Student:	Email:
Kaleb Alstott	alstottk1@mymail.nku.edu

Time on Task:	Progress:
4 hours, 25 minutes	100%

Report Generated: Sunday, November 28, 2021 at 10:19 PM

Guided Exercises

Part 1: Update the Information Security Policy Document

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

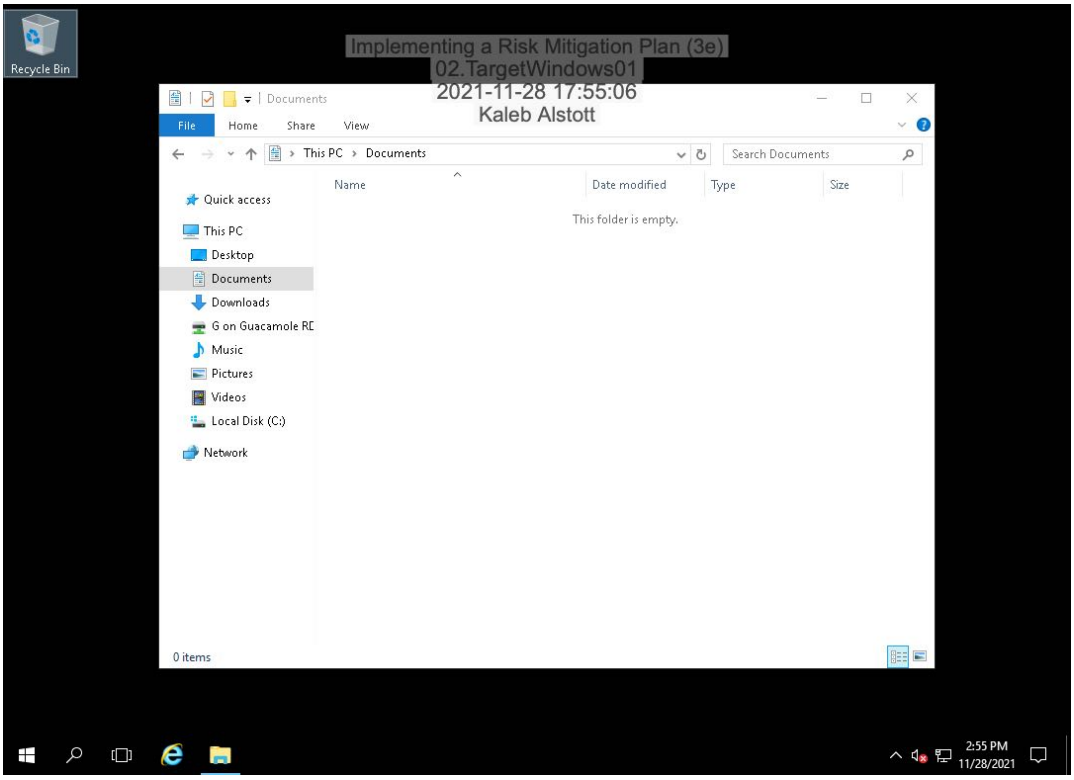
1. Password should have a capital letter, lowercase letter, number, and special character 2. Password needs to be 8 characters long 3. Password changed every 90 days 4. Passwords cannot be duplicated once used

