POLICY DOCUMENT

20 MARCH 2017

INFORMATION SECURITY POLICY

DOCUMENT CONTROL

Organisation	Shank International Pte Ltd
Title	Information Security Policy
Author	Nandprasad Shiwsaakar
Filename	Shank International Pte Ltd Info Security Policy
Owner	DPO
Subject	Information Security Policy
Review date	05 Jul 2016

REVISION HISTORY

Revision Date	Revised by	Previous Version	Description of Revision

DOCUMENT DISTRIBUTION

This document will be distributed to:

Name	Job Title	Email Address

CONTRIBUTORS

The following individuals/groups contributed to the contents of this document

- Straits Interactive Pte Ltd
- HR. Finance, Admin, and Operations

POLICY STATEMENT

Shank International Pte Ltd ("SIPL" or "the Organisation") is committed to ensuring the proper protection of all information assets within its possession.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

PURPOSE

Information is a valuable asset that SIPL has a responsibility and requirement to protect, especially with regards to complying with the Personal Data Protection Act. The objectives of this policy are as follows:

- Protecting the Organisation's business information and all client or customer information within its possession;
- Establishing minimum principles or safeguards to protect the Organisation's information resources from loss, theft, destruction, unauthorised manipulation, unauthorised disclosure, or unavailability; and
- Establishing responsibility and accountability for Information Security in the Organisation.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Security Policy addresses all these areas to ensure CIA: i.e. Confidentiality, Integrity and Availability.

The following policy details the basic requirements and responsibilities for the proper management of information assets at SIPL. The policy specifies the means of information handling and transfer within the Organisation.

SCOPE

This Information Security Policy applies to all groups of **People** (including consultants, advisors, agents, associates and part-timers), Business **Processes** and all **Systems** that make up SIPL's Information Systems. This includes all Management, Departments, Partners, Employees, Consultants/Advisors, Associates, contractual third parties and agents of the Organisation who have access to Information Systems or information used for SIPL's business purposes.

DEFINITION

This policy should be applied whenever 's Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper
- Data stored electronically (including in mobile devices)
- Communications sent by post / courier or using electronic means
- Stored tape or video
- Speech

RISKS

At SIPL, we recognise that there are risks associated with users accessing and handling information in order to conduct its official core business as it relates to five main areas:

- Prospecting for Clients
- Client's Needs Analysis & Proposal to Client
- Application to Insurers/Manufacturers/Providers
- Processing & Administration of Application
- Completion & Delivery of Policy

Documents This policy aims to mitigate the following risks:

- The non-reporting of information security incidents;
- Criminal Activity such as breaches from past or present employees / associates (human error, sabotage, theft, fraud, insider trading, negligence, workspace revenge, liability for employee actions, lawsuits against employer, etc);
- Outages that result from a component of the information system going offline as a result of an attack;
- Unauthorised access which may lead to improper modifications, disclosures or deletions (which may apply to e- mails, databases or confidential reports);
- Lost Assets (money, data) resulting from theft, breach or improper disposal techniques;
- Hacking and software viruses (worms, viruses, Trojans, malware, password cracking and other system penetration);
- Actions from competitors (industrial espionage, intellectual property theft, copyright / patent infringement, price surveillance, etc);
- Improper or negligent usage of office equipment/software/systems (e.g. weak passwords, unattended printouts from fax machines, photocopiers, scanners, etc);
- Inadequate destruction or disposal of data.

Non-compliance with this policy could have a significant effect on the efficient operation of SIPL and may result in financial loss, loss of reputation/goodwill and an inability to provide necessary services to our customers.

APPLYING THE POLICY

For information on how to apply this policy, readers are advised to refer to Appendix 1.

For effective implementation of this policy, the following players with their respective roles and responsibilities are necessary:

DATA OWNER	The person or organisational entity that owns the personal data and has following accountabilities: • Protection and safeguarding of the data • Retention, archiving, retirement or disposal of the data • Accuracy of the data • Access control over the data (i.e. who can have access to what data) • Disclosure of the data (i.e. which third party can have access to what data) • Granting of permission for the verification and correction of the data by the Data Subject • Transfer of the data overseas *Example of Data Owner: Head of Department or Functional Manager*
DATA COLLECTOR	The person or organisational entity that has the responsibility to collect the personal data from Data Subjects either as the Data Owner or as the assignee of the Data Owner. Has responsibility for notifying the Data Subject of the purpose of collecting, using and disclosing the personal data, and obtaining the consent from the Data Subject. *Example of Data Collector: Consultant/Advisor, HR staff*
DATA USER	The person or organisational entity that uses the personal data after having been granted access by the Data Owner. The Data Owner and the Data Collector can also be their own Data User. *Example of Data User: Anyone authorised by the Data Owner*

DATA INTERMEDIARY	The person or organisational entity that has responsibility for collecting, processing, transmitting or transferring personal data on behalf of the Data Owner or Client/Customer. The Data Intermediary may also be the Data Collector. The Data Intermediary may not be the Data User. *Example of Data Intermediary: Outsourced payroll processing; consultant/advisor forwarding client's personal documents to insurers to assess eligibility for insurance scheme*
DATA CUSTODIAN	The person or organisational entity that has assigned responsibility from the Data Owner for custodian the personal data using technology, IT systems or physical means. Has responsibility for the following: • Organising the data in easily accessible databases and data structures • Cataloguing the physical documents and files containing personal data • Implementing secure measures and security systems to protect and safeguard the data • Ensuring integrity of the data and databases • Making data access available to authorised Data Users • Making data transmission and transfer available to authorised Data Intermediaries *Example of Data Custodian: IT Department, Document Librarians*

POLICY COMPLIANCE

If any user is found to have breached this policy, he/she may be subjected to SIPL's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from **DPO**.
In the event that you have knowledge of anyone who may be breaching this policy, please contact **DPO**.

