Aas Health Foundation

Swayambhu Apt 2, Near Nasare Sabhagruh,

Hudkeshwar Road, Nagpur – 440034.

Information Security Policy

1. Introduction

Aas Health Foundation (hereinafter referred to as "the Foundation") recognizes the importance of maintaining the confidentiality, integrity, and availability of its information assets. This Information Security Policy establishes the framework for protecting the Foundation's information from unauthorized access, use, disclosure, alteration, and destruction.

The Foundation is committed to ensuring the protection of sensitive data related to its operations, stakeholders, and beneficiaries. This policy sets out the principles, roles, responsibilities, and guidelines for managing information security risks in all areas of the Foundation's activities.

2. Purpose

The purpose of this policy is to:

- Safeguard the information assets of the Foundation against risks such as data breaches, cyber-attacks, and unauthorized access.
- Ensure compliance with relevant laws, regulations, and industry standards regarding data protection and information security.
- Provide clear guidelines for employees, partners, and third parties on how to handle and protect information.
- Foster a culture of information security awareness within the organization.

3. Scope

This policy applies to all information assets, systems, and technologies used by the Foundation, including:

- Electronic and physical data, records, and files.
- Software, applications, and networks.
- Employees, contractors, volunteers, and third-party service providers with access to Foundation information.

4. Information Security Objectives

- **Confidentiality**: Ensure that information is only accessible to authorized individuals or entities.
- **Integrity**: Ensure that information is accurate, reliable, and protected from unauthorized modification or corruption.
- **Availability**: Ensure that information is accessible and usable when needed by authorized parties.

5. Information Security Responsibilities

- **Board of Directors**: Responsible for overseeing and approving the information security strategy and ensuring its alignment with the Foundation's objectives.
- **Information Security Officer (ISO)**: The designated ISO will oversee the implementation of the policy, conduct risk assessments, and ensure the enforcement of security controls.
- **Employees and Volunteers**: All employees and volunteers must adhere to this policy and take reasonable precautions to protect sensitive information.
- **Third-party Service Providers**: Any external entities that access the Foundation's data must comply with the information security policy and enter into binding agreements to safeguard the data.

6. Information Security Principles

1. **Access Control**:
    - Access to sensitive information shall be granted based on the principle of least privilege, meaning that users have access only to the information necessary for their roles.

- All users will be required to authenticate their identity through secure login credentials (e.g., passwords, multi-factor authentication).

2. **Data Classification**:
    - Information will be classified based on its sensitivity and the potential impact of unauthorized access, and security controls will be applied accordingly. Information will be categorized as: public, internal, confidential, or restricted.
3. **Data Encryption**:
    - Sensitive information, especially personal and financial data, shall be encrypted both in transit and at rest to prevent unauthorized interception or access.
4. **Incident Response and Reporting**:
    - The Foundation will maintain an incident response plan to handle security breaches, including the identification, containment, investigation, and remediation of incidents.
    - Employees and stakeholders must immediately report any suspected security incidents or breaches to the designated Information Security Officer or IT support team.
5. **Physical Security**:
    - Physical access to facilities and systems containing sensitive information will be restricted to authorized personnel only.
    - Devices such as laptops, servers, and external storage devices containing sensitive data must be securely stored when not in use.
6. **Data Retention and Disposal**:
    - Data will be retained only as long as necessary for operational, legal, or regulatory purposes. When no longer needed, data must be securely disposed of, either through data wiping or physical destruction of storage devices.
7. **Security Training and Awareness**:
    - All employees and volunteers will undergo regular training on information security best practices, including how to identify phishing attacks, use strong passwords, and secure personal devices.
    - Awareness programs will be conducted periodically to reinforce the importance of information security.

8. **Compliance**:
    - The Foundation will comply with all relevant legal and regulatory requirements concerning information security, including data protection laws (e.g., GDPR, HIPAA), industry standards, and best practices.

7. Risk Management

The Foundation will conduct regular risk assessments to identify potential threats to its information assets and implement appropriate security controls to mitigate these risks. This includes evaluating the impact of various threats such as cyber-attacks, system failures, and natural disasters, and planning mitigation strategies accordingly.

8. Monitoring and Auditing

The Foundation will monitor information systems for any unusual or unauthorized activity. Regular security audits and vulnerability assessments will be conducted to ensure compliance with the information security policy and to identify areas for improvement.

9. Enforcement

Non-compliance with this policy may result in disciplinary action, including termination of employment or contract, and potential legal action. Any violation of information security protocols or failure to adhere to this policy must be reported immediately and will be investigated thoroughly.

10. Review and Updates

This Information Security Policy will be reviewed at least annually or whenever there are significant changes to the Foundation's operations, technologies, or regulatory requirements. Updates to the policy will be communicated to all stakeholders.

11. Contact Information

For any questions or concerns regarding this Information Security Policy, or to report an information security incident, please contact:

Information Security Officer (ISO)

Email: Help@aashealthfoundation.com

Phone: 7304317605
Address: Aas Health Foundation, Hudkeshwar Road, Nagpur, MH – 440034.

Conclusion

Aas Health Foundation is committed to ensuring the highest standards of information security to protect the data and information assets of its stakeholders. All employees, contractors, and third parties must adhere to the principles and guidelines set out in this policy to ensure the ongoing safety and confidentiality of the Foundation's information.