Fed F1rst Control Systems

Scenario 1:

Device Hardening

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

You have been provided cloud-lab 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
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.

Solution:

FED F1RST CONTROL SYSTEMS DEVICE HARDENING

Windows 10 Hardening Checklist:

MachineID: 4F6AD745-3C7A-498D-BACD-46C5F60FF2BD

Item	Current Status	Recommended Status
Update	System is missing critical updates and automatic updates have been turned off.	The desktop should be configured to automatically update, or update can be managed using SCCM, WSUS etc.
Firewall	Firewall disabled	Firewall should be enabled
Disk Encryption	BitLocker Drive Encryption is turned off	BitLocker Drive Encryption should be turned on

Logging and Monitoring	Security Event log is enabled	Maximun log size can be increased
Local Security Policy	Account lockout policy and password policy are not properly configured	Password policy(age, complexity, length, history) and Account lockout policy(duration, threshold) should be configured according to industry standards.
Local Policy	Audit policies are not enabled	Audit policy(logon events, directory service access, system events etc.) should be configured
Guest Account	Guest Account is enabled	Disable guest account from powershell using “Set-LocalUser -Name Guest -Enabled $false”
Antivirus	Antivirus is disabled	Turn on Antivirus by navigating to Settings > Windows Security > Virus & threat protection > Turn on Virus & threat protection

Windows Server Hardening Checklist:

MachineID: 00376-40000-00000-AA947

Item	Current Status	Recommended Status
Firewall	Firewall disabled	Firewall should be enabled and configured depending on the server’s role (i.e. Public/External or Private/Internal)
Roles and Features	Roles and Features of the server not configured	Depending on the purpose of the server (e.g. Application server, Web Server, Database server etc.) the appropriate role should be configured in Sever Manager
Windows Update	The server isn’t configured to check for updates	The server should be configured to automatically update, or update can be managed using SCCM, WSUS etc.
Logging and Monitoring	Security Event logging is not enabled	Enable security logging and configure necessary parameters including log size, log path etc.
Local Security Policy	Access to local security policy to confirm status was denied by server	The following policies should be configured according to industry standard: account lockout, password policy(age, complexity, minimum length etc.), Multi Factor Authentication, User Account Control
Antivirus	Windows Defender is installed	The Antivirus software should be updated regularly to prevent Zero-day Attack
Disk Encryption	BitLocker Drive Encryption is turned off	BitLocker Drive Encryption should be turned on
Server Message Block (SMB)	SMB Version 1 is enabled	Disable SMB Version 1 by running the powershell command “Set-SmbServerConfiguration -EnableSMB1Protocol $false”
Windows SmartScreen	Windows SmartScreen is turned off	Navigate to the Control Panel > System and Security > Security and Maintenance > Turn on Windows SmartScreen

Scenario 2:

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 are encouraged to view various samples that are available via internet research and adjust sections to fit the use case of Fed F1rst.

Solution:

FED F1RST CONTROL SYSTEMS POLICIES

Title: Access Control Policy

Executive Summary:

Fed F1rst data and systems are valuable resources of the organization and must be treated as such. This Access Control Policy outlines the procedures and guidelines for managing access to Fed F1rst's resources. These systems and resources are to be used for Fed F1rst purposes only.

The policy covers the creation of accounts, password management, privilege management, network segmentation, and monitoring. It is designed to ensure the confidentiality, integrity, and availability of Fed F1rst's systems and data.

It is the responsibility of every employee, contractors, third-party vendors, and any other individuals accessing Fed F1rst's networks, systems and data to know these policies and to conduct activities accordingly.

Purpose:

The purpose of this policy is to establish a framework for controlling access to Fed F1rst's resources to mitigate the risk of unauthorized access, data breaches, and system vulnerabilities. The access control measures aim to protect sensitive information, maintain regulatory compliance, and safeguard our infrastructure from potential threats.

