INFORMATION SECURITY POLICY

1. Introduction

Purpose

This document defines the Sankash Private Limited's (the "Company") position on information security. The policy is applicable across the Company and is also subject to amendment at any time depending upon the changes in business requirements or environment with requisite approvals.

The primary objectives of this policy and security program are:

- Manage the risk of security exposure or compromise of the Company information assets;
- Reduce opportunities for the introduction of errors in information assets supporting the Company business processes;
- Provide management direction and support for information security, Support the security requirements of the business.

Scope

This Information Security Policy applies to all information assets of the Company, in any format whatsoever, as well as the processes and systems that support them. This policy is applicable to entities, staff and all others who have access to or manage the Company's information.

Information security refers to the protection of information from accidental or unauthorized access, destruction, modification or disclosure.

This policy must be communicated by supervisors to all employees and all others who have access to or manage the Company information.

Owner

The Board of Directors is the owner of this policy and will be responsible for reviewing and updating the policy as and when required based on the change in the business requirements or environment. The board will also ensure that the updated policy is implemented across the organization.

Document Structure

This document is structured following security categories of ISO 27001 standard:

- Security Policy;
- Organizational Security;
- Asset Classification and Management;
- Human Resources Security;
- Physical and Environmental Security;
- Operation Management;
- Communications and Network Management;
- Access Control;
- Information System Acquisition, Development and Maintaince;
- Information Security Incident Management;
- Business Continuity Management;
- Compliance;

2. Information Security Policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Information Security Policy Document

The information security policy will provide management direction and support to information security. The information security policy will be communicated throughout the Company in a form that is relevant, accessible and understandable to the intended audience. The policy will explain the policies, principles and compliance requirements for particular importance to the organization.

Review of Information Security Policy

Major changes in the IS Policy will need approval from the Information Security Counsil. The Information Security Council (ISC) will be formed comprising of senior management representation of the Company. Information Security Counsil is required to take further approval from the Company's Board of Directors and will put up the proposal to the Board accordingly.

Minor changes in day-to-day activities/ functions/ procedures will be approved by the ISC.

3. **Organisational Security**

Objective: To manage information security within an organization.

Internal Organization

The Information Security Management System will enforced by:

- Establishing a management framework to initiate and control the implementation of information security within the Company;
- Ensuring that a governance framework is developed to maintain information security within the Company;
- Assigning the security roles and co-ordinating the implementation of security across the Company.

Management will approve the information security policy, assign security roles and co-ordinate and review the implementation of security.

Management to Information Security

The Information Security Council (ISC) will be formed comprising of senior management representation of the Company. The roles and responsibilities will include:

- Periodic review of information security;

- Review of security incident monitoring processes within the Company;
- Approval and review of information security projects;
- Approval of new or modified information security policies;
- Performing other necessary high-level information security management activities.

Confidentiality/Integrity/Availability

All information will be protected from unauthorized access to help maintain information‟s confidentiality and integrity.

Information will be readily available for authorized use as needed by the user in the normal performance of their duties. Appropriate processes will be implemented to ensure the reasonable and timely recovery of information, applications and systems.

External Parties

The risks associated with access to the Company's internal systems by third parties will be assessed and appropriate security controls implemented.

When using an external contractor to manage information processing facilities, risks will be identified in advance, mitigating controls will be identified and established, and contractor expectations will be incorporated into the contract for these services.

4. Asset Classification and Control Policy

Information Management

Information, like other assets, must be properly managed from its creation, through authorized use, to proper disposal. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Information will be classified according to its value, sensitivity, consequences of loss or compromise, and legal and retention requirements.

A person will be responsible for assigning the initial information classification and make all decisions regarding controls, access privileges of users, and daily decisions regarding information management. Periodic high-level business impact analyses will be performed on the information to determine its relative value, risk of compromise, etc. Based on the results of the assessment, information will be classified into one of Company information classifications, where appropriate.

Each classification will have a set or range of controls, designed to provide the appropriate level of protection of the information and its associated application software commensurate with the value of the information in that classification.

Privacy and Handling of Private Information

The Company holds personal identifiable information to carry out the business. The protection of the privacy of personal information is of utmost importance and Company must conduct business so as to protect the rights of privacy of all members of the public.

Personal data, including information about students, employees, members of the public, organizations and business partners, collected and maintained by the Company must:

- Be used only for the stated purpose for which it was gathered;
- Be gathered in lawful and fair circumstance;
- Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose.

Release Private Information to Third Party

The Company will take prior permission of Information Provider before disclosure of personal information to the third party.