POLICY GOVERNANCE

The following table identifies who within SIPL is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	CEO and DPO
Accountable	DPO
Consulted	HR, Finance, Admin and Ops Departments
Informed	All employees.

REVIEW AND REVISION

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by CEO and DPO.

REFERENCES

The following SIPL policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy
- Internet Acceptable Usage Policy
- Software Policy
- Computer, Telephone and Desk Use Policy
- Remote Working Policy
- Removable Media Policy

APPENDIX: APPLYING THE POLICY

A1) ORGANISATIONAL SECURITY AND ACCESS CONTROL

IDENTIFYING INFORMATION ASSETS

DESCRIPTION/RATIONALE

At the outset it is important to identify all the important information assets belonging to the Organisation, especially those pertaining to personal data. This is to enable the Organisation to implement appropriate policies and practices to govern the management and protection of such information assets organisation-wide.

RISK/EXPOSURE

Without an organisation-wide view of what important information assets the Organisation owns or is responsible for, the Organisation could be susceptible to loss or theft of information assets, unauthorised access to confidential information, or criminal activity related to malicious attack on the information assets.

PREVENTIVE MEASURE/ACTION

The process of identifying important information assets should be sensible and pragmatic. Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records
- Computer databases
- Data files and folders
- Software licenses
- Physical assets (computer equipment and accessories, tablets, mobile phones)
- Key services
- Key people
- Intangible assets such as reputation and brand

The Organisation must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. The inventory list must be updated periodically to include new information assets acquired and exclude those that are no longer required for business or legal purposes.

CLASSIFYING INFORMATION

DESCRIPTION/RATIONALE

On creation, all information assets must be assessed and classified by the owner/department according to their content. As a minimum, all restricted and confidential information assets must be classified and labelled accordingly, so that appropriate measures can be put in place to protect and restrict access to each class of information asset.

RISK/EXPOSURE

Without proper classification of information assets, the level of security and protection accorded may not be commensurate with the level of confidentiality of the information. This could result in accidental/unauthorised access to or viewing of confidential information, or misuse/mishandling of confidential documents.

PREVENTIVE MEASURE/ACTION

The classification of information assets should be evaluated based on:

- Sensitivity and Confidentiality
- Potential Liability
- Intelligence Value
- Criticality to the business

The classification will determine how the document should be protected and who should be allowed access to it. The way the document is handled, published, moved and stored will be dependent on the classification.

The classes are:

- UNCLASSIFIED
- CONFIDENTIAL

All of the Organisation's information must be adequately protected according to its information classification. All Users have a responsibility to safeguard information in all forms, from its creation through its useful life to its authorised disposal. The Information Owner at each stage of the Organisation's business process is responsible for the protection of the information used at that particular stage.

RETENTION OF RECORDS

DESCRIPTION/RATIONALE

The Organisation/relevant departments should not retain any records of personal data that are no longer relevant or being used for any legitimate business, legal or statutory purposes.

RISK/EXPOSURE

Retaining records of personal data beyond their useful legitimate purposes may result in misuse of the information that is no longer relevant or outdated.

PREVENTIVE MEASURE/ACTION

The Organisation/relevant departments may retain personal data for tax, audit and other business and legal purposes (as stated in the Data Protection Policy). The considerations will be based on the record types (level of sensitivity) and retention periods (duration of storage). Any effort to retain data (electronic or physical) must be justified by demonstrable business needs as well as any applicable regulatory requirements. Process controls should be implemented that protect data from loss, falsification or inadvertent destruction. Adequate protection measures must be in place for electronic and physical records.

Employees and consultants/advisors should not retain personal information beyond what is necessary to carry out the role/function in the following scenarios:

- When the client decides not to follow through with the consultant/advisor's proposal;
- When the client withdraws his/her application to the relevant Authorities.
- When the recruitment process is completed for managers, supervisors or organisation leaders (at which time they should not retain the application forms of the job candidates).

DUPLICATION AND DESTRUCTION OF RECORDS

DESCRIPTION/RATIONALE

Once records of personal data are no longer needed, they should be anonymised or securely destroyed/deleted, including duplicated records or documents.

RISK/EXPOSURE

Not destroying records of personal data beyond their legitimate purposes may result in misuse of the information that is no longer relevant or outdated.

PREVENTIVE MEASURE/ACTION

Records of personal data (both physical and electronic) that no longer have any legitimate business or legal use should be securely destroyed/deleted. Those data that are required for analysis or statistical purposes should be anonymised.

