**Security Assessment Report**

**for**

**Fielder Medical Center (FMC)**

**Version 1.0**

Prepared by

Pruhart Security Consulting

**FOR OFFICIAL USE ONLY**

**Document Revision History**

The security assessment report (SAR) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed annually. Reviews made as part of the assessment process shall also be recorded below.

This document history shall be maintained throughout the life of the document and the associated system.

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| 01/05/20XX | Document Publication | 1.0 | Sophia Martin |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**From:** Sophia Martin, Head Consultant, Pruhart Security Consulting

**To:** Board of Directors, Fielder Medical Center (FMC)

On behalf of Pruhart Security Consulting, I would like to thank you for the opportunity to provide a security audit and assessment for FMC. We have finalized our preliminary reporting and are disseminating our findings below for your review.

Our key findings indicate FMC needs specialized support in updating and modernizing its network and internal controls to address the changing landscape of laws, regulations, and standards that apply to federal government compliance. Specifically, FMC needs to address the following:

1. There is a lack of security controls and policies, including access control policies and procedures, account management, least privilege, and security attributes.
2. The systems design is outdated, requiring immediate attention to remediate gaps between the previous and outdated systems security plan (SSP) and compliance requirements.
3. Security and privacy plans need to be updated to reflect the organizational needs and requirements. This includes:
   1. an information security program plan based on compliance and the organization’s needs
   2. an updated system inventory/asset list based on the organization’s systems
   3. a risk assessment completed after updating the current SSP to reflect the new controls within the network and information systems
4. There is a lack of multifactor authentication (MFA) and a need to identify and authenticate organizational users requiring access to the network and information systems.

We appreciate the time FMC employees spent with us to help us compile this report. If you have any questions, please feel free to consult Pruhart Security Consulting at any time.

Regards,

Sophia Martin, Head Consultant, Pruhart Security Consulting

**Table of Contents**

1 Overview 5

1.1 Applicable Standards and Guidance 5

1.2 Purpose 5

2 System Overview 6

2.1 System Name 6

3 Assessment Methodology 7

3.1 Overall Security Findings 8

3.2 Overall Findings Across All Connected Systems 8

3.3 Security and Privacy Control Families/Control Enhancements 9

**1 Overview**

This document represents the security assessment report (SAR) for FMC as requested as part of the security assessment and posture for FMC and related entities. This SAR contains the summary results of the comprehensive security test and evaluation of FMC. This assessment report, and the results documented herein, supports program goals, efforts, and activities necessary to achieve compliance with organizational security requirements.

Title III, Section 3544, of the E-Government Act of 2002, dated December 17, 2002, requires agencies to conduct periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. Appendix III of Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, requires federal agencies to do the following:

* Review the security controls in each system when significant modifications are made to the system, but at least every three years. §3(a)(3)
* Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. §8(a)(1)(g); §8(a)(9)(a)
* Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time. §8(b)(3)(b)(iv)
* Ensure that a management official authorizes in writing the use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and reauthorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application. §(3)(b)(4)

**1.1 Applicable Standards and Guidance**

The following standards and guidance are applicable to FMC:

* Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53, Revision 5]
* Risk Management Guide for Information Technology Systems [NIST SP 800-30]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]

**1.2 Purpose**

The purpose of the SAR is to provide the system owner(s), CISO, and security authorization officials with a summary of the security assessment during the security review for FMC. A security assessment has been performed on FMC to evaluate the system’s implementation of and compliance with the organization's baseline security controls. As a federally funded healthcare facility, FMC must ensure it meets all Federal Information Security Management Act (FISMA) compliance mandates.

The organization requires information systems to use internal and third-party assessment organizations to perform independent security assessment testing and documentation of the SAR. Security testing for FMC was performed by the head consultant of Pruhart Security Consulting, Dr. Sophia Martin.