The Company will allowed to release Personal Information to Government agencies mandated under the law for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.

The Company may transfer sensitive personal information, including any information, to any other body corporate or a person in India, or located in any other country, The Company will ensure that same level of data protection is adhered to by the Third Party.

5. Human Resource Security

Objective: To ensure that users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Prior to employment

The Company will carry background screening, as required for the role, on permanent staff will be carried out at the time of job applications. A similar screening process shall be carried out or incorporated as part of the contract for contractors and temporary staff in accordance with the Risk Assessment of the External Parties.

During employment

The Company will require employees, contractors and third party users apply security in accordance with Company's established policies. The Company will ensure that information security within their departments is treated as mandatory and employees are encouraged to adhere to Company's information security policies. All employees of the organization and, where relevant, third-party users will receive appropriate training and regular updates in Companies policies and procedures.

Termination of employment

Human Resources will notify about the transfer or termination of any employee and any other third party personnel or contractors of the organization without delay.

The system user IDs will be disabled after an employee has permanently left the Company. Company property, including, but not limited to, portable computers, library books, documentation, building keys, magnetic access cards, etc. will be returned at the time when an employee leaves the organization.

6. **Physical and Environmental Security**

Company's information processing facilities must be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls to protect from unauthorized access, damage and interference. Physical security perimeters should be established in Company's environments where servers are stored or operational in wiring closets for network and telephone connections, where printers used for printing confidential or sensitive information, and any other location where critical or sensitive Company's computer equipment may be in use or stored. The purpose of the security perimeter is to prevent unauthorized access to the computer resource, or to prevent theft of the resource.

Sensitive information must be removed from view and physically secured when not in use. Measures must be taken to insure that such information cannot be read or copied by unauthorized persons. Physical security of the machine when unattended is one approach. The use of computer screen savers or similar technology is required to ensure that sensitive information is not displayed after a specified period of inactivity. When unattended or physically unsecured for more than a few minutes, all computers must be locked.

7. **Operation Procedure and Responsibilities**

Responsibilities, processes and procedures should be established and documented for the management and operation of all information processing facilities. This includes the development of appropriate operating instructions and incident response procedures.

Operating procedures for the Company’s systems and applications should be documented and maintained. Documented procedures should also be prepared for housekeeping activities associated with information processing and communication facilities such as computer startup and shutdown procedures, back-up, equipment maintenance, computer room management and safety.

Operational Change Control

Changes to Company’s administrative information processing facilities and systems must be authorized and controlled through a change management process with appropriate checks and balances. Formal management responsibilities and procedures ensure satisfactory control of all changes to equipment, software or procedural documentation. Operational software will be subject to strict change control. When programs are changed, an audit log containing all the relevant information will be created and maintained.

Incident Management Procedures

An incident management process will be established to track the types, volumes and costs of security incidents and malfunctions. This information will be used to identify recurring or high impact incidents and to record lessons learned. This may indicate the need for additional controls to limit the frequency, damage and cost of future incidents, or to be taken into account in the policy review process.

All users Company’s systems should be made aware of the procedure for reporting security breaches, threats, weaknesses, or malfunctions that may have an impact on the security of Company information. All Company staff and contractors are required to report any observed or suspected incidents to local management as quickly as possible.

Incident management responsibilities and procedures will be clearly defined and documented to ensure a quick, effective and orderly response to security incidents.

The Company will investigate significant security incidents and implement corrective actions to reduce the risk of re occurrence.

Segregation of duties

All the mutually exclusive roles and corresponding access permissions will be identified and reviewed annually.

Whenever a Company computer-based process involves sensitive information, the system will include controls involving separation of duties or other compensating control measures that ensure that no one individual has exclusive control over these types of information assets.

Separation of development, test and operational facilities

Separate people will perform production application source code development and maintenance, production application staging and operation, and production application data manipulation.

Production business application software in development will be kept strictly separate from this same type of software in testing through physically separate computer systems or separate directories or libraries with strictly enforced access controls.

Employees who have been involved in the development of specific business application software will not be involved in the formal testing or day-to-day production operation of such software.

System Planning and Acceptance

System and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. Requirements for new systems must be established, documented and tested prior to their acceptance and use. Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing capability and storage are available.

Acceptance criteria based on best practices for new information systems, upgrades and new versions of existing systems must be established. Suitable tests will be performed to ensure requirements have been met prior to formal system acceptance

Third party service delivery management

The Company will reserve the right to immediately terminate network connections with all third-party systems not meeting the information security requirements.

