Written Information Security Policy (WISP) for [Healthcare Organization Name]

Introduction

[Healthcare Organization Name], including its three hospitals and 25 clinics, is committed to protecting the confidentiality, integrity, and availability of all physical and electronic information assets across our organization. This Written Information Security Policy (WISP) establishes the framework for managing and protecting the organization's information assets, ensuring compliance with legal, regulatory, and contractual obligations related to information security.

Scope

This policy applies to all employees, contractors, affiliates, and any other individuals who access, use, or manage the organization's information assets.

Policy Objectives

1. **Information Security Management**
   - Establish and maintain an information security program that is designed to protect the organization's information assets from threats, whether internal or external, deliberate or accidental.
2. **Asset Management**
   - Maintain an inventory of all critical information assets and define appropriate protection responsibilities. Ensure that all assets are classified according to their sensitivity and criticality to the organization.
3. **Human Resources Security**
   - Ensure that all employees, contractors, and third-party users understand their responsibilities and are suitable for the roles for which they are considered. Provide appropriate training and ongoing awareness to ensure compliance with this policy.
4. **Physical and Environmental Security**
   - Protect physical and electronic information from unauthorized access, damage, and interference. Secure physical areas, equipment, and network infrastructure against unauthorized access, tampering, and damage.
5. **Communications and Operations Management**
   - Establish secure management processes and procedures for the effective and secure operation of information processing facilities. Ensure the security of data in networks and the protection of connected services from unauthorized access.
6. **Access Control**
   - Restrict access to information and information processing facilities to authorized individuals based on their role and the principle of least privilege. Ensure that users are provided access for only those processes that they have been specifically authorized to use.
7. **Information Systems Acquisition, Development, and Maintenance**

    - Ensure that information security is an integral part of the information systems across the lifecycle. This includes information systems for new developments and enhancements to existing systems.
8. **Information Security Incident Management**
    - Establish a management process to ensure a quick, effective, and orderly response to information security incidents.
9. **Business Continuity Management**
    - Maintain plans to protect critical business processes from the effects of major failures or disasters and to ensure their timely resumption.
10. **Compliance**
    - Ensure compliance with legal, regulatory, and contractual requirements regarding information security and privacy.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, legal action, and financial liability for damages caused by the violation.

Policy Review and Modification

This policy will be reviewed annually and updated as necessary to reflect changes in technology, security threats, legal, regulatory, and organizational changes.

Acknowledgment

All employees, contractors, and third-party users of information systems and services within [Healthcare Organization Name] are required to acknowledge that they have read and understood this policy and agree to comply with its terms.

This Written Information Security Policy is a cornerstone of [Healthcare Organization Name]'s commitment to secure and responsible information management. Adherence to this policy is essential for protecting the organization's information assets and ensuring the trust of our patients, staff, and partners.