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 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, and 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: LabVM-258506

Item	Current Status	Recommended Status
Missing Security Updates	Windows Desktop lacks critical security updates, leaving it vulnerable to known exploits and attacks.	Schedule regular Windows updates to ensure the system is up to date with the latest security patches.
Weak User Password Policy	Windows Desktop allows users to set weak passwords or doesn't enforce password complexity requirements.	Enforce strong password policies, including minimum length, complexity requirements, and regular password expiration.
Inadequate Firewall Configuration	Windows Desktop firewall is not properly configured to restrict incoming and outgoing network traffic.	Review and update firewall rules to allow only necessary network traffic, block unnecessary ports, and enable logging for monitoring purposes.
Lack of Endpoint Protection	Windows Desktop does not have endpoint protection software installed or activated.	Install and configure antivirus/antimalware software on the desktop, ensure real-time protection is enabled, and schedule regular scans.
Unrestricted User Privileges	Users on the Windows Desktop have unnecessary administrative privileges.	Implement the principle of least privilege by restricting user accounts to standard user rights unless

		administrative access is required for specific tasks.
Unused or Outdated Software	Windows Desktop has unused or outdated software installed, increasing the attack surface.	Regularly audit installed software, uninstall any unnecessary applications, and keep all software up to date with the latest security patches.

Windows Server Hardening Checklist:

MachineID: JumpVM-258506

Item	Current Status	Recommended Status
Unpatched System Vulnerabilities	Windows Server lacks critical security updates, leaving it vulnerable to known exploits and attacks.	Schedule regular Windows updates and patches to ensure the server is up to date with the latest security fixes.
Weak Administrative Passwords	Weak or default passwords are used for administrative accounts on the Windows Server.	Enforce strong password policies for administrative accounts, including minimum length, complexity requirements, and regular password changes.
Inadequate Firewall Configuration	Windows Server firewall is not properly configured to restrict incoming and outgoing network traffic.	Review and update firewall rules to allow only necessary network traffic, block unnecessary ports, and enable logging for monitoring purposes.
Misconfigured User Permissions	User permissions on the Windows Server are not properly configured, leading to excessive or insufficient access rights.	Review and adjust user permissions to follow the principle of least privilege, granting users only the access they need to perform their tasks.
Outdated or Unsupported Applications	Windows Server hosts outdated or unsupported applications that are no longer receiving security updates	Identify and upgrade or replace outdated applications with supported versions to mitigate security risks.
Lack of Auditing and Monitoring	Auditing and monitoring settings on the Windows Server are not configured to	Configure auditing policies to track critical security events, set up centralized

	track security events effectively.	logging for analysis, and implement monitoring solutions to alert administrators of suspicious activities.

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 with 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.

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

Fed F1rst Control Systems

Title: Access Control Policy

Executive Summary: The Access Control Policy outlines the guidelines and procedures for controlling access to FedF1rst Control Systems' network and resources. It aims to ensure the confidentiality, integrity, and availability of company data and resources by establishing clear access control measures.

Purpose: The purpose of this policy is to define the acceptable use of access control measures to safeguard FedF1rst Control Systems' sensitive information and resources. It aims to mitigate cyber risks, ensure compliance with regulatory requirements, and protect the organization from unauthorized access and data breaches.

Scope: This policy applies to all employees, contractors, consultants, and third-party vendors who have access to FedF1rst Control Systems' network and resources. It encompasses all information, electronic and computing devices, and

network resources used to conduct FedF1rst business or interact with internal networks and systems.

Policy:

1. **Creating Accounts:**
    1.1. User accounts will be created for employees, contractors, and authorized third-party vendors based on the principle of least privilege.
    1.2. Requests for account creation must be submitted to the IT department and approved by the appropriate authority.
    1.3. Accounts will be provisioned with access rights tailored to the individual's job responsibilities and least privilege principle.
2. **Password Management:**
    2.1. Passwords must adhere to the company's password policy, including complexity requirements, minimum length, and regular expiration.
    2.2. Users are responsible for keeping their passwords confidential and not sharing them with anyone.
    2.3. Passwords should be changed periodically, and employees must report any suspected compromise of their passwords immediately.
3. **Privilege Management:**
    3.1. Access privileges will be granted based on the principle of least privilege, where users are granted only the access necessary to perform their job functions.
    3.2. Access rights will be reviewed regularly and adjusted as needed, based on changes in job roles or responsibilities.
    3.3. Employees must not share their access credentials or provide unauthorized access to others.
4. **Network Segmentation:**
    4.1. The network will be segmented to separate different types of traffic and restrict access between network segments.
    4.2. Access control lists (ACLs) and firewalls will be used to enforce network segmentation and control traffic flow.
    4.3. Critical systems and sensitive data will be isolated from less secure network segments to minimize the risk of unauthorized access.
5. **Monitoring:**

5.1. Access to network resources will be monitored using intrusion detection systems (IDS), intrusion prevention systems (IPS), and logging mechanisms.