Extra care should be taken in the following scenarios:

- Office equipment (especially those on lease) such as multi-functional copiers/fax/printers with internal hard disks/removable drives should be reformatted/destroyed.
- Unwanted prints/misprints should be shredded or destroyed through a secure document disposal service.
- Back-ups of personal information/records in shared drives should be destroyed.

ACCESS CONTROL

DESCRIPTION/RATIONALE

It is the Organisation's policy that access to personal information by an individual employee or consultant/advisor to the internal information system should be tied to the role/job responsibility of the respective personnel. No employee or consultant/advisor should have greater information access than is necessary to capably perform his or her job function.

RISK/EXPOSURE

Without a proper scheme of access control for the Organisation's internal information systems, the Organisation could be susceptible to:

- Negligent, accidental or deliberate system misuse by employees, consultants/ advisors, contractors or third- party users
- Unauthorised access to confidential information
- Identity or data theft
- Sabotage or attacks by malicious third-parties

PREVENTIVE MEASURE/ACTION

The access control policy should be based on the following principles where reasonable:

A) PRINCIPLES

SEGREGATION OF DUTIES

Segregation of duties must be implemented, where appropriate, so that no individual acting alone can compromise the system. This is to reduce the risk of negligent or deliberate system misuse by employees, contractors or third- party users.

LEAST PRIVILEGE

Access should only be granted on the basis of the lowest possible level of access required to perform the function. This limits the damage that can result from accident, error or unauthorised use of the respective system.

NEED TO KNOW OR ACCESS

Access should be granted to users only on a need-to-know-basis that is relevant to the job function. This also applies to third-parties who provide services to the Organisation.

Department heads/managers/IT must have the ability to know who is accessing the information, when and what specifically was accessed to ensure accountability and easier identification, should an account be compromised.

For third-parties or partners working with the Organisation, a formal contract should be put in place, containing or referring to all the information security requirements to ensure compliance with the Organisation's security policies and standards.

In granting third-party access to the Organisation's internal information systems, appropriate security controls should be implemented according to the assessed degree of risk.

B) AUTHENTICATION AND AUTHORISATION

DESCRIPTION/RATIONALE

When giving internal information access to personnel or via their accounts, the appropriate authentication and authorisation for access, usage, and monitoring of access should be used. Access to the Organisation's computing resources must be controlled through the use of appropriate identification and authentication mechanisms and logical access controls.

RISK/EXPOSURE

Without properly defined authentication and authorisation policies and mechanisms, the Organisation runs the risk of unauthorised personnel (both internal and external) trying to make unauthorised access or hacking into the Organisation's internal information systems.

PREVENTIVE MEASURE/ACTION

User IDs and passwords are to be appropriately used and protected. Each user is personally responsible for the usage of their IDs and passwords which must not be shared with other individuals.

The following are guidelines that SIPL advocates (or as it relates to the IT/Password policy):

- System passwords should be independently assigned and used (not shared).
- Blank-field passwords are not allowed.
- Passwords should contain at least eight characters or as the appropriate characters as the system supports.
- A combination of upper and lowercase letters, numbers and at least one special character (e.g. %&*) should be used in composing the password.
- Passwords should be actively cycled at least once every quarter.
- Inactive accounts of terminated or departed employees should be disabled completely.
- Password schemes should not be associated with anything that may be broadly familiar to the individual or others at the Organisation (nicknames, birthdates, etc).

All passwords should never be stored (or recorded) in any location that is within plain view of a casual observer (both virtually/physically).

Where practical, two-factor authentication (use of password together with a security token or security code generated in real-time and sent via SMS or email) should be used.

When releasing personal information to external parties, due diligence should be done to authenticate the requester first prior to release and whether the requester has the authority to access or receive the respective information. If the request is for a third party, then an authorisation letter should be produced by the individual concerned.

A2) PERSONNEL INFORMATION SECURITY

HUMAN RESOURCE POLICIES

DESCRIPTION/RATIONALE

Employees and consultants/advisors of SIPL together with the policies, processes and systems, constitute the major components of an information security regime. In a number of information security breaches, the people are the weakest link, whether by ignorance, negligence or malicious intent. Therefore it is important for the Organisation to have robust HR policies for the screening of potential employees at the recruitment stage, making known to them the Organisation's information security policies and practices when they become employees, and ensuring that they conform to these policies and practices.

RISK/EXPOSURE

Employees could commit criminal breach of trust, theft of personal data, misuse of confidential information, malicious actions on the Organisation's information systems, or attempt at unauthorised entry/access to the Organisation's information assets.

PREVENTIVE MEASURE/ACTION

Screening and Background Check. Potential candidates for employment by the Organisation must be screened and their background checked during the recruitment stage. Additional checks should be done for those taking up trusted positions. Prior to employment, those handling personal data should have clear information security roles and responsibilities, which may also include specific responsibilities for protection of particular information assets.
These should be clearly explained to new employees and should be stated in the terms and conditions of employment.

Confidentiality/Non-Disclosure Agreement. All employees must formally accept a binding confidentiality or non- disclosure agreement concerning personal and proprietary information provided to or generated by them in the course of employment. They are required to sign a confidentiality or non-disclosure agreement as a part of their initial terms and conditions of employment and annually thereafter.

