Fed F1rst Control Systems

Title: IT Asset Management Policy

Executive Summary: The IT Asset Management Policy governs the acquisition, deployment, and lifecycle management of IT assets, including hardware, software, and data, to optimize resource utilization and minimize security risks.

Purpose: To establish procedures for inventorying, tracking, and maintaining IT assets, ensuring proper control and accountability throughout their lifecycle.

Scope: This policy applies to all IT assets owned or operated by the organization, including those used by employees, contractors, and third-party vendors, both on-premises and remote locations.

Policy:

1. Introduction

This IT Asset Management Policy outlines the principles and procedures governing the acquisition, deployment, management, and disposal of IT assets within FedF1rst. The policy aims to ensure the security, integrity, and efficiency of IT assets while aligning with industry best practices and regulatory requirements.

2. Scope

This policy applies to all IT assets owned, leased, or otherwise controlled by FedF1rst, including but not limited to hardware, software, networking equipment, and data.

3. Objectives

- Ensure the availability, reliability, and performance of IT assets to support business operations.
- Protect sensitive information and intellectual property stored or processed on IT assets.
- Mitigate the risks associated with unauthorized access, data breaches, and cyber threats.

- Facilitate compliance with relevant laws, regulations, and industry standards related to IT asset management and security.

4. Roles and Responsibilities

- **IT Department**: The IT department is responsible for the overall management and oversight of IT assets, including procurement, deployment, maintenance, and disposal.
- **Asset Owners**: Each IT asset will have a designated owner who is responsible for its proper use, maintenance, and security throughout its lifecycle.
- **Employees**: All employees are responsible for adhering to this policy and reporting any issues or concerns related to IT asset management and security.

5. Asset Lifecycle Management

- **Acquisition**: IT assets shall be acquired through approved channels and in accordance with established procurement procedures. All acquisitions must be documented, including purchase orders, licenses, warranties, and support agreements.
- **Deployment**: IT assets shall be deployed in a secure manner, following configuration standards and best practices to minimize vulnerabilities and ensure compatibility with existing systems.
- **Maintenance**: Regular maintenance and updates shall be performed to keep IT assets up to date with security patches, firmware upgrades, and software updates. Maintenance schedules and procedures shall be documented and followed diligently.
- **Monitoring**: IT assets shall be monitored continuously for performance, security incidents, and compliance with established policies. Monitoring tools and techniques shall be

employed to detect and mitigate potential threats and vulnerabilities.

- **Disposal**: At the end of their lifecycle, IT assets shall be decommissioned and disposed of securely to prevent unauthorized access to sensitive data. Disposal methods shall comply with environmental regulations and industry standards for data destruction.

6. Security Controls

- **Access Control**: Access to IT assets shall be granted on a need-to-know basis, using strong authentication mechanisms such as passwords, multi-factor authentication, and role-based access control.
- **Data Encryption**: Sensitive data stored or transmitted by IT assets shall be encrypted using industry-standard encryption algorithms and protocols to prevent unauthorized disclosure or modification.
- **Vulnerability Management**: Regular vulnerability assessments and penetration testing shall be conducted to identify and remediate security vulnerabilities in IT assets.
- **Incident Response**: An incident response plan shall be developed and maintained to address security incidents and breaches involving IT assets. The plan shall outline procedures for reporting, investigating, and mitigating security incidents in a timely manner.
- **Backup and Recovery**: Regular backups of critical data stored on IT assets shall be performed to ensure data availability and integrity in the event of system failures, disasters, or cyber attacks.

7. Compliance and Audit

- **Compliance**: IT asset management practices shall comply with relevant laws, regulations, and industry standards, including but

not limited to GDPR, ISO 27001, and NIST Cybersecurity Framework.

- **Audit**: Periodic audits and assessments shall be conducted to evaluate the effectiveness of IT asset management controls and ensure compliance with this policy. Audit findings shall be documented, and corrective actions shall be taken as necessary to address identified deficiencies.

8. Training and Awareness

- **Training**: Employees shall receive regular training and awareness programs on IT asset management best practices, security policies, and procedures to ensure understanding and compliance.
- **Communication**: Changes to IT asset management policies, procedures, or controls shall be communicated to all relevant stakeholders in a timely manner to ensure awareness and adherence.

9. Policy Review and Revision

This IT Asset Management Policy shall be reviewed annually and updated as necessary to reflect changes in technology, business requirements, and regulatory landscape.

10. Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment, in accordance with FedF1rst's disciplinary procedures.

Revision Number	Date Revised:	Revised by:	Notes: