Policy Document

Information Security Policy (Personal Data)

30 Nov 2017

Document Control

Company	Prosec Services Pte Ltd
Title	Information Security Policy (Personal Data)
Author	Al R Dizon, DPO
Filename	Prosec Infosec Policy.docx
Owner	Jonathan Low, Head IT
Subject	Information Security Policy (Personal Data)
Review date	

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

- Management of Prosec Services Pte Ltd
- PDPA committee of Prosec Services Pte Ltd (comprising all Heads of Departments)

Contents

Policy Statement

Prosec Services Pte Ltd ("Prosec" or "the Company") is committed to ensuring the proper protection and safeguarding of all information assets within its possession or under its control, in compliance with the Personal Data Protection Act (PDPA) 2012.

Purpose

Information is a valuable asset that Prosec has a responsibility and requirement to protect, especially with regards to complying with the PDPA. The objectives of this Policy are as follows:

- Protecting the Company's personal data within its possession or under its control;
- Establishing minimum principles or safeguards to protect the Company's information assets from loss, theft, destruction, unauthorised manipulation, unauthorised disclosure, or unavailability; and
- Establishing responsibility and accountability for Information Security in the Company.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Company 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** of information. It details the basic requirements and responsibilities for the proper management of information assets at Prosec. It also specifies the means of information handling and transfer within the Company and with external parties.

Although this Policy pertains to personal data only, some processes and good practices may also be applied to other forms of information possessed by the Company, such as business information, contracts and agreements, and intellectual property.

Scope

This Information Security Policy applies to all groups of **People** (employees, contract staff, associates and part-timers), Business **Processes** and **Systems** (both manual and computerised) that make up Prosec's Information Systems.

Aspects of this Policy, especially the section on Physical and Environmental Information Security (see later), are applicable to security personnel who are deployed at the Clients' sites.

Definition

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

- Data and text printed on hardcopies or written on paper
- Data stored electronically in databases or on other devices (including mobile devices)
- Digital documents (Microsoft Office or equivalent, PDF)
- Communications using electronic means (emails, faxes)
- Audio-video recordings
- Speech recordings
- Photographs and digital images
- CCTV footage
- Biometric data

Risks

At Prosec, we recognise that there are risks associated with employees or other persons (as stated above) accessing and handling personal data in order to conduct the Company's businesses and provide services to our clients.

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 reports containing personal data);
- 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);
- 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 Prosec and may result in financial loss, loss of reputation/goodwill and an inability to provide necessary services to our employees and clients.

Applying the Policy

The areas of coverage of this Policy are:

- Information Assets Management and Access Control
- Personnel Information Security
- Physical and Environmental Information Security
- Use of Information Technology and Online Services

The details are in the Appendix.

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

Data Owner	The person or organisation entity that owns the personal data and has the 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 (i.e. the individual whose personal data is collected, used and disclosed)

	• Transfer of the data overseas *Example of Data Owner: Head of Department or Functional Manager*
Data Collector	The person or organisation 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: Departmental Staff, Part-timers*
Data User	The person or organisation 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 external third party that has responsibility for collecting, processing, transmitting or transferring personal data on behalf of the Data Owner. The Data Intermediary is only responsible for the Protection and Retention obligations of the PDPA. The Data Intermediary may not be an employee of Prosec. **In the case of providing security services to our Clients, we are the Data Intermediaries of these Clients.** *Example of Data Intermediary: Third-party service provider (e.g. printing services, payroll processing services, security services)*
Data Custodian	The person or entity that has assigned responsibility from the Data Owner for custoding 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, Admin Department*

Policy Compliance

If any user is found to have breached this Policy, he/she may be subjected to Prosec'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 the Data Protection Officer (DPO) or Head, IT Department.

In the event that you have knowledge of anyone who may be breaching this Policy, please contact the DPO.

Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

Policy review will be undertaken by the DPO together with IT Department.

References

The following policies of Prosec are to be used in conjunction with this Information Security Policy:

- IT Policy

Approval and Effective Date: 30/11/17

Approved by: _____ Date: 30/12/17

Name: Rene M Shepherdson Jr, PBM
Designation: GM / Director, Prosec Singapore Pte Ltd

Prepared by:

Data Protection Officer
Name: Al R Dizon
Email: dpo@prosegur-prosec.sg

Appendix: Applying the Policy

A1) Information Assets Management and Access Control

Identifying Information Assets

Description/Rationale
There is a need to identify all the important information assets belonging to Prosec, so that the Company can implement appropriate policies and practices to govern the management and protection of such information assets.

Risk/Exposure
Without a Company-wide view of what important information assets Prosec owns or is responsible for, the Company could be susceptible to loss or theft of information assets, unauthorised access to personal data, or criminal activity related to malicious attack on the information assets.

Preventive Measure/Action
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
    - IT application systems
    - Physical assets (e.g. computer equipment and accessories, tablets, mobile phones)

Prosec 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, business continuity 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
As a minimum, all documents containing personal data must be classified and labelled accordingly, so that appropriate measures can be put in place to protect and restrict access to each class of documents.

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 personal data, or misuse/mishandling of documents containing personal data.

Preventive Measure/Action
The classification scheme 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.

One such classification scheme is:

- UNCLASSIFIED – open access to anyone (e.g. information made available to the public)
- RESTRICTED – confined to those within Prosec (e.g. internal policies)
- CONFIDENTIAL – confined to those with a 'need to know' basis within Prosec (e.g. HR data of employees)

Retention of Records

Description/Rationale
Prosec 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
Prosec may retain personal data (electronic and physical) for tax, audit and other business and legal purposes (as stated in the Document Retention Policy). Process controls should be implemented that protect data from loss, falsification or inadvertent destruction.

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

- When the client decides to terminate Prosec's services
- When the data subject withdraws consent or instructs Prosec to do so
- When the job applicant is unsuccessful/rejected
- When an employee resigns or his/her employment is terminated
- When the statutory retention period is reached

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 data/records in shared drives should be destroyed.

Access Control

Description/Rationale
Access to personal data in Prosec's internal information systems should be tied to the role/job responsibility of the respective employee. No employee should have greater information access than is necessary to capably perform his/her job function.

Risk/Exposure
Without a proper access control policy for Prosec's internal information systems, the Company could be susceptible to:

- Negligent, accidental or deliberate system misuse by employees
- Unauthorised access to personal data
- 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 Prosec.

Department Heads and 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 Prosec, a formal contract should be put in place, containing or referring to all the information security requirements to ensure compliance with Prosec's information security policies and standards.

In granting third-party access to Prosec'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 personnel access to Prosec's internal information systems, the appropriate authentication and authorisation for access, usage, and monitoring of access should be used.

Risk/Exposure
Without properly defined authentication and authorisation policies and mechanisms, Prosec runs the risk of unauthorised personnel (both internal and external) trying to make unauthorised access to or hacking into the Company'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 his/her own IDs and passwords which must not be shared with other individuals.

Suggested guidelines for a password policy are as follows:

- System passwords should be independently assigned and used (not shared).
- Do not use the same password for a number of applications.
- 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 or half-yearly.
- Inactive accounts of terminated or departed employees should be disabled immediately and completely.
- Password schemes should not be associated with anything that may be broadly familiar to the individual or others at Prosec (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 data 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
A number of information security breaches have shown that the people are the weakest link, whether by ignorance, negligence or malicious intent. Therefore it is important for Prosec to have robust HR policies for the screening of potential employees at the recruitment stage, making known to them Prosec'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 personal data, malicious actions on Prosec's information systems, or attempt at unauthorised entry/access to Prosec's information assets.

Preventive Measure/Action
Screening and Background Check. Potential candidates for employment by Prosec must be screened and their background checked during the recruitment stage. Additional checks should be done for those taking up trusted or sensitive positions (including those at clients' sites). 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 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 Prosec's policies and procedures at least once a year.

Resignation. Upon resignation from Prosec, the employee's physical access to the Company's premises and IT rights (e.g. email) must be terminated immediately. If, subsequently, the ex-employee approaches any of Prosec's staff to obtain personal data belonging to the Company, staff must not accede to such requests.

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

Entry into Premises

Description/Rationale
Employees, contractors and visitors entering and moving about Prosec'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 Prosec's premises, the Company runs the risk of people making unauthorised access to physical offices and work areas where personal data 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
Prosec should implement:

- Secure access to offices and facilities using employee access cards. As an additional layer of security, the employee may be required to key in the access code or to use biometrics.
- Employee ID card to be displayed at all times.
- Third-party and visitor's ID card to be worn at all times.

The photo images and other security data used for identifying and authenticating individuals should be encrypted, and the database containing such data should be securely protected.

Access and Usage of Keys

Description/Rationale
Keys can open doors, lockers, cabinets, offices and rooms where Prosec's personal data 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 personal 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 persons 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 documents with personal data 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 previously saved jobs in the memory of the equipment to make printouts and copies of documents containing personal data, 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 exposed and lying around. Users should also be reminded to collect their original documents after they have scanned the documents.

All unwanted printouts and faxes containing personal 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 personal data is left behind.

Submission of Physical Forms and Documents

Description/Rationale
Prosec's staff often have to submit physical forms and documents containing personal data and supporting documents to HQ for processing. These 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 they contain being viewed, duplicated or distributed 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 staff concerned. As an added security measure, the submission box should be monitored by CCTV camera.

Movement of Physical Documents Containing Personal Data

Description/Rationale
Prosec's staff often have to handle the movement of physical documents and contracts/ agreements containing personal data between departments for processing or to external third-parties for further processing. These documents must be handled properly and securely, and be accounted for in transit, before they reach their intended recipients.

Risk/Exposure
If the documents containing personal data are not handled properly and securely during transit, there could be risks of them getting lost or misplaced due to negligence, and the personal 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 documents containing personal data, staff should be reminded to be vigilant in looking after the documents, putting them in secure tamper-proof envelopes. 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.

Electronic Transmission of Sensitive Personal Data

Description/Rationale
Transmitting sensitive personal data of individuals electronically, especially those pertaining to salary details, credit card details or medical history, via email or other electronic means to recipients both locally and overseas must be done through secure means.