Awareness. To ensure awareness of the importance of information security, all employees are required to attend Information Security training and regular updates on organisational policies and procedures at least once a year.

Resignation. Upon resignation from the Organisation, the employee's physical access and IT rights (e.g. email) must be terminated immediately.

Return of Property. Upon resignation from the Organisation, the employee must return all access cards, keys, IT equipment, storage media and other valuable corporate assets to the Organisation on or before his/her last day of employment.

ENTRY INTO PREMISES

DESCRIPTION/RATIONALE

Employees, consultants/advisors, contractors and visitors entering and moving about the Organisation's premises should have controlled and restricted access through some form of identification and authentication.

RISK/EXPOSURE

If there is no proper identification and authentication of personnel entering and moving about the Organisation's premises, the Organisation runs the risk of people making unauthorised access to physical offices and work areas where confidential information is processed and stored to view, duplicate or steal the information. If the personal data used for identification and authentication is not properly protected, there is risk of identity theft and compromise of the security and access control system.

PREVENTIVE MEASURE/ACTION

The Organisation should use:

The biometric data, photo images and other security data used for identifying and authenticating individuals should be encrypted.

ACCESS AND USAGE OF KEYS

DESCRIPTION/RATIONALE

Keys can open doors, lockers, cabinets, offices and rooms where the Organisation's confidential information assets are kept. Procedures for controlling the movement and usage of keys are thus important.

RISK/EXPOSURE

Keys in the hands of unauthorised persons could enable them to enter restricted areas to view, duplicate or steal confidential data or perform malicious acts on information assets and computer systems. Improper control over the movement of keys could lead to lost keys or unauthorised duplication of keys.

PREVENTIVE MEASURE/ACTION

Usage of keys should be handled with care as negligence or carelessness could lead to unnecessary exposures of personal data. Access to keys should only be granted to authorised staff and the relevant movement of keys and contact details should be recorded. There should be a secure keypress which can be locked at all times and the main key held by an authorised person.

Leaving keys within the locks should be avoided and all cabinets and rooms containing personal and confidential documents should be locked when unattended or after office hours.

USE OF OFFICE EQUIPMENT

DESCRIPTION/RATIONALE

The multifunction photocopier, printer, scanner and fax machine is where a lot of documents containing personal data are printed, photocopied, scanned and faxed. It is thus important to have strict control measures on the use of this office equipment.

RISK/EXPOSURE

Without proper control measures, unauthorised persons can access the previous saved jobs in the memory of the equipment to make printouts and copies of confidential documents and even fax or email them out. Uncollected printouts and faxes can be viewed by unauthorised persons.

PREVENTIVE MEASURE/ACTION

The multifunction equipment should have password control so that only authorised users can use it. Users must be reminded to collect their printouts and faxes as soon as possible and not leave them lying around. Users should also be reminded to collect their original documents after they have scanned the documents. All unwanted printouts and faxes containing confidential data should be properly destroyed using a paper shredder or a secure disposal service.

When the lease of the multifunction equipment expires and is to be returned to the vendor, the built-in memory should be erased to ensure no confidential information is left behind.

SUBMISSION OF FORMS AND DOCUMENTS

DESCRIPTION/RATIONALE

SIPL's consultants/advisors often have to submit forms with clients' personal data and supporting documents to the HQ Processing Dept (PO) for processing. The confidential information contained within these forms and documents must be handled properly and securely, and be accounted for.

RISK/EXPOSURE

If the forms and documents are not handled properly and securely, there could be risks of them getting lost/misplaced or be removed/stolen, and the confidential data contained within being viewed or duplicated by unauthorised persons.

PREVENTIVE MEASURE/ACTION

At the submission counter there must be staff responsible for receiving the submitted forms and documents, checking for completeness, and acknowledging receipt. If the counter is not manned, there must be a submission box with a one-way pigeon hole for slotting in the forms and documents. The submission box must be securely locked and only authorised persons can open it to retrieve the submitted forms and documents. Once these forms and documents are checked for completeness, an acknowledgement should be made known to the consultant/advisor concerned. As an added security measure, the submission box should be monitored by CCTV camera.

MOVEMENT OF CONFIDENTIAL DOCUMENTS

DESCRIPTION/RATIONALE

SIPL's consultants/advisors often have to handle the movement of documents and contracts/agreements containing clients' personal/sensitive data to the HQ Processing Dept (PO) for processing or to insurers/manufacturers/providers for application of financial investment or insurance products. These confidential documents must be handled properly and securely, and be accounted for in transit, before they reach their intended recipients, even though the consultants/advisors merely act as data intermediaries (e.g. in the case of clients' supporting medical and health screening reports to insurers).

RISK/EXPOSURE

If the confidential/sensitive documents are not handled properly and securely during transit, there could be risks of them getting lost or misplaced due to negligence, and the confidential data contained within being viewed or duplicated by unauthorised persons. If the movement and delivery of the documents is done through a courier service, there could be risks of them getting lost or misplaced or sent to the wrong addressee due to the courier's negligence.

