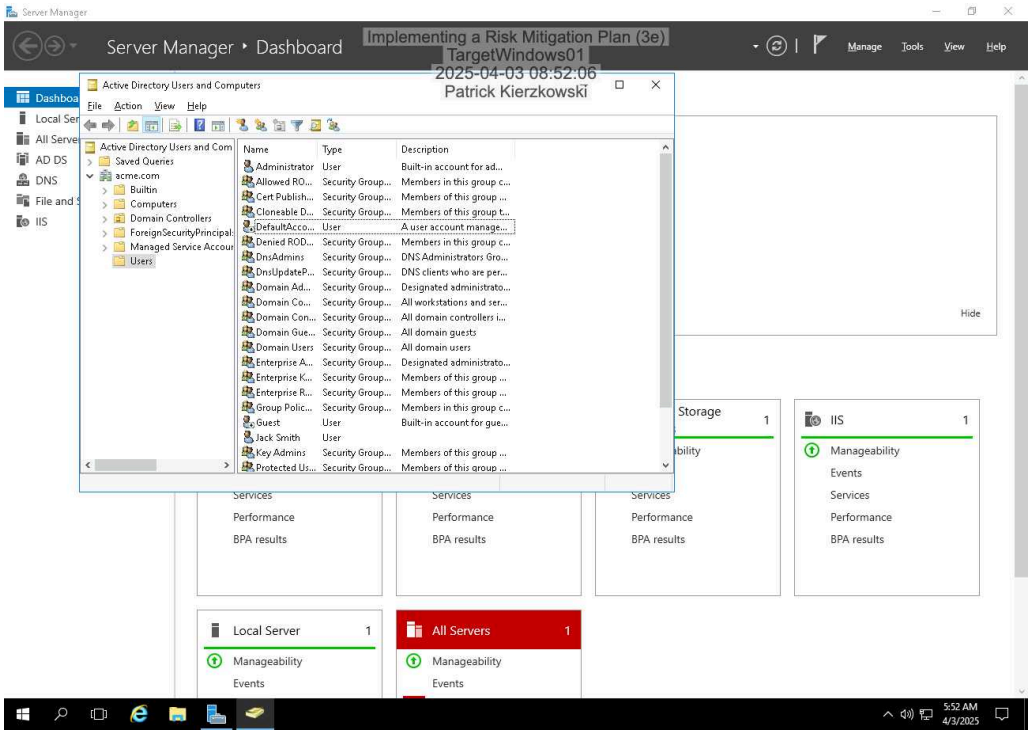
7. **Make a screen capture** showing the **empty Documents folder and empty Recycle Bin icon**.



12. **Make a screen capture** showing the **empty acmeFTP folder and empty Recycle Bin icon**.

