Solution House Software (Pty) Ltd

INFORMATION SECURITY POLICY
of
SOLUTION HOUSE SOFTWARE
and all its subsidiaries
(Hereinafter referred to as SHS)

May 2021

Version: 1.1

1. Introduction

1.1 The Information Security Policy defines the requirements for creating and maintaining a strong information security position through the application of information security controls, information ownership and information protection. Implementation of this policy is intended to significantly reduce risk to the confidentiality, integrity and availability of SHS information systems and resources that enable achievement of SHS's strategic and operational objectives.

1.2 SHS shall establish and maintain comprehensive protection and clear accountability for all its' information assets and resources. This includes information assets that are proprietary to SHS, private to SHS customers and partners, and all other private and proprietary information and assets and resources that, if subject to inadvertent or unauthorized access or disclosure, would likely cause financial, legal, or reputational damage to SHS or its' customers and partners.

2. Policy Objectives

2.1 To protect SHS's information by safeguarding its confidentiality, integrity and availability.

2.2 To establish safeguards to protect the information resources from theft, abuse, misuse and any form of damage.

2.3 To establish responsibility and accountability for Information Security within the organization

2.4 To encourage management and employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.

2.5 To provide suitable coverage of International Standards and related information security best practices.

3. Applicability

3.1 This policy and associated standards, procedures and guidelines apply to all

i. SHS employees
ii. Consultants
iii. Contractors
iv. Sub-contractors

and their respective facilities supporting SHS operations, who use it's services and assets, and where SHS data is stored or processed, including any third party contracted by SHS to handle, process, transmit, store or dispose of data, whether SHS is the data owner or is acting upon the instruction of its' customers.

3.2 This policy is supported by a range of security controls documented within operating procedures, technical controls embedded in information systems and other controls that will be advised to employees from time to time by SHS through information security standards, procedures and guidelines.

4. Roles and Responsibilities

4.1 It is the responsibility of each SHS employee, consultant and contractor to read and understand this Policy as well as the associated procedures and documentation that will implement it.

4.2 Management is accountable for implementing and supporting this Policy and shall ensure that the necessary information security controls are implemented and complied with.

4.3 The Information Officer, as well as SHS and its executive shall:

a. Approve and authorise information security procedures
b. Ensure that all users are aware of the applicable policies, standards, procedures and guidelines for information security
c. Ensure that policy, standards and procedural changes are communicated to applicable users and management
d. Evaluate information security potential risks and introduce mitigating measures to address these risks
e. Revise the information security policy and standards for effective information security practices
f. Facilitate and coordinate the necessary information security procedures within SHS

g. Coordinate the implementation of new or additional information security controls
h. Review the effectiveness of information security measures and implement remedial controls where deficits are identified
i. Coordinate awareness strategies and rollouts to effectively communicate information security mitigation solutions.

5. Definitions

5.1 Governance

The mechanisms an organisation uses to ensure that its members follow its established processes and policies. It is the primary means of maintaining oversight and accountability in a loosely coupled organizational structure. A proper governance strategy implements system to monitor and record what is going on, takes steps to ensure compliance with agreed policies, and provides for corrective action in cases where the rules have been ignored.

5.2 Incident

Any event which is not part of the standard operation of a service which causes, or may cause, an interruption to, or a reduction in, the quality of that service

5.3 Standard

Guideline documentation that reflects agreements on products, practices, or operations by nationally or internationally recognised industrial, professional, trade associations or governmental bodies.

5.4 System

An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective

5.5 User

An individual utilising Information Systems to achieve the business goals required to realise the mandate.

6. Principles

6.1 This policy addresses the associated risks to the information assets and includes risks such as:

a. Uncontrolled access, connections, and unintentional user errors

b. Security of the information systems compromised by unsupported business practices
c. Ensuring the integrity and validity of data
d. Poor operating procedures
e. Malicious code and viruses
f. Uncontrolled system or data changes
g. Internet and public domain access
h. Breach of legislation or non-compliance with a regulatory or ethical standard

6.2 The implemented controls shall be reviewed annually, or more frequently should the need arise. Upon completion of review, the policies will be adjusted where necessary.

7. Application

7.1 Information Security Policy Statements

This section contains formal policy requirements, each followed by a policy statement describing the supporting controls and supplementary guidance.

a. Information Security
- Roles and responsibilities for information security governance shall be identified and a Risk Committee shall be established.
- Third parties will be identified and managed in accordance with a legal contract to ensure that no unauthorised access is gained to SHS – both logically and physically.
- Senior management fully supports and commits to the enforcement of all aspects of security throughout SHS.

b. Asset Management
- All assets shall be protected by the appropriate level of protection. Assets will be handled in line with identified level of criticality.
- Information Asset Owners shall be identified and held accountable for the protection of assets under their authority.

c. Employee Security
- Security education, training and awareness programmes will be conducted to ensure that employees are aware of

security threats and concerns and are equipped to apply the security principles at all times.