PREVENTIVE MEASURE/ACTION

During transit of the confidential/sensitive documents, the consultant/advisor should be reminded to be vigilant in looking after the documents, putting them in secure temper-proof boxes or briefcases/luggage's with locks or combinations. There should be proper procedures for the handover and acknowledgement of the documents from one party to the next.

When using courier services, it is important to hire one that is reliable and reputable, with a proper process of tracking the movement of documents in transit and of acknowledging the handover and receipt of the documents.

TRANSMISSION OF SENSITIVE DATA

DESCRIPTION/RATIONALE

Confidential/sensitive data pertaining to individuals that are transmitted via email or other electronic means to recipients both locally and overseas must be done through secure means.

RISK/EXPOSURE

If the confidential/sensitive data are transmitted through non-secure means there could be risks of unauthorised access or modification to the data, hijack of the data, misuse of the data, or identity theft.

PREVENTIVE MEASURE/ACTION

Where possible, sensitive data transmitted via email or other electronic means should be secured or encrypted (e.g. Public-key-infrastructure). As a minimum, documents with personal data (e.g. pdf, axles) sent via electronic media (email, thumb drive, etc) must be password-protected. The password to access the documents must be sent separately to avoid compromise of security.

A3) PHYSICAL AND ENVIRONMENT INFORMATION SECURITY

At SIPL's office premises, personal data of employees, consultants/advisors and clients are being captured, processed, used, shared, stored and archived. These data can be in hardcopies such as forms, documents, contracts, agreements, spreadsheets and correspondences kept in files, folders and binders, and stored in drawers, cabinets and storage areas. These data can also be in electronic form and are stored in corporate databases, servers, hard disks and shared drives/folders. Thus it is critical for SIPL to have in place adequate physical and environment security of its office premises to protect the information assets against unauthorised or illegal access and theft of records, files and documents.

Sensitive information should not be stored in an area where the general public or staff has access or where there is regular traffic of individuals who are not authorised to view such information. Such records should be locked in cabinets or isolated in a locked room with restricted access.

RECEPTION AREAS

DESCRIPTION/RATIONALE

The reception area is where visitors sign in and sign out, suppliers/vendors report to deliver goods, and couriers deliver documents and parcels/packages. It is the first stage of screening of outsiders before they are allowed access to the offices.

R*ISK/EXPOSURE*

Personal data of visitors and outsiders are recorded as proof of identity. If such data are not properly shielded from public view, they could be browsed or photographed by the outsiders without permission when the receptionists are busy or when they are not around.

PREVENTIVE MEASURE/ACTION

To minimise exposure of personal data, be they recorded by hand or keyed into the computer, the record book or computer screen should be shielded from public view. Proper verification of the visitors' identities must be carried out to ensure that only those with legitimate business with the Organisation can be allowed to enter the office premises.

SERVICE COUNTERS

DESCRIPTION/RATIONALE

A service counter is where consultants/advisors submit clients' KYC forms, agreements/ contracts and supporting documents to the HQ Processing Dept (PO) for processing. These forms and documents contain a lot of personal data and hence have to be handled carefully and be properly accounted for.

RISK/EXPOSURE

Where there are no proper procedures on how these forms and documents are to be handled and accounted for, the documents could be lost, stolen or misplaced. When the counter staff are busy or attending to some other matters, the confidential documents could be within easy reach of unauthorised persons who could view or photograph them.

PREVENTIVE MEASURE/ACTION

Service counters should have reasonable "barriers" (e.g. restricted entry, physical barriers) between the service staff and the people they are serving. Confidential documents should not be left on the counter. All files/paper documents/in-trays at the service counter should be shielded from public view.

In the event a document containing personal data is submitted, it should only be received by the authorised person and should not be left exposed. There should be proper acknowledgement of handover and receipt of files and documents between the counter staff and consultants/advisors.

Locked submission boxes should be installed for consultants/advisors to deposit their forms and documents after office hours and when the service counter is not manned.

MEETING ROOMS

DESCRIPTION/RATIONALE

Meeting rooms are where staff of the Organisation hold their internal meetings, or where the Organisation's staff meet with external visitors. Meeting rooms are usually equipped with whiteboards/flipcharts, audio-visual equipment, and computer terminals for people to upload their presentation slides for projection or for access to the corporate databases or Internet to retrieve information. Personal/sensitive data could be shared among the meeting members and these have to be protected against unauthorised access by other people who are not part of the meeting.

RISK/EXPOSURE

Trails of personal/sensitive data left behind at the end of the meeting could pose information security risks, e.g. writings on whiteboards/flipcharts, electronic files copied to computer terminals in the meeting room, confidential documents on the tables or chairs.

PREVENTIVE MEASURE/ACTION

All whiteboards should be cleaned after meetings to ensure that no sensitive data is visible. All paper documents (including flipcharts) should either be kept or disposed. If sensitive documents are stored in the meeting room, these should be in locked cabinets.

All electronic files copied or downloaded to the computer terminals should be erased at the end of the meeting. All media devices containing confidential data (e.g. portable hard disks, USB storage devices, thumb drives) should be removed from the meeting room or their contents deleted.

Documents containing sensitive information should not be left unattended, even if it is for a few minutes.