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

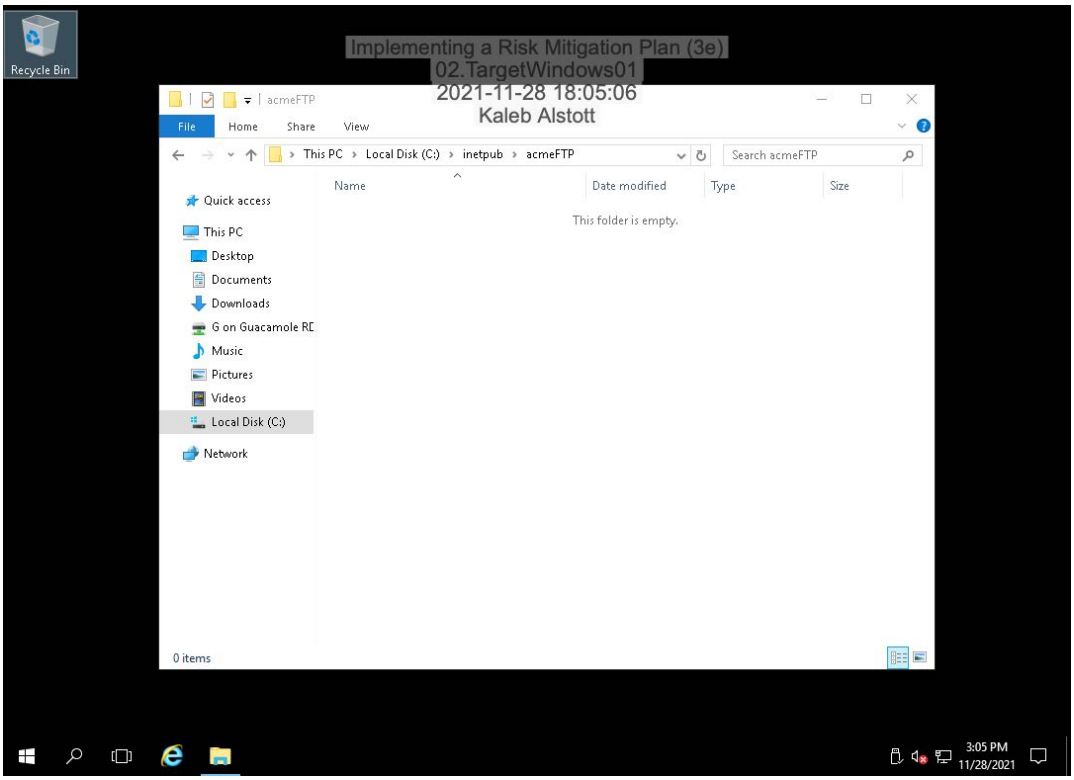
1.Employees must create a complex password with specific requirements 2. Employees need to meet required password length 3. Employees need to have a changed password by 90 days 4. Employees shall not duplicate or reuse passwords

Part 2: Sanitize a Windows Server

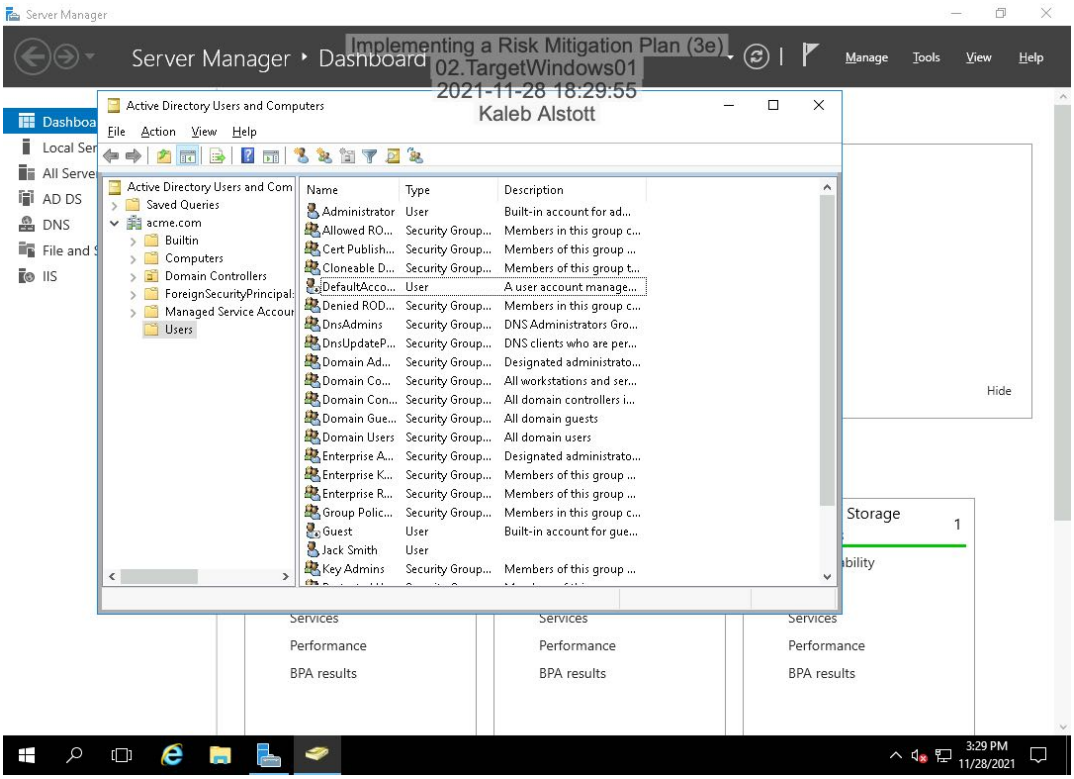
7. **Make a screen capture** showing the **empty Documents folder and empty Recycle Bin icon**.