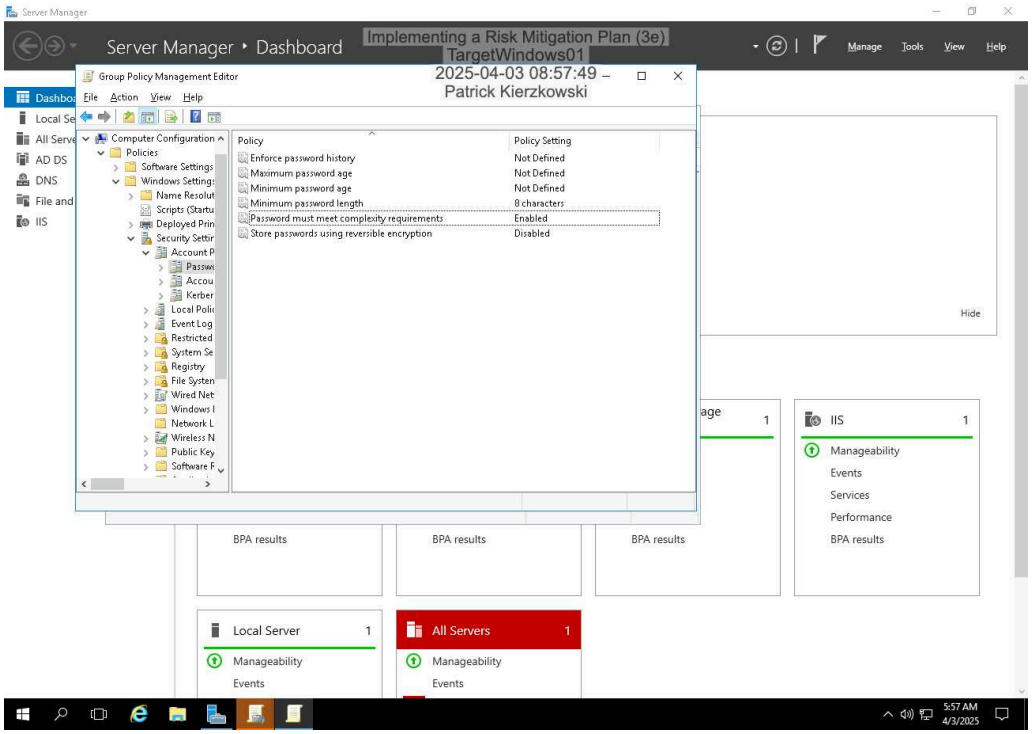


22. **Make a screen capture** showing the **Active Directory Users and Computers console without the Database_Test user**.



Part 3: Update the Active Directory Password Policy

11. **Make a screen capture** showing the **updated password policy**.

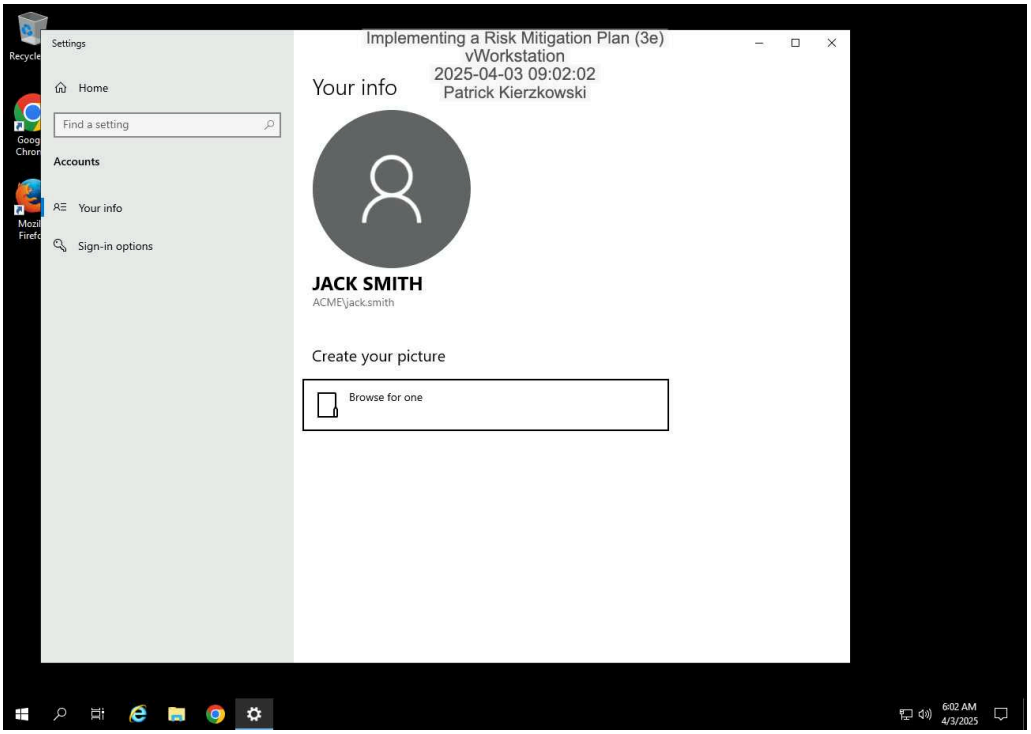


Part 4: Change a User Password

12. **Record** the new password that you used.