CONSULTANTS' WORK AREAS - COMPUTER TERMINALS

DESCRIPTION/RATIONALE

These are flexi-work areas equipped with computer terminals that are set aside for the use of consultants/advisors. Personal/sensitive data could be used, processed and shared at the work areas and computer terminals. Because of the public nature of the workspace it is important that proper procedures be in place to manage and protect the personal/sensitive data.

RISK/EXPOSURE

Trails of personal/sensitive data left behind at the end of each usage session could pose information security risks,
e.g. downloaded files and work files containing personal/sensitive data left behind in the hard disk of the public terminal, thumb drive inserted in the USB port of the computer not removed, web browsers with browsing history, saved passwords from autocomplete feature, confidential documents on tables or chairs.

PREVENTIVE MEASURE/ACTION

All electronic files containing personal data that are created, downloaded or copied to the public terminals should be deleted after use. Extra care should be taken to ensure that no residue files are left in the public terminal's folders (e.g. Downloads, My Documents, Desktop). Recycle Bins of the public terminal should be emptied after use.

Users must logoff from the information systems they have accessed from the public terminals. All portable media (e.g. portable hard disks, thumb drives) used must subsequently be removed.

In addition, the public terminal's automatic 'Save Password' feature must be disabled to prevent unauthorised access through 'remembered' logins. The privacy settings in the web browser should be correctly configured to disable autocomplete features and browsing history.

Notices should be displayed prominently at the work areas and public terminals to remind users to carry out the above safeguards and to remove all portable media devices and confidential documents when they leave the work area. IT personnel should check the work areas and public terminals regularly for any exposures.

CONSULTANTS' WORK AREAS - TELEPHONES

DESCRIPTION/RATIONALE

These are flexi-work areas equipped with phone lines and handsets for the use of consultants/advisors. Personal phone numbers are used by them to make cold calls to individuals. It is important to have safeguards against the consultants/advisors calling someone on the DNC registry or SIPL's blacklist.

RISK/EXPOSURE

Consultants/advisors could inadvertently or deliberately call people on the DNC list or unsubscribe contact lists. There could be accidental exposure of the contact list.

PREVENTIVE MEASURE/ACTION

Cold calls by consultants/advisors must only be conducted in designated areas with telephones enabled with call- barring services (see DNC Policy). Those engaging in such activities must first sign in/out so that records can be kept of their movements and be referenced in the event of a complaint. All calls made must abide by the DNC rules and guidelines as stipulated in the Organisation's DNC policy. Contact lists containing personal data should be carefully handled and should not be left exposed or lying around.

Notices should be displayed prominently at the consultants' work areas to remind them to check the DNC registry and blacklist prior to making a call if no consent has been given by the individuals concerned.

STAFF WORK DESK / WORKSPACE

DESCRIPTION/RATIONALE

This is the place where the internal staff perform most of their work, including handling, using, processing and sharing personal data either in physical or electronic form. It is important that there are information security policy and procedures in place to ensure that every staff is aware of his/her responsibility in protecting the Organisation's information assets.

RISK/EXPOSURE

The main areas of risk/exposure include confidential documents exposed and lying around on the desks, drawers and cabinets storing confidential files not locked, door to office not locked, unwanted papers containing personal/sensitive data not properly destroyed, and computer terminals displaying personal/sensitive data in full view to those who are not supposed to look at the data.

PREVENTIVE MEASURE/ACTION

All staff should adopt a clean-desk policy, meaning that no papers, documents or files containing private/sensitive data should be left exposed or unattended even for short periods. They must comply with the following requirements with respect to printed information and computer screens:

- Staff must keep sensitive or confidential information in printed form locked away in drawers or cabinets when not being used or when it will be unattended for an extended period (e.g. when away for meetings, at lunch times or overnight)
- Remove such documents from printers, photocopiers or fax machines immediately
- Dispose of unwanted papers securely using a paper shredder or a secure disposal service
- Lock computers when unattended (e.g. pressing Ctrl-Alt-Del and then Enter)

Where applicable, the office should be locked when the staff is away to prevent theft of or unauthorised access to confidential documents. No items such as bags, mobile devices and keys (to cabinets, drawers and rooms containing sensitive documents) should be left unattended.

DOCUMENT STORAGE AREAS

DESCRIPTION/RATIONALE

These are areas dedicated to the storage of confidential documents and files. Within the storage area there could be cabinets, file compactors or storage boxes. Such areas have to be securely protected as they have a concentration of confidential information assets of the Organisation in one location.

RISK/EXPOSURE

The main areas of risk/exposure include unauthorised access to and theft of confidential documents, unlocked cabinets, unlocked doors and fire hazard.

PREVENTIVE MEASURE/ACTION

Document storage areas containing confidential documents and files must be securely locked and accessible only to authorised personnel. All cabinets must be locked and the keys taken out from the keyholes. All file compactors and storage boxes must be secured. All entry/exit points to the storage areas should be monitored by CCTVs.

Access to physical documents kept at the storage area should be segregated by functional roles such that only personnel on a 'need to know' basis can have access to their respective stored contents. Where practical, there should be physical barriers to segregate the cabinets and storage boxes according to functional areas.

There should be inventory / file movement records to account for potential missing / unreturned files in each storage cabinet.