All agreements with organizations providing services to the Information Security function will stipulate that the Company will have the right to audit the information security controls implemented.

Third-party vendors will be given only in-bound connection privileges when the Company determines that they have a legitimate business need.

Protection against malicious and mobile code

Malicious software checking systems will run continuously on all personal computers, local area network servers, firewalls, and on electronic mail servers. All files coming from external sources will be checked before execution or usage.

All files containing software or executable statements will be verified to be virus free prior to being sent to any third party. Before any files are restored to a production Company computer system from backup storage media, these will be scanned with the latest version of the virus screening software.

Back-up

Backups of critical Company's data and software are performed regularly. A threat and risk assessment is performed at least annually to determine the criticality of business systems, and the time frame required for recovery. Processes will be developed to back-up the data and software. Restoration of data is tested periodically. Formal disaster recovery plans for each critical Company's application will be developed, documented and tested periodically. Test results will inform changes to disaster recovery plans.

Media Handling

Removable media such as disk and backup tapes must be labeled clearly. Media would be classified based on the sensitivity of the data stored in it.

Media will be disposed depending on the sensitivity of the information contained in it. Information on media will be erased securely if the media is to be reused.

All movements of media, in and out of an organization, will be recorded. Security measures will be taken when media containing sensitive information is sent.

Monitoring

All production application systems that handle sensitive Company information will generate logs that capture every addition, modification, and deletion to such sensitive information.

Computer systems handling sensitive, valuable, or critical information will securely log all significant security relevant events including, but not limited to, password guessing attempts, attempts to use privileges that are not authorized, modifications to production application software, and to system software.

A formal problem management procedure will be in place to record the security problems, reduce their incidence, and to prevent their recurrence.

8. Communications and Network Management

Network Management

The Company will implement a range of network controls to maintain security in its trusted, internal network, and to protect connected services and networks. The network includes any device that is attached via a wired or wireless connection with an IP address.

Host Scanning

The Company reserves the right to scan any device attached to its network on a periodic basis to ensure optimal configuration to protect against known vulnerabilities.

Network Security Checking

Network vulnerability scans will be conducted periodically on systems that are essential to supporting a process that is critical to the Company’s business and annually on all other systems. The vulnerability scanning process is followed and tested at all times to minimize the possibility of disruption to the Company’s networks by such reviews.

Penetration and Intrusion Testing

All production computing systems that provide information to external parties, either directly or through another service that provides information externally, will be subjected to penetration analysis and testing. A suitably qualified evaluation team or authorized third party will test to validate potential vulnerabilities.

Only authorized administrators will perform penetration testing and Company must approve each test. Any other attempts to perform such tests or to determine how a system may change or behaves under abnormal circumstances, whether successful or not, will be deemed an unauthorized access attempt and will result in disciplinary or legal action.

Internet and Electronic Mail Acceptable Use

All uses of the Company's network and of Company's electronic mail facilities will be within the bounds of the Companys Computer and Network Authorization and Use policy.

Connections to Third Party Networks

A risk analysis will be performed to ensure that the connection to the third party network will not compromise the Company's network. Controls, such as the establishment of firewalls will be implemented between the third party and the Company to protect the Company's networks. These connections will be periodically reviewed or tested by the Company.

Security of Electronic Mail

Electronic mail is inherently not secure and should not be used to transmit highly sensitive/confidential information, due to the security risks.

Portable Computing Devices and Information Media

Highly sensitive (confidential) data should never be in unencrypted format on portable computing devices and information media. When using portable computing devices (e.g. laptops, smart phones, personal data assistants) to access information special care must be taken to ensure that device and information accessed by that device is not compromised.When accessing databases containing confidential information the mobile device user must be careful to never save data to the local hard- drive or other mobile storage device.

Remote Access

Remote connection to the Company's networks is allowed only through a Virtual Private Network (VPN) maintained by Company's business use access when remote work-related business is an absolute necessity.

9. **Access Control Policy**

Objective: Access Control systems are in place to protect the interests of all users of The Company computer systems by providing a safe, secure and readily accessible environment in which to work.

Business requirement for Access Control

The Company will ensure that access to its information and business processes is controlled as per the business and security requirements. Access to Sensitive information will be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the Information Owner.

User access management

The Company will have defined operating instruction for managing logical access controls for business applications, information services and data. These will encompass the new user creation to user de-registration and will include specific instruction to deal with name changes, transfers, temporary staff, contractors, third party and employees who have resigned/ terminated from the services of the Company. This will also include privilege id management, periodic review of access rights and the implementation of password controls.

