Fed F1rst Control Systems

Course Project Scenario:

You are a security engineer for Fed F1rst Control Systems. Fed F1rst has recently spun out of a larger organization into a stand-alone company. You have been tasked with implementing the endpoint portion of the organization's security policy.

The tasks that follow represent real tasks that would be performed on a scheduled and on an as-needed basis (for instance, server hardening is typically performed upon installation.) You will harden a Windows 10 desktop as well as a Windows 2016 server. In the exercises you performed during the course, you hardened a CentOS Linux server. Those skills will come in handy here. From there, you will create several security policies for the organization. As with hardening, you also performed this activity, but for different areas of the Information Technology department, during the course. Additionally, you will create build sheets for Windows and Linux cloud servers using the knowledge you have gained throughout the course. Finally, you will conduct a subset of a server self-assessment that is common during pre-work for compliance audits.

Develop a hardening strategy for Windows Operating Systems:

You have access to a Windows 2016 Server and a Windows 10 Desktop that are indicative of the images currently used by Fed F1rst.

1. Log on to each device as Udacity-Student with a password of UdacityRocks!
2. Perform an analysis on the typical areas of securing the Windows Operating System including any 3rd party applications that may be installed. Check for things such as updates, permissions, antivirus, firewall as well as other items.
3. Fill out the appropriate form below with findings and recommendations. To successfully pass this portion you must find the 3 critical issues in each server and an additional 3 items that require mitigation. *Note, it is not required to change the configuration of the items, only to document and offer remediation notes.

Windows 10 Template (Add rows as needed):

MachineID: Windows 10 Pro

Item	Current Status	Recommended Status
OS version (Outdated)	Windows 10 1809	Windows 10 22H2
Firewall	Firewall is disable.	Firewall will be enable.
Local Guest account	Account is enable.	Account will be disable.
Minimum Password length		It must be 14 digits.
Password expiration	It is disable, and not set.	It will be enable and configurated.
Bitlocker encryption	Turned off	Turn on.
Windows Update (Update History)	Outdated updates have been installed.	Check available updates and install it.
WinSCP	Current version of WinSCP is 5.13	Update latest version of WinSCP.
Virus and Threat Protection	It is disable.	It will be enable.
Log in as Carol_HR Windows 10 with RDP	Carol can't log in to Windows 10 with RDP.	Enable and set for Carol log in to Windows 10 with RDP
Log in as member of Operations group	Member of Operations group have access to HR folder and they can delete important files and directories from it.	Set permissions right on the Server.
Log in as member of IT group	Member of IT group have access to Operations folder and they can delete important files and directories from it.	Set permissions right on the Server.
If somebody log in as member of IT,HR,	They will not see the contents of the folder. (for	Set permissions right on the Server.

Accounting, Operations groups	example files of public interest)	

Windows Server Hardening Checklist:

MachineID: Windows Server 2016 Datacenter

Item	Current Status	Recommended Status
OS version	Windows Server 2016 version 1607 (14393.4104)	Update for Windows Server 2016 version 1607 (14393.6897)
Firewall	Firewall is disable.	Firewall will be enable.
Minimum Password length	It is 0 now.	It must be 14 digits.
Password expiration	It is disable, and not set.	It will be enable and configurated
Security Event log	Not accessible, not set up.	It will be accessible, configurated.
Local Guest account	Account is enable.	Account will be disable.
Server Roles and features documantation	Not documented	It must be documented.
Password complexity	Not accessible, no data.	It will be enable and configurated.
Windows Update (Update History)	No updates have been installed yet.	Check available update and install it.
Bitlocker encryption	Turned off	Turn on.
Microsoft Visual C++ 2010	Current version 10.0.40219 is not supported.	Remove this version of application and update latest version.
HR folder permission	Operations have too many permissions. (Modify,Read & Execute, Read, List folder contents,Write)	Reduce Operations permissions on HR folder. (Read & Execute, Read, List folder contents)
Operations folder permission	IT have too many permissions. (Full control, Modify,Read & Execute, Read, List folder contents,Write)	Reduce IT permissions on Operations folder. (Read & Execute, Read, List folder contents)
Public folder permission	IT,HR, Accounting, Operations haven't necessary permissions. (Read & Execute, Read, List folder contents)	Set necessary permissions for IT,HR, Accounting, Operations on Public folder. (Read & Execute, Read, List folder contents)
Accounting folder permission	IT have too many permissions. (Full control, Modify,Read & Execute, Read, List folder contents,Write)	Reduce IT permissions on Operations folder. (Read & Execute, Read, List folder contents)

Create Security Policies

You have been asked to create the following policies for Fed F1rst: *Access Control Policy, Information Security Policy, and IT Asset Management Policy*. You have been provided a basic template below to use.

For success, the Access Control Policy must include information on: Creating Accounts, Password Management, Privilege Management, Network Segmentation, and Monitoring.

The Information Security Policy must include information on: Data classification, Responsibilities of data security, and how to handle Restricted Data.

The IT Asset Management Policy must include information on: Types of Assets Covered, Asset acquisition and Asset tagging.

You are encouraged to view various samples that are available via internet research and adjust sections to fit the use case of Fed F1rst. For instance, Fed F1rst is a Control Systems Manufacturer, so the language will need to be geared towards an organization with those characteristics and not one such as a University or a Financial firm. These policies will be reviewed by the Board of Directors and the Leadership team of Fed F1rst so please maintain proper grammar and professional language when creating the document.

I prepared each document in a separate file and I am attaching them to my zip file!

Security Policy Template [Make a copy for each policy]:

Fed F1rst Control Systems

Title:

Executive Summary:

Purpose:

Scope:

Policy:

(Add Sections specific to the policy as needed)

Revision Number	Date Revised:	Revised by:	Notes:

Self-Assessment

Using the provided Self-Assessment document (link) login to all 3 of the provided virtual machines with the provided credentials of Udacity-Student and password UdacityRocks! (Note: in the Linux VM, the username is case sensitive.) and perform the Self-Assessment. As with the hardening task, you do not have to perform the mitigation tasks, only note them in the form.

Cloud Server Build Sheet

Using the provided template, create a vendor-agnostic checklist/build sheet for future cloud servers. You may use the provided VMs and the hardening checklist as a guide. Also notes from the cloud server lesson will provide additional context. The build sheet will allow for automated deployments via images that meet the organization's security policies as well as compliance standards.