ACCESS TO OFFICE AREAS / PREMISES

DESCRIPTION/RATIONALE

This refers to parameter security and access to internal premises of the Organisation. Adequate physical protection and security is necessary to prevent intruders or unauthorised personnel from entering the office areas and internal premises.

RISK/EXPOSURE

Main areas of risk/exposure include unauthorised or forced entry, insider data breaches and lost information assets.

PREVENTIVE MEASURE/ACTION

There should be a mechanism to authenticate access by individuals through a robust security system using passcode or biometrics. Staff should be made to wear staff ID badges or passes at all times.

Access to office areas and premises should be limited to certain hours. Access to work areas should be restricted to personnel who are directly handling certain confidential data (e.g. HR, Finance).

ACCESS TO RESTRICTED/SECURE AREAS

DESCRIPTION/RATIONALE

Restricted/secure areas include server room, communications equipment room and CCTV room where personal data are captured and stored. Adequate physical protection and security is necessary to prevent intruders or unauthorised personnel from entering these areas.

RISK/EXPOSURE

Main areas of risk/exposure include unauthorised or forced entry, insider data breaches and lost information assets.

PREVENTIVE MEASURE/ACTION

Only authorised personnel are strictly allowed to enter these restricted/secure areas. HR and department managers should review the list of people who are authorised to enter these areas, at least once a year.

VIDEO SURVEILLANCE DEVICES / CCTVS

DESCRIPTION/RATIONALE

All main entrances and exits to the Organisation's office premises, restricted/secure areas and other critical locations (e.g. document submission area, document storage areas) must be monitored to detect any intrusion or forced entry by unauthorised personnel.

RISK/EXPOSURE

Main areas of risk/exposure include theft of information assets, insider sabotage, potential invasion of privacy, unauthorised disclosure of video footage and industrial espionage.

PREVENTIVE MEASURE/ACTION

CCTVs should be positioned at strategic locations to monitor entrance/exit points where personal data are kept/stored in addition to monitoring general premises. Notices should be displayed prominently to inform visitors that the office premises are under CCTV surveillance.

The monitoring should be done round the clock by trained personnel. Video footages should be recorded and stored for at least one month. There should be controlled access to captured video footages as they contain personal data.

PUBLIC AREAS WITH WI-FI

DESCRIPTION/RATIONALE

Public areas with Wi-Fi could be accessed SIPL's employees and consultants/advisors using mobile devices. There could be vulnerabilities to users from the unprotected Wi-Fi networks.

RISK/EXPOSURE

Main areas of risk/exposure include malware and virus attacks, and identity theft.

PREVENTIVE MEASURE/ACTION

To minimise risks from the non-secure Wi-Fi networks, all mobile devices should have firewalls and anti-virus software installed.

A4) USE OF INFORMATION TECHNOLOGY

HARDWARE AND SOFTWARE INSTALLATION, MODIFICATION AND REMOVAL

DESCRIPTION/RATIONALE

At appropriate times, when the IT needs of the Organisation grow, new hardware and software will have to be installed. Existing networks and hardware will have to be reconfigured or modified. Old or obsolete hardware and equipment will have to be retired or removed.

Also, SIPL's employees and consultants/advisors may be bringing in their own laptops, tablets, portable storage and mobile devices to connect to the Organisation's IT infrastructure and networks.

There must be proper policies and approval mechanisms for governing the installation, modification and removal of hardware and software within the Organisation, and the bringing in of own devices by employees and consultants/advisors.

RISK/EXPOSURE

Without proper policies and approval mechanisms governing the installation, modification and removal of hardware and software within the Organisation, and the authorisation for people to bring in their own devices, the integrity and performance of the IT infrastructure could be affected or disrupted.

PREVENTIVE MEASURE/ACTION

Only authorised personnel are permitted to add, remove or modify any equipment, hardware or software within SIPL's environment. This ensures that all hardware is approved, and all software remains virus free, registered, and licensed to the Organisation with all copyrights protected.

Personal storage devices, including tablets but not limited to external hard drives, USB thumb drives, mobile devices, etc., must not be used for storing Restricted or Confidential information unless the relevant devices are protected via screen locks, passcodes and encryption.

Only the following authorised, pre-approved, Organisation-supplied and personally owned hardware, mobile devices and software are acceptable:

- Desktop computer
- Notebook/laptop computer
- Tablets
- Mobile devices
- Portable storage devices (e.g. thumb drives, portable hard disks)
- Microsoft Office
- Anti-virus software

Users are responsible for ensuring that their own laptop computers and authorised portable storage devices containing business information are protected from loss, theft, destruction and unauthorised disclosure and are physically secured in an appropriate manner at all times.

PROTECTION AGAINST MALICIOUS CODE/VIRUSES/MALWARE/SPYWARE

DESCRIPTION/RATIONALE

In a highly networked IT environment, where personal/sensitive data are easily and widely transmitted and shared among SIPL's employees, consultants/advisors and even third-parties, one of the main threats is the infection by malicious code, viruses, Trojans, worms, malware, spyware, etc introduced via shared thumb drives, web browsing or downloading of apps. Therefore it is extremely important for the Organisation to have adequate preventive measures and protection against such a threat.