User Responsibilities

Most vital aspects of security mechanism are user awareness. The user will be educated about the significance of password security, ways of compromising passwords, perils in sharing password with other users, user responsibility in guarding passwords, etc. Users will be responsible to keep personal password confidential.

Network access controls

The Company will enforce adequate control to ensure that connected users or services have access only to those services for which they are authorized and the do not compromise the security of any other network services.

Every sensitive and high-reliability system managed by or owned by the Company will have its own dedicated computers and networks.

All Company internal network devices, including, but not limited to, routers, firewalls, and access control servers, will have unique passwords or other access control mechanisms.

Operating system access control

The Company will have its own operating system access control to make sure that only authorized user and services access the Operating System.

The Company will have its own procedure to access in the Operating System. A unique user ID will be created for any new Information System access request based on their stated business needs and security constraints. The Company will provide unique password management system.

Application and Information access control

All computer-resident information that is sensitive, critical, or valuable will have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

Access will be restricted for programs or system utilities that can dynamically alter data to those people who demonstrate a business need.

User privileges will be defined such that ordinary users cannot gain access to, or otherwise interfere with, either the individual activities or the private data of other users.

Mobile Computing

The Company acknowledges the need for facilities like mobile computing and teleworking in the current competitive and technology oriented era. Such facilities will be granted to users with prior approval.

The Company will set up an adequate control framework to address the potential risks involved in such a set up like the safety of the equipment, confidentiality and integrity of information stored by the equipments, unauthorized access to Company network, security of data travelling through public networks, etc.

10.Information System Acquisition, Development and Maintaince

Object: To ensure that security is conceived and implemented at the right time in a cost- efficient manner. The Company will ensure that adequate and reliable control mechanism is defined prior to the development of IT system or prior to the evaluation of new software packages or enhancement to existing system.

Security requirement of system

Before a new system is developed or acquired, the Company will clearly specify the relevant security requirements. Business requirements for new systems or enhancements to existing systems will specify the required security controls. While identifying required controls the Company will consider the business value of the information assets involved, potential damage that may occur as a result of failure.

All software developed in-house to process sensitive, valuable, or critical information such as production systems, will have a written formal specification.

The Company may seek assistance of external security specialist for defining the control requirement.

Correct processing of applications

The Company will ensure that appropriate input data validation controls are existing/built-in the systems, prior to their deployment in the production environment.

Privileges will be established such that system users are not able to modify information data in an unrestricted manner. All the critical transactions will be logged and reviewed periodically based on the criticality involved.

Cryptographic controls

The Company will consider data encryption for highly sensitive and critical information that will be identified through risk assessment. The encryption type and other implementation details will be decided after taking into account relevant legislation and the controls applicable to data transmission.

Security of System files

Access to system files will be controlled to ensure that IT projects and supporting activities are carried out in a secured manner. Responsibility to protect integrity of system files will reside with the respective owners.

Security in development and support process

The Company will remain distinct environments for development, test and production to ensure integrity of application software and date. Theses environments will be for a specific purpose only.

Business application software in development will be kept strictly separate from production application software through physically separate computer systems or separate directories or libraries with strictly enforced access controls.

Every non-emergency change to production systems will be shown to be consistent with the information security architecture and approved by management as part of the formal change control procedure.

All Company networked production systems will be adequately-staffed for expediently and regularly reviewing and installing all newly released systems software patches, bug fixes, and upgrades online with the host hardening checklist.

Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers will go through the established change management procedure.

Third parties who develop software for the Company will be bound by a contract.

Technical vulnerability management

The Company will be responsible for the technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching and asset tracking. Before installing patches, the risks associated with installing the patch will be assessed.

Patches for production information systems will be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.

11.Information Security Incident Management

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Reporting information security events and weaknesses

The Company will establish a framework for reporting, responding to an escalating information security event, configure the same in the incident management system. All employees, contractors and third party users will be responsible for reporting all identified security events and incidents promptly.

The Company will establish an incident management procedure for reporting, responding to an escalating any suspected security weakness or threat to systems or services. Users will report all information security alerts, warnings and suspected vulnerabilities to the management, in a timely manner, and will share such information with only by authorized personnel. Employees will promptly notify management of all conditions that could lead to a disruption of business activities.

Management of information security incidents and improvements

Management will establish a procedure to ensure an effective, timely and orderly response to information security incidents. Information security incidents will be monitored and analyzed on a weekly basis. Incidents with high business impact will be identified and appropriate controls will be enhanced to reduce the risk of future occurrences of such incidents.