**2 System Overview**

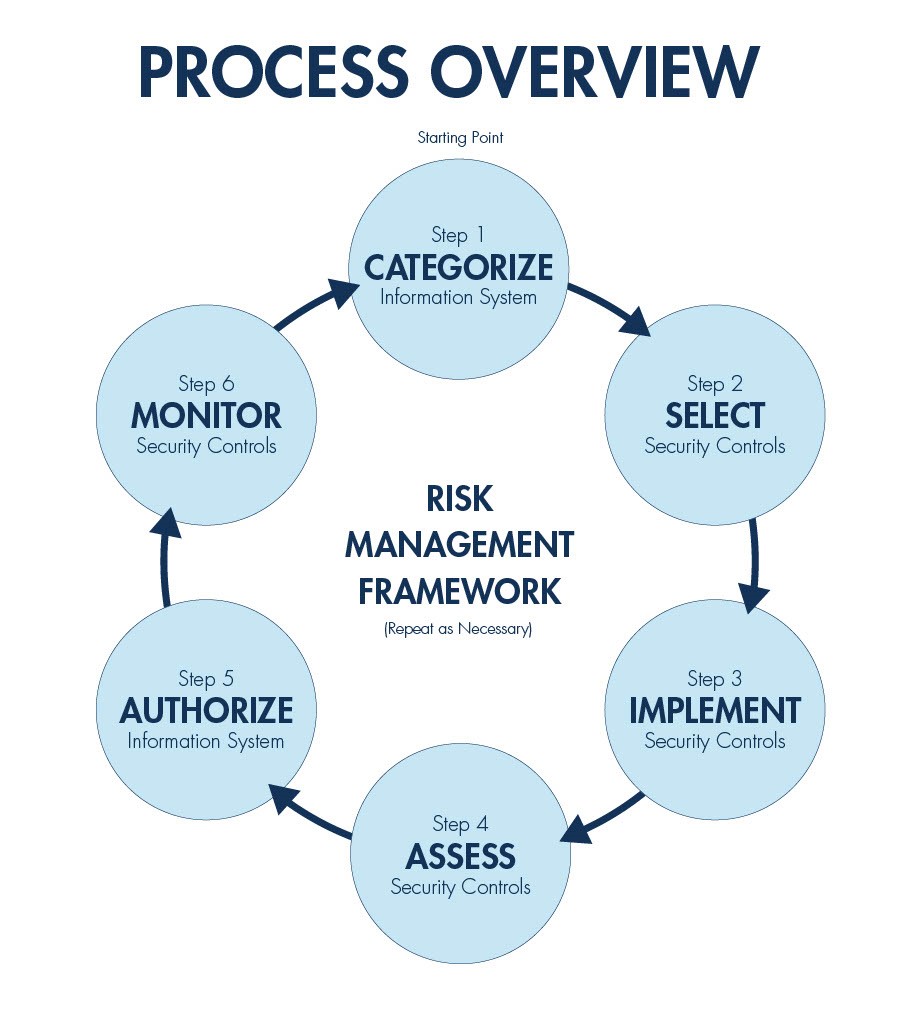
**2.1 System Name**

| **Unique Identifier (UUID)** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| e3dr4fae-10jyn-8510-r781-87y1896e67b7 | FMC Phoenix | FMC-HQ |

**3 Assessment Methodology**

The security assessment uses a logical and prescriptive process for determining risk exposure for the purpose of facilitating decisions, as is aligned with the risk management framework (RMF) described in NIST 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The RMF describes six steps that apply to the system development life cycle. Assessing security controls constitutes Step 4, as illustrated in the figure below:

**Figure 3.0.1: Risk Management Framework**



This methodology, used to conduct the security assessment for FMC’s systems, is summarized in the following steps:

1. Perform tests from the systems security plan (SSP) and record the results.
2. Identify vulnerabilities on the platform.
3. Identify threats and determine which threats are associated with the cited vulnerabilities.
4. Analyze risks based on vulnerabilities and associated threats.
5. Recommend corrective actions.
6. Document the results.

**3.1 Overall Security Findings**

The following findings are based on a risk analysis and gap analysis between the current systems within FMC and their requirements to meet compliance to control families within NIST SP 800-53r5 and high-level requirements of PCI DSS compliance.

The current system does not provide adequate protection as outlined within the Privacy Act. Information stored on FMC systems contains personal identifiable information (PII), including and not limited to name, address, social security number (SSN), and other private information. This information is required to allow authorized government agencies access to this information and artifacts to verify doctor qualifications.