Scope:

This policy applies to all employees, contractors, third-party vendors, and any other individuals who access, manage, or handle Fed F1rst's information assets. It encompasses the use of information, electronic and computing devices and network resources to conduct Fed F1rst's business.

Policy:

1. **Creating Accounts:**
    - User accounts must be created only for authorized individuals who require access to Fed F1rst Control Systems' resources to perform their job duties.
    - Account creation must follow a formal approval process, including verification of the user's identity and authorization from the appropriate department or manager.
    - User accounts must be assigned with the least privilege necessary to fulfill job responsibilities, following the principle of least privilege.
    - All user accounts must be periodically reviewed and deactivated promptly upon termination of employment or contract.
2. **Password Management:**
    - Users are required to create passwords that comply with Fed F1rst's password complexity requirements which includes:
        i. Minimum length of 12 characters
        ii. At least one capital letter, one number, one special character
    - Passwords must not be shared, written down, or stored in an insecure manner.
    - Passwords must be changed regularly, following a defined password expiration policy of 60 days.
    - Multi-factor authentication (MFA) must be enforced for account logins to access Fed F1rst's systems and data.
3. **Privilege Management:**
    - Access privileges must be granted based on the principle of least privilege, limiting users' access rights to only what is necessary to perform their job functions.

- Access privileges must be reviewed and updated regularly to ensure alignment with job roles and responsibilities.
- Administrative access to critical systems must be restricted to authorized personnel and monitored closely.

4. **Network Segmentation:**
    - Fed F1rst's network must be segmented to segregate sensitive systems and data from less critical assets.
    - Access controls, such as firewalls and intrusion detection systems, must be implemented to enforce network segmentation and prevent unauthorized access between network segments.
    - Network segmentation must be regularly reviewed and updated to adapt to changing business requirements and security threats.
5. **Monitoring:**
    - Fed F1rst must implement robust monitoring mechanisms to track and log all access attempts, including successful and failed logins.
    - Logs must be regularly reviewed for suspicious activities or security incidents.
    - Intrusion detection and prevention systems must be deployed to monitor network traffic for signs of unauthorized access or malicious behavior.

Revision Number	Date Revised:	Revised by:	Notes:
1.0.0	**April 7th, 2024**	**Jubril Edun – CISO**	

Title: Information Security Policy

Executive Summary:

Fed F1rst is committed to the ensuring information security and preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organization.

The Information Security Policy provides guidelines and procedures for protecting Fed F1rst's information assets, including data classification, responsibilities of data security, and handling restricted data. It aims to safeguard the confidentiality, integrity, and availability of sensitive information and ensure compliance with regulatory requirements.

Purpose:

The Information Security Policy aims to define the principles and responsibilities for safeguarding Fed F1rst's information assets throughout their lifecycle. By implementing effective information security measures, Fed F1rst aims to mitigate the risk of data breaches, unauthorized access, and data loss, thereby protecting our reputation and maintaining customer trust.

Scope:

This policy applies to all employees, contractors, third-party vendors, and any other individuals who access, manage, or handle Fed F1rst's information assets. It encompasses the use of information, electronic and computing devices and network resources to conduct Fed F1rst's business.

Policy:

1. **Data Classification:**
    - Information assets must be classified based on their sensitivity, value, and criticality to the organization.
    - Classification labels must be applied to all information assets to indicate their level of sensitivity and determine appropriate handling and protection measures.
    - Data classification categories, such as Public, Internal Use Only, Confidential, and Restricted, must be clearly defined and communicated to all employees.
        1. Public: Data are considered Public when their unauthorized disclosure, alteration or destruction would cause little to no risk to the Fed F1rst or its affiliates.
        2. Internal Use Only: Data classified as Internal Use Only are intended solely for use within the organization and should not

be disclosed to individuals outside of the company without proper authorization. Unauthorized access, alteration, or sharing of this data could potentially harm the organization's operations or reputation.