d. Physical and Environmental Security
   - Physical and environmental controls shall be in place to protect SHS and its supporting information processing facilities from unauthorised access, intentional or accidental damage or interference.

e. Communications and Operations Management
   - Critical operational procedures such as uptime, security, back-up and recovery shall be documented and implemented to ensure correct and secure operations within SHS and its supporting information processing facilities, communication facilities and networks. Exchange of information will be managed to prevent the loss, modification or misuse of information.
   - All breaches of security shall be reported and managed accordingly.

f. Access Control
   - Access (both locally and remotely) to computers, systems and networks shall be granted in line with requirements.
   - This access will be managed and monitored to ensure that no unauthorised access is gained.
   - The use of mobile computing facilities will be managed to ensure protection of these facilities.

g. Disaster Recovery Management
   - Business continuity management plans and procedures shall be established and maintained to facilitate the normal functioning of critical business activities in the event of failures or disasters.

h. Data Classification
   - Sensitive information
     Information in this category may not be distributed without consideration of its sensitive nature.
     - Confidential information is SHS information normally handled in the same manner as private information, but may be accessed by other authorised employees under limited additional circumstances.

- Public Information
  Information in this category is distributed without restriction. Examples: Marketing materials, Municipality website

i. Information Handling
   - Unauthorised disclosure of sensitive information is prohibited.
   - Unauthorised tampering or alteration of sensitive information is prohibited.
   - Unauthorised destruction or disposal of sensitive information is prohibited.
   - Laws and policies governing information retention must be complied with.
   - When confidential information is being transported or stored, it must be protected from unauthorised disclosure, modification, or destruction.
   - If encryption is not possible appropriate compensating controls must be considered and implemented.
   - Before access is granted to confidential information, a signed non-disclosure agreement must be on file for that individual or organisation.
   - When appropriate, criminal and reputational background checks must be conducted.
   - Confidential information being transported to or stored with a third party outside of the SHS cloud services or physical premise must be approved by the Information Owner.
   - Confidential information, both digital and physical, must be disposed of properly to prevent unauthorised disclosure.

j. Identity and Access
   - Information users will be given the minimum level of access to systems and information that their duties require.
   - Human Resources must report change of an employee employment status or role to other organizational stakeholders immediately.
   - Remote access to the network or systems is will be logged and monitored where appropriate.
   - Passwords, pass-phrases, and private keys (physical and private digital) must be protected, and may not be shared.

k. Information Compromise
   - Should it be suspected that sensitive data has been accessed by an unauthorised party or has been used

improperly by an authorised party, then the discovering individual must report the incident immediately to the Information and Compliance Officers
- Should a password, pass-phrase, or key be believed to have been compromised, it must be changed immediately. If that password authorises access to sensitive information, the incident must be reported.

l. Infrastructure
- Infrastructure must be protected from theft, intrusion, malicious code, and abuse.
- It must be regularly patched for security and stability.
- Locations that house digital and paper copies of confidential data must have appropriate physical preventative, detective, and deterrent controls.
- Infrastructure must be reinforced with appropriate redundancy, backup, and disaster recovery plans and technologies.
- A layered security strategy must be applied to information, network, and system architecture and design whenever possible, especially pertaining to sensitive information.

m. Assessment and Compliance
- Risk assessments must be regularly conducted to reveal security posture, and to identify vulnerabilities and weaknesses in software, infrastructure, policy, procedure and practices
- Employees must participate in information security awareness that will be provided by SHS.
- Controls shall be in place to ensure compliance with legal, legislative, regulatory or contractual obligations and any other security requirements.

n. Intended Use Guidelines for Corporate Electronic Messaging Systems
- Users shall not use SHS's e-mail systems to display or communicate disruptive, destructive, unproductive, inappropriate or objectionable material.
- Personal use of SHS's e-mail systems is discouraged to the extent that such use would, in management's judgment:
  - Become excessive or create a distraction
  - Limit one's ability to achieve SHS's business goals
  - Introduce information security risks

  - Introduce disruptive, destructive, unproductive, inappropriate or objectionable elements to the work place
  - Does not subject the company, its customers or its stakeholders to information security risks
- SHS's IT Department provides each user a server-based storage location for electronic messages and takes technical and administrative precautions to ensure that other peer users cannot access that location.

8. Compliance and Enforcement

8.1 Violation of this policy, will lead to restriction of access to information, and disciplinary action or penalty

8.2 Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual will be the responsibility of that user or that individual. The penalty, thereof, will be determined by the SHS disciplinary process.

8.3 SHS may use any legislation relevant to the usage or protection of Information Systems (or information), in prosecuting the person who has violated this policy.

9. Policy Review

This policy shall be reviewed on at least an annual basis to

a. Determine if there have been changes in International, National or Internal references that may impact on this policy.
b. Determine if there are improvements or changes within the SHS systems or processes that should be reflected in this policy