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

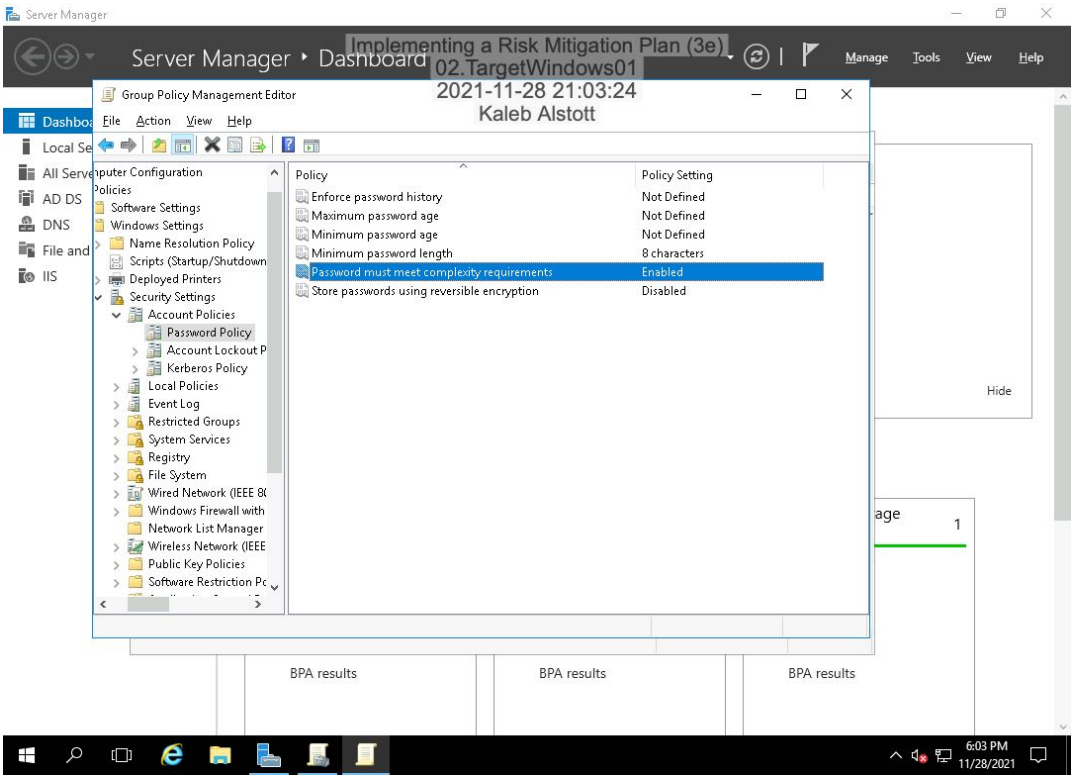


22. **Make a screen capture** showing the **Active Directory Users and Computers console without the Database_Test user**.