5.2. Authorized individuals within FedF1rst Control Systems may monitor equipment, systems, and network traffic at any time for security and network maintenance purposes.

5.3. Regular audits of user accounts, access logs, and network traffic will be conducted to ensure compliance with this policy.

Title: Information Security Policy

Executive Summary: The Information Security Policy establishes the framework for protecting FedF1rst Control Systems' sensitive information and data assets. It outlines the guidelines and procedures for data classification, defines responsibilities for data security, and provides guidance on handling restricted data to ensure confidentiality, integrity, and availability.

Purpose: The purpose of this policy is to safeguard FedF1rst Control Systems' data assets from unauthorized access, disclosure, alteration, or destruction. It aims to ensure compliance with regulatory requirements, mitigate cyber risks, and maintain trust and confidence in the organization's information security practices.

Scope: This policy applies to all employees, contractors, consultants, and third-party vendors who handle or have access to FedF1rst Control Systems' data assets. It encompasses all data, regardless of format or storage location, and applies to data processed, stored, or transmitted by FedF1rst Control Systems' information systems.

Policy:

1. **Data Classification:**

1.1. All data assets will be classified based on their sensitivity, criticality, and regulatory requirements to ensure appropriate protection measures are applied.

1.2. Data classification levels will include public, internal use, confidential, and restricted data, with specific criteria defined for each classification level.

1.3. Employees are responsible for identifying and classifying data by the Data Classification Policy and labelling data appropriately.

2. **Responsibilities of Data Security:**
    2.1. Employees are responsible for ensuring the security and confidentiality of FedF1rst Control Systems' data assets in their custody or under their access.
    2.2. Data custodians will be appointed for each data asset to oversee its security, access controls, and compliance with data protection standards.
    2.3. Managers and supervisors are responsible for enforcing data security policies and providing necessary training and resources to employees.
3. **Handling Restricted Data:**
    3.1. Restricted data, including personally identifiable information (PII), financial data, trade secrets, and intellectual property, will be handled with the utmost care and protection.
    3.2. Access to restricted data will be limited to authorized personnel with legitimate business need-to-know and appropriate access permissions.
    3.3. Employees must follow established procedures for accessing, storing, transmitting, and disposing of restricted data by legal and regulatory requirements.

Title: IT Asset Management Policy

Executive Summary: The IT Asset Management Policy establishes the procedures for managing and maintaining FedF1rst Control Systems' IT assets throughout their lifecycle. It defines the types of assets covered, outlines the process for asset acquisition, and establishes requirements for asset tagging to ensure effective tracking and inventory management.

Purpose: The purpose of this policy is to ensure proper acquisition, use, and disposal of IT assets to support business operations effectively. It aims to optimize asset utilization, minimize risks associated with asset loss or theft, and maintain accurate records of IT assets for financial and compliance purposes.

Scope: This policy applies to all IT assets owned, leased, or used by FedF1rst Control Systems, including hardware, software, and data assets. It encompasses all stages of the asset lifecycle, from procurement and deployment to retirement and disposal.

Policy:

1. **Types of Assets Covered:**

   1.1. IT assets covered by this policy include hardware (e.g., computers, servers, networking equipment), software (e.g., operating systems, applications), and data assets (e.g., databases, documents).

   1.2. All IT assets, regardless of type or value, are subject to the provisions of this policy and must be managed under established procedures.

2. **Asset Acquisition:**

   2.1. All IT asset acquisitions must be approved by the appropriate authority, such as the IT department or designated asset manager.

   2.2. Before acquisition, a comprehensive assessment of business requirements, budgetary constraints, and technical specifications will be conducted to ensure alignment with organizational goals and objectives.

   2.3. Procurement processes will adhere to applicable laws, regulations, and internal policies, including vendor selection, contract negotiation, and purchase authorization.

3. **Asset Tagging:**

   3.1. All IT assets will be tagged with unique identifiers for tracking and inventory management purposes.

   3.2. Asset tags will include information such as asset name, serial number, location, owner, acquisition date, and asset classification.

   3.3. Asset tagging will be conducted at the time of acquisition and maintained throughout the asset lifecycle to facilitate accurate tracking, auditing, and reporting.

Revision Number	Date Revised:	Revised by:	Notes:
1	May 1, 2024	Fed F1rst Policy Team	Updated Access Control Policy

2	May 1, 2024	Fed F1rst Policy Team	Updated Information Security Policy
3	May 1, 2024	Fed F1rst Policy Team	Updated IT Asset Management Policy

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.