3. Confidential: Confidential data is information that, if disclosed or accessed by unauthorized parties, could result in financial loss, legal implications, or damage to the organization's reputation. Access to confidential data should be restricted to individuals with a legitimate need-to-know and appropriate security measures should be in place to protect its confidentiality.
4. Restricted: Data classified as Restricted are highly sensitive and critical to the organization's operations, and unauthorized access, disclosure, or modification could have severe consequences. Only individuals with explicit authorization and a specific business need should have access to restricted data. Enhanced security protocols and monitoring should be implemented to safeguard this information from unauthorized access or misuse.

2. **Responsibilities of Data Security:**
    - All employees are responsible for safeguarding Fed F1rst Control Systems' information assets and complying with this Information Security Policy.
    - Information owners must identify and classify information assets under their purview, determine access controls, and ensure appropriate protection measures are in place.
    - Information custodians are responsible for implementing and maintaining security controls to protect information assets according to their classification level.
    - The Information Security Officer (ISO) is responsible for overseeing the implementation of information security policies, conducting risk assessments, and providing guidance on security best practices.
3. **Handling Restricted Data:**

- Restricted data, including personally identifiable information (PII), financial data, intellectual property, and trade secrets, must be handled with the utmost care and protection.
- Access to restricted data must be restricted to authorized individuals with a legitimate need-to-know, based on the principle of least privilege.
- Encryption must be used to protect sensitive data during storage, transmission, and processing.
- Any incidents involving the unauthorized access, disclosure, or loss of restricted data must be reported immediately to the Information Security Officer for investigation and remediation.

Revision Number	Date Revised:	Revised by:	Notes:
1.0.0	**April 7th, 2024**	**Jubril Edun – CISO**	

Title: IT Asset Management Policy

Executive Summary: The IT Asset Management Policy outlines the procedures for managing Fed F1rst Control Systems' IT assets, including the types of assets covered, asset acquisition, and asset tagging. It aims to ensure effective tracking, utilization, and protection of IT assets throughout their lifecycle to support business operations and minimize risks.

Purpose: The purpose of this policy is to establish guidelines and responsibilities for the acquisition, tracking, and management of IT assets owned or used by Fed F1rst Control Systems. By implementing an effective IT asset management process, we aim to optimize asset utilization, reduce costs, and mitigate the risk of loss or unauthorized access to sensitive information.

Scope: This policy applies to all IT assets owned, leased, or used by Fed F1rst, including but not limited to hardware, software, networking equipment, and mobile devices. It encompasses all stages of the asset lifecycle, from acquisition to disposal, and applies to all employees, contractors, and third-party vendors responsible for IT asset management.

Policy:

1. **Types of Assets Covered:**
    - IT assets covered by this policy include, but are not limited to:
        - Hardware: Computers, servers, networking equipment, printers, and peripherals.
        - Software: Operating systems, applications, and licensed software.
        - Networking Equipment: Routers, switches, firewalls, and wireless access points.
        - Mobile Devices: Smartphones, tablets, laptops, and other portable devices.
        - Data Storage Devices: Hard drives, solid-state drives, and storage arrays.
    - All IT assets must be inventoried, tracked, and managed according to the procedures outlined in this policy.

2. **Asset Acquisition:**
    - All IT asset acquisitions must be approved through the appropriate procurement process and budget allocation.
    - IT assets must be acquired from reputable vendors and suppliers, ensuring compatibility, reliability, and compliance with legal and regulatory requirements.
    - Asset acquisition records, including purchase orders, invoices, and warranty information, must be maintained and documented in the asset management system.
3. **Asset Tagging:**
    - All IT assets must be tagged with a unique identifier or asset tag upon acquisition to facilitate tracking and identification.
    - Asset tags must include essential information such as asset name, serial number, location, and acquisition date.
    - Asset tags must be affixed to visible and accessible locations on the asset to ensure easy identification and inventory management.

- Any changes to asset location, status, or ownership must be promptly updated in the asset management system to maintain accurate records.

Revision Number	Date Revised:	Revised by:	Notes:
1.0.0	**April 7th, 2024**	**Jubril Edun – CISO**	