Part 3: Update the Active Directory Password Policy

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

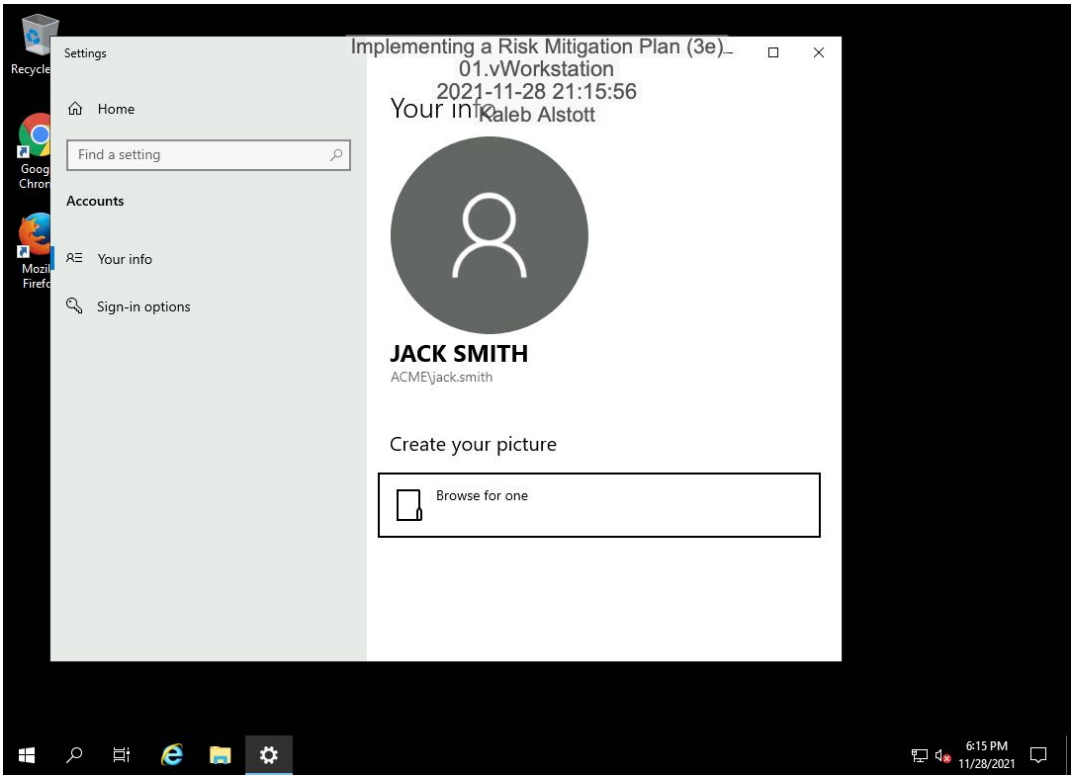


Part 4: Change a User Password

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

Bananas890@

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.

1.We would first start by defining each role with their specific responsibilities of users, systems, networks, server maintenance and security protocols/administrations. There needs to be a policy in place making sure encryptions are in place with software, downloads, and such servers. 2. First we would state and put in place a policy were we directly tell users that they cannot store any sensitive information on their computers. The next policy put into place would be to make sure passwords are stored in appropriate places and encrypted. 3. The policy I would create for disciplinary actions would be possible firing from the job. A policy for minor disciplinary options would be a possible suspension.

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.

We have already done a data protection and privacy of personal info, deleted certain files Information, updated the policy document, went through and examined the responsibilities within the policy document, set up policies to train, educate, and improve security.

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

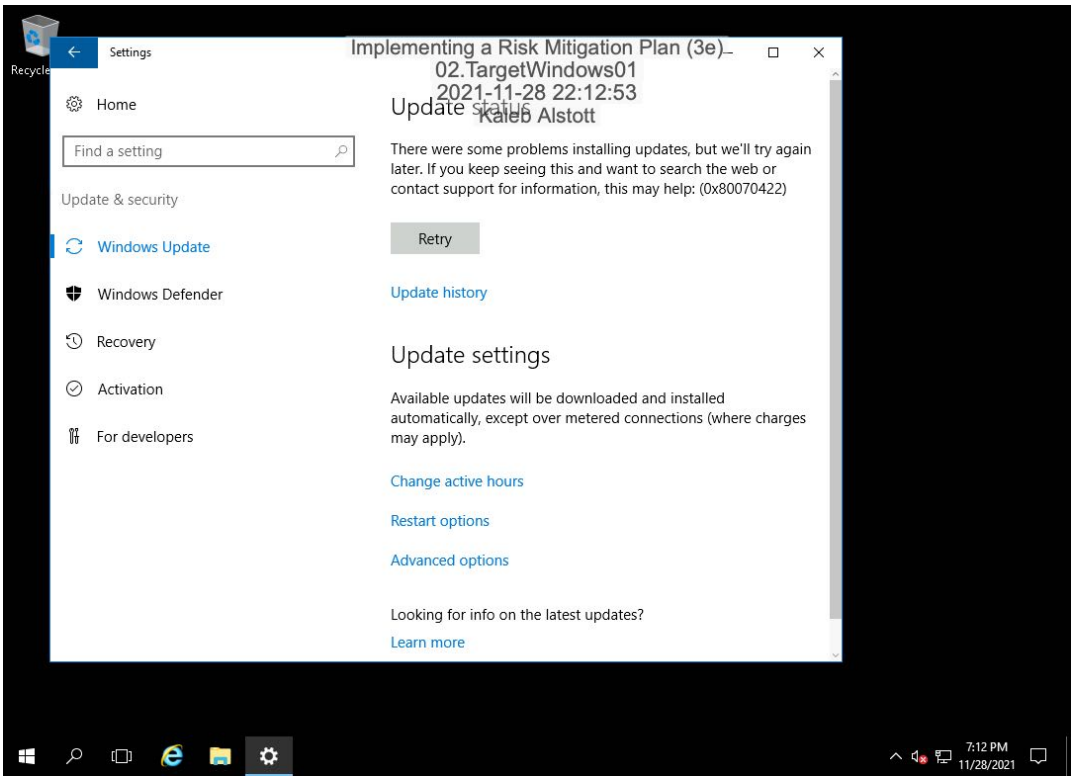
Enforce intellectual property rights Correct data processing Technical vulnerability management Management of information security incidents Business continuity management