**3.2 Overall Findings Across All Connected Systems**

All connected systems at FMC are aging and in need of review, prioritization, compliance, upgrade, and the development of a maintenance plan. The following control families and/or control enhancements need to be addressed to ensure FMC’s governance and compliance:

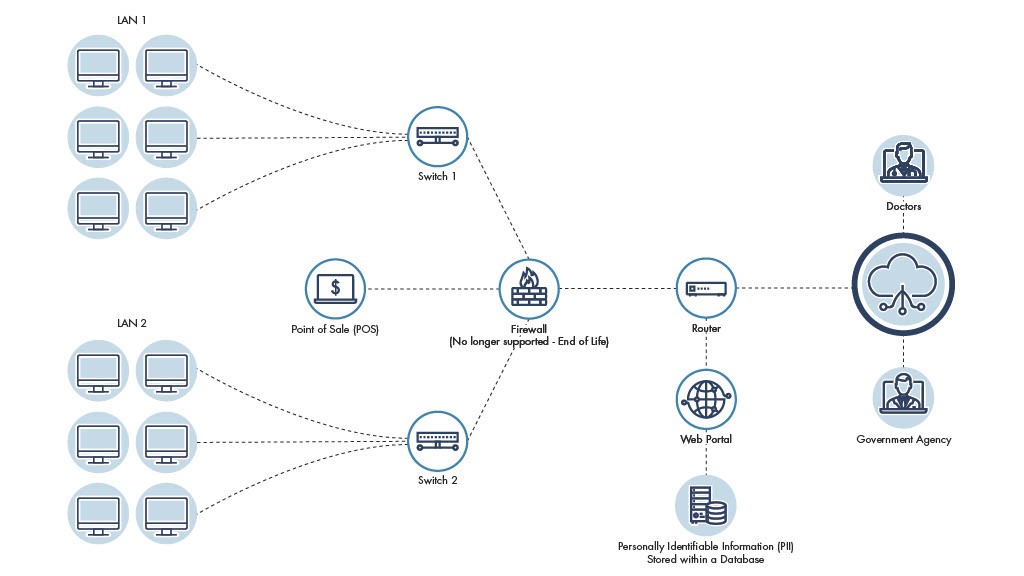
1. During the audit process, we determined that the workstations connected to both switches do not have proper antivirus (AV) protection; specifically, some workstations have unlicensed AV solutions, and others do not have an active AV solution.
2. End-point protection is currently inadequate to protect the network and systems.
3. A multifactor authentication (MFA) is not present on the network.
4. FMC has stated its intent to meet PCI DSS compliance. FMC plans to eventually complete a point-of-sale (POS) system at its physical location for customers to purchase equipment. This POS requires a secure and maintained network, specifically a firewall and the removal of vendor-supplied defaults regarding passwords and other security requirements. In addition, this system is missing an AV solution.
5. Authorized government agencies require secure access to an FMC web portal to review documents and other artifacts to help in the verification process for certified doctors.
6. Doctors use FMC’s services to upload their PII and other artifacts. During our assessment, we determined there currently is no secure process to authenticate doctors on FMC’s network or to protect the PII from unauthorized access.

**3.3 Security and Privacy Control Families/Control Enhancements**

Pruhart Security Consulting was contracted by FMC to identify its security posture on its current system(s), conduct a risk analysis, and disseminate the results of Pruhart Security Consulting findings to FMC stakeholders. A brief gap analysis is provided below based on our findings and recommendations for the new system.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Identifier** | **Control / Control Enhancement** | **Notes** | **Rating** |
| AC-6 | Least Privilege | Least privilege needs to be employed based on duties and systems. |  |
| CA-5 | Plans of Action and Milestones | Develop and track planned remediation actions. |  |
| CA-7 | Continuous Monitoring | A continuous monitoring strategy is required to support business needs and the new system. |  |
| RA-3 | Risk Assessment | An updated risk assessment that identifies and determines the likelihood and impact of risks associated to the new system is required. |  |
| RA-7 | Risk Response | Justification or rationale on mitigation risk strategies based on either remediation or acceptance of risk is required. |  |

**Figure 3.3.1: Network Topology Based on Findings**

****