P@ssw0rd!

14. **Make a screen capture** showing the **Jack Smith account logged in on the vWorkstation**.



Challenge Exercises

Part 1: Define a Security Policy for Handling Sensitive Information

Create one or more clauses for each policy requirement.

2.2.1 - All employees shall have a password for information services and computers they have been using. The password must meet the required minimum length, and include a symbol or numbers. 2.2.2- Employees shall not share their passwords with other employees. If an co-worker or anyone asks for your password, report them to HR. 2.2.3 - Employees shall not write their passwords on papers. Employees are encouraged to use a password manager to store passwords.2.2.4 - Employees shall not use their personal password in the computer and services of the Acme. A unique password should be used incase Acme has a breach or you do.
Failure to comply with these policies may lead to termination of contract

Part 2: Map Your Actions to the ISO/IEC 27002 Information Security Controls

Describe what you have already done in response to four of the security controls.

Information Security Awareness, Education, and Training: Employees were informed of the policies that are set in stone and were told to encrypt sensitive info. Appropriate training is going to be provided to confirm all employees understand what is expected.
Information Security Policies: Security policies were updated so employees know how to handle sensitive information . Employees were also informed that failure of meeting these security policies can lead to termination of contract. Allocation of Information Security Responsibilities: Everyone knows what their job is and how to do it. For example, employees properly storing sensitive information, and the security team checks for problems and fixes them.Data Protection and Privacy of Personal Information: Clear text files were deleted that contained sensitive information.

Identify the five security controls that are not applicable to this case.

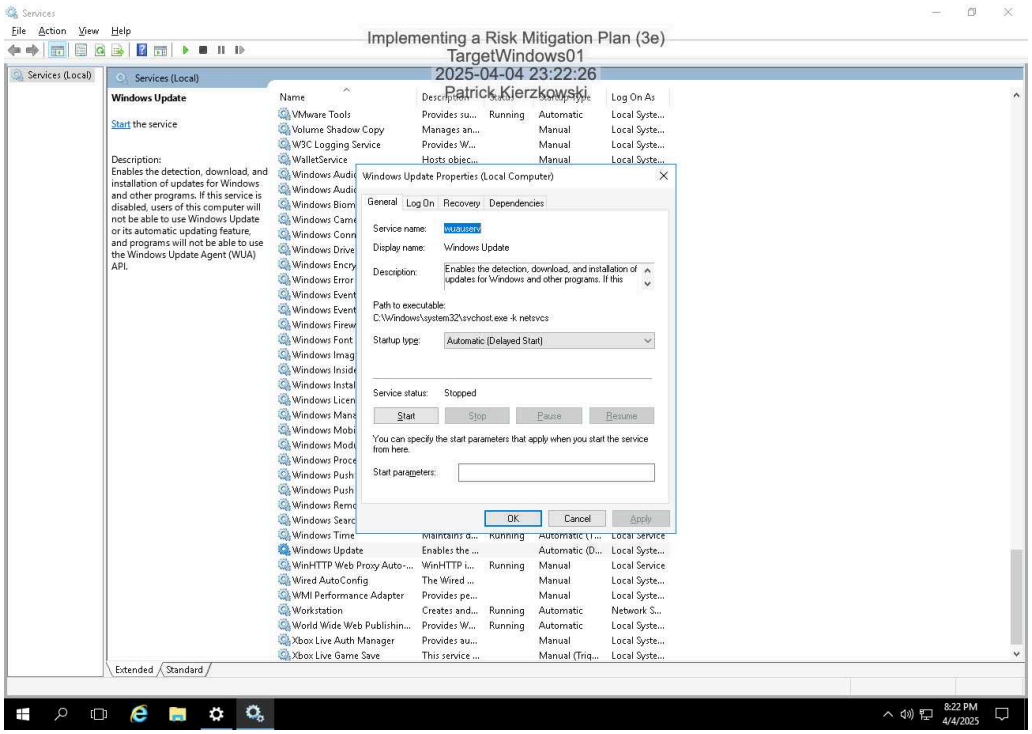
Enforce Intellectual Property Rights: There are no copyright issues in this case.Correct Data Processing: This is more about how data is entered or stored, rather than how it's storedBusiness Continuity Management: We are focusing more on data confidentiality, rather than what to do if a disaster or system failure happensProtection of Organizational Records: Same here, we are focusing on current ways that files can be stored, rather than how they conserve files in the long term.Management of Information Security Incidents: There was no security breach, it was just an action to prevent problems before they can be exploited.