RISK/EXPOSURE

If there is inadequate preventive measures or protection against malicious code, viruses, Trojans, worms, malware, spyware, etc, the entire computer network, computer systems and databases within the Organisation could be infected, resulting in lost or illegally modified data, corruption of databases, theft of personal IDs and passwords, or disruption to computer networks and systems.

PREVENTIVE MEASURE/ACTION

Users have the accountability to protect their workstations, notebooks and mobile devices from malicious code, viruses, Trojans, worms, malware, spyware, etc and to report suspicious infection or incidents to the responsible parties. (Please refer to the IT Policy for more details).

All users should ensure they have installed anti-virus programs and that these are updated to the latest versions. All users should also be taught how to turn on built-in/bundled firewalls that come with their computers and mobile devices. The IT Department should implement firewalls and other protective measures at the network level and to minimise system vulnerability at open ports (incoming and outgoing emails and messaging systems).

SHARED DRIVES AND FOLDERS

DESCRIPTION/RATIONALE

Shared drives and folders offer a convenient platform for different users to have common access to electronic data containing personal/sensitive data from their workstations, notebook/laptop computers or mobile devices. These shared drives and folders could be sited within the consultants'/advisors' organisations or hosted in the cloud through external cloud service providers (e.g. Dropbox, Google Drive). There should be proper control mechanisms to protect the personal/sensitive data and to restrict access to authorised persons only.

RISK/EXPOSURE

Shared drives and folders could be easily hacked into and the personal/sensitive data stolen or compromised if there is inadequate protection and control mechanisms. Other consequences could include the introduction of malicious code or viruses, account/service hijacking and identify theft.

PREVENTIVE MEASURE/ACTION

Where possible, two-factor authentication (2FA) should be used for access to cloud-based shared services (such as Dropbox, Google Drive). Invitation to grant third-party access must be disabled.

For local shared folder that requires no user authentication, the shared files (e.g. Excel spreadsheets, Word documents) should be password protected, and where practical, be encrypted.

PROTECTION OF ELECTRONIC DOCUMENT

DESCRIPTION/RATIONALE

Within SIPL, and between SIPL and the consultants'/advisors' organisations, a lot of electronic documents containing personal/sensitive data are being created, processed, shared and transmitted. These documents must be adequately protected lest they are accessed by unauthorised persons.

RISK/EXPOSURE

Unauthorised access to the electronic documents containing personal/sensitive data, whether done accidentally or deliberately, could result in information leakage and exposure, or illegal modification/falsification of the data.

PREVENTIVE MEASURE/ACTION

Where practical, all Word, Excel and PDF documents containing personal/sensitive data should be password protected or encrypted. Transmission of such documents should be done over secure and encrypted networks (e.g. via VPN).

Personal/sensitive data stored in mobile devices should also be encrypted using the built-in function in the device or purchased apps.

PROTECTION OF COMPUTER SCREEN

DESCRIPTION/RATIONALE

The computer screen, whether on desktop or portable mobile computing devices, provides the interface for users to read and access personal/sensitive data. As such, they should be protected against viewing by persons who are not supposed to see the data.

RISK/EXPOSURE

Unauthorised persons could view personal/sensitive data on the computer screens, whether accidentally or deliberately, resulting in information leakage and exposure, or illegal modification/falsification of the data.

PREVENTIVE MEASURE/ACTION

All users should enable the screen lock function or screen saver with password/PIN feature on their computers and mobile devices.

PROTECTION OF MOBILE DEVICES

DESCRIPTION/RATIONALE

Mobile computing devices (e.g. tablets, smart phones) used by SIPL's employees and consultants/advisors could contain personal/sensitive data, which must be adequately protected.

RISK/EXPOSURE

When mobile devices are misplaced, lost or stolen, the personal/sensitive data stored within them could be accessed by unauthorised persons, resulting in information leakage and exposure, identity theft or malicious use by third- parties.

PREVENTIVE MEASURE/ACTION

If the mobile device has the built-in function or purchased apps to auto-delete or wipe off personal data remotely when the device is lost or stolen, it should be activated.

A5) THIRD PARTY OUTSOURCING

SIPL takes a serious view of any third party outsourcing, especially with regards to collection, processing and analysis involving personal data.

The third-party outsourcing contract should include security controls such as the following:

- Security roles and responsibilities
- Requirements for information protection in order to achieve levels of security with the third party that are equivalent to those of the Organisation
- Information ownership and appropriate use
- Physical and logical access controls
- Security control testing of the third party
- Continuity of services in the event of a disaster/unplanned outage
- Right to conduct audits
- A clear statement of respective liabilities

A6) SECURITY INCIDENT MANAGEMENT

Information security events (including situations where users find that they are able to circumvent security safeguards) or incidents must be reported, recorded, investigated and resolved. Users must immediately report any security violations or incidents to their manager/department head and the Data Protection Officer.

This includes loss of notebooks/laptops and mobile devices containing personal data, exposure or misplacement of confidential documents.

Approval and Effective Date:_____

Approved by:_____Date: _____

CEO, Shank International Pte Ltd

Name: _____

Prepared by:

Data Protection Officer

Name: _____

Email: _____