All internal investigations of information security incidents, violations, and problems, will be conducted by authorized staff.

12.Business Continuity Management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Information Security Aspects of Business Continuity Management

A managed process for development and maintenance of business continuity will exist throughout the organization. The following key components of Business Continuity Management will be considered: Identification of critical business processes, Risk assessment and Business impact analysis, Preparation of Business Continuity Plan (BCP), Regular testing and maintenance of BCP.

Business Continuity and Risk Assessment

- The management will conduct a formal risk assessment and business impact analysis to determine the requirements of BCP. Respective functional teams will conduct the impact analysis and identify the causal threats and assess the impact keeping in view the classification of information assets within the process. Risk will be assessed as a function of the threat probability and business impact.
- Business impact analysis will be carried out to evaluate the acceptable downtime of all the critical business application systems & processes and their impact on the business.
- Risk and business impact assessment will be reported by the process owners to the Information Security Council (ISC).

Developing and implementing continuity plans including information security

Business continuity plans will be developed based on the risks faced by the organization. The BCP will assist in counteracting interruptions to business activities, to protect critical business processes from the effects of major failures or disasters, and to continue business operations during the contingency period.

Business Continuity Planning Framework

- A single common framework shall be followed in drafting continuity plans as per business requirements, which will include the key stakeholders, including third parties. The risks and business impacts shall be considered in developing and updating the business continuity strategy of the company. The framework shall include, but not be limited to: Disaster Recovery Plan, Business Resumption Plan, Crisis Management Program, Testing and maintenance program.
- The plan will include established emergency procedures, existing fallback arrangements for computer services, telecommunications and accommodation/facilities. Further, each plan will specify the conditions for activating the plan and the individuals responsible for executing the plan. Also, the plan will include business resumption (migration) procedures, and a test schedule for the plan.
- BCP will be issued to identified and authorized personnel only. Adequate education activities will have to be conducted to create understanding and awareness about the business continuity plan. BCP will include the roles and responsibilities to be performed by the contingency team members, in the event of a contingency.

Testing, Maintenance and Reassessing Business Continuity Plan

The BCP will be tested on a yearly basis to ensure the practicability and workability of the plan. Further, the plan will be reviewed on a yearly basis, and updated to reflect all the changes in the identified critical business processes.

Crisis Management

Business continuity plan shall comprise of a crisis management program.

13.Compliance

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

Compliance with legal requirement

All relevant statutory, regulatory and contractual requirements will be defined explicitly and documented for all information processing facilities.

The Company will be the legal owner of all business information stored on or passing through its systems, except the information clearly owned by third parties. Software and hardware will be used in compliance with all legal, statutory, regulatory and contractual compliance and after due authorization.

Intellectual property rights (IPR)

- The Company will be the legal owner of all business information stored on or passing through its systems, except the information clearly owned by third parties;
- All intellectual property, such as patents, copyrights, inventions, etc., developed by a user while employed by the Company, will be the property of the Company;
- At the time of termination of their relationship with the Company, all employees will return any intellectual property provided or developed during the period of the person's employment;
- All Company intellectual property will be classified as per the Company's data classification policy and labelled and handled as per Company policies;
- Software and hardware will be used in compliance with all legal, statutory, regulatory and contractual compliance and after due authorization.

Compliance with Security policies and standards, and technical compliance

The company will prepare an annual plan to ensure its computer and communications systems are compliant with this policy.

The Company will an annual review and random tests of production computer system backup processes. The Technical compliance check will be regularly carried out, which involves examination of operational systems to ensure that hardware and software controls have been correctly implemented.

Data protection and privacy of personal information

The company will implement controls for collecting, processing, and disseminating personal information.

Only select authorized personnel will have access to such information. The security controls will address:

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and properly;
- Ensuring that information is accurate, complete and up-to-date, adequate and relevant;
- Compliance with individual's rights, such as subject access and also in Compliance with the relevant data protection/ privacy regulations.

Prevention of misuse of information processing facilities

Company's information systems will be used only after authorization from management and for business purposes only. The Company will not be responsible for the safe keeping of any personal data on its systems.

Information system audit considerations

Internal Audit will review the adequacy of information system controls and compliance with such controls annually. Internal Audit will conduct annual compliance checks related to this information security policy.

Programming source code and its related technical analyses used to compromise security will be disclosed only to authorized personnel with a justifiable business requirement. All information assets directly connected to the Internet must be subjected to periodic risk assessment performed.

Non Compliance

Failure to comply with the Information Security Policy, result in disciplinary action.