Describe what you could do to implement the remaining security control.

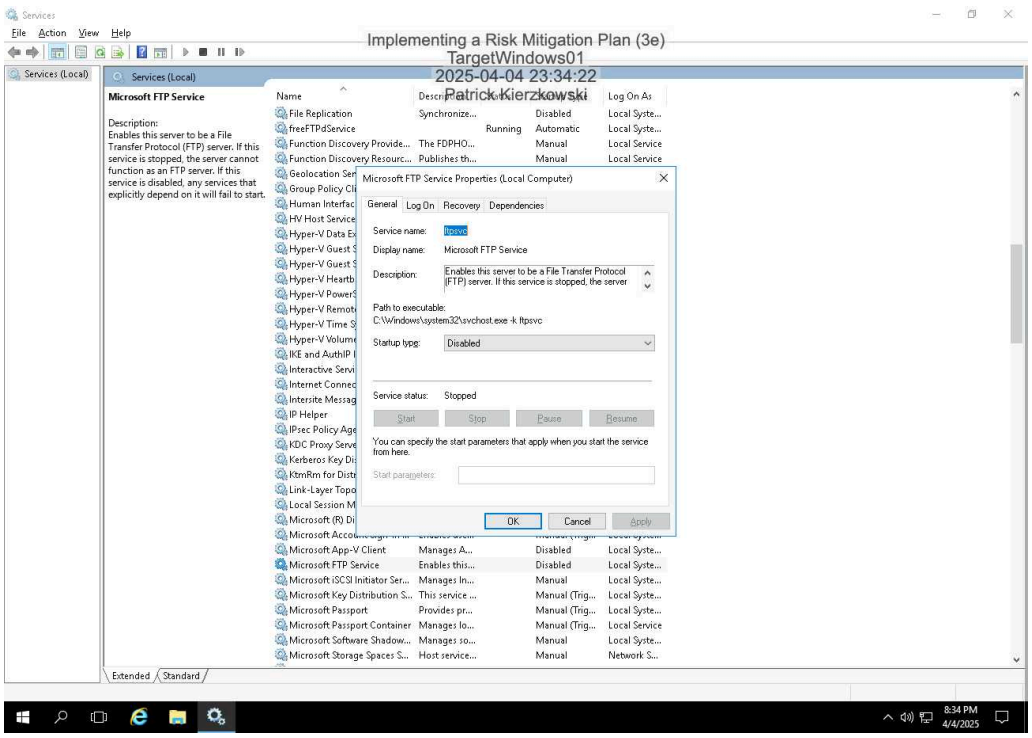
Technical Vulnerability Management:What can be done to implement the remaining security control is to regularly scan systems for things such as unencrypted sensitivity information. Automated tools can detect clear text files and then patches can be made to deal with those vulnerabilities

Part 3: Harden TargetWindows01

Make a screen capture showing the **activated Windows Update service**.



Make a screen capture showing the **disabled Microsoft FTP service**.



Make a screen capture showing the **uninstalled third-party management tool that you located**.