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

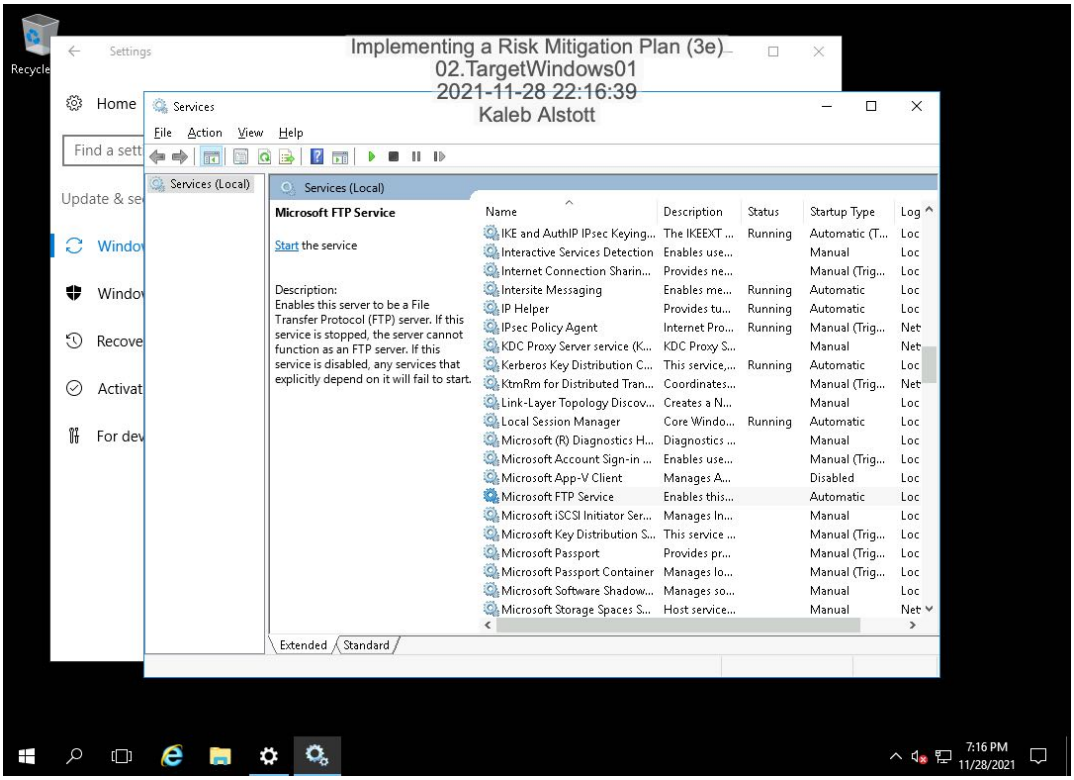
Protection of files. We would have an encryption to the server that holds our files.

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**.