Risk/Exposure
If such sensitive personal 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 personal data transmitted via email or other electronic means should be secured or encrypted. As a minimum, documents with personal data sent via electronic media (email, thumbdrive, etc) must be password-protected. The password to access the document must not be sent in the same email as the document in order to avoid compromise of security. The password should be sent via a separate email or via another medium (e.g. SMS).

The IT Department should put in place data loss/leakage prevention (DLP) software to detect and prevent the transmission of sensitive personal data beyond the authorised recipients. The DLP software scans outbound documents, e-mail messages and file attachments containing sensitive personal data to ensure that they have undergone the prescribed checks and controls.

A3) Physical and Environmental Information Security

Adequate physical and environmental security of Prosec's office premises is necessary to protect the information assets against unauthorised or illegal access and theft of records, files and documents.

Personal data should not be stored in an area where the general public has access or where there is regular traffic of individuals who are not authorised to view such information (including internal staff). Such records should not be left unattended, but be locked in cabinets or isolated in a locked room with restricted access.

Reception / Security Counters

Description/Rationale
The reception/security counter 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 premises.

Risk/Exposure
Personal data of visitors and outsiders, as recorded in the visitor's book, could be exposed to accidental viewing by outsiders as they fill in their personal particulars. The personal data in the visitor's book could also be browsed or photographed by the outsiders without permission when the persons on duty are busy or when they are not around.

Preventive Measure/Action
To minimise exposure of personal data contained in the visitor's book, the Officers on duty could record the visitors' particulars on their behalf. Instead of a visitor's book, the persons on duty could request each visitor to fill in his/her personal particulars on a single sheet of paper.

If an electronic means of registration is used (e.g. on an iPad), there should be a new blank screen for each visitor.

The visitor's book should be kept away from public view, and preferably under lock and key when the person on duty is away, even for a short while.

Meeting Rooms

Description/Rationale
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 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 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, documents containing personal data left on the tables or chairs.

Preventive Measure/Action
All whiteboards should be cleaned after meetings to ensure that no personal data is visible. All paper documents (including flipcharts) should either be kept or disposed. If documents containing personal data 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 personal data (e.g. portable hard disks, USB storage devices, thumbdrives) should be removed from the meeting room or their contents deleted.

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

Common Work Areas - Computer Terminals

Description/Rationale
Personal/sensitive data could be used and processed using shared computer terminals at the common work areas. Because of the shared nature of usage it is important that proper procedures be in place to manage and protect one's personal/sensitive data.

Risk/Exposure
Trails of personal/sensitive data left behind at the end of each usage session could pose information security risks. For example,

- Downloaded files and workfiles containing personal/sensitive data left behind in the hard disk of the shared terminal
- Thumbdrive 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 shared terminals should be deleted after use. Extra care should be taken to ensure that no residue files are left in the shared terminal's folders (e.g. Downloads, My Documents, Desktop). Recycle Bins of the shared terminal should be emptied after use.

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

In addition, the shared 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 shared 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 shared terminals regularly for any exposures.

Staff Workdesk / 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 Prosec's information assets.

Risk/Exposure
The main areas of risk/exposure include

- Documents containing personal data exposed and lying around on the desks
- Drawers and cabinets storing confidential files not locked
- Door to office not locked
- Unwanted papers containing personal data not properly destroyed
- Computer terminals displaying personal 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 personal 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 personal data 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), which can only be unlocked via a password set by the staff

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

Document Storage Areas

Description/Rationale
These are areas dedicated to the storage of documents and files containing personal data. 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 personal data of Prosec in one location.

Risk/Exposure
The main areas of risk/exposure include unauthorised access to and theft of documents containing personal data, unlocked cabinets, unlocked doors and fire hazards.

Preventive Measure/Action
Document storage areas housing documents and files with personal data 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 practicable, 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 perimeter security and access to internal premises of Prosec. 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 by off-duty personnel and site officers 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 personal data (e.g. HR, Finance) and those working at Prosec's main office.

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 Prosec's office premises, restricted/secure areas and other critical locations (e.g. server room, 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 or depending on the capacity of the recording media). There should be controlled access to captured video footages as they contain personal data.

A4) Use of Information Technology and Online Services

Hardware and Software Installation, Modification and Removal

Description/Rationale
At appropriate times, when the IT needs of Prosec 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, Prosec's employees may be bringing in their own laptops, tablets, portable storage and mobile devices to connect to the Company'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 Prosec, and the bringing in of own devices by employees.

Risk/Exposure
Without proper policies and approval mechanisms governing the installation, modification and removal of hardware and software within Prosec, and the authorisation for people to bring in their own devices, the integrity and performance of the IT infrastructure could be compromised.

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

Personal computing devices, including tablets, smartphones, portable hard drives and USB thumbdrives, must not be used for storing personal data unless the relevant devices are protected via screen locks, passcodes and encryption.

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

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

As an additional level of security, Prosec will enter the MAC addresses of the authorised and approved desktop computers, laptop documents and other devices so that only these can have access to Prosec's IT networks and resources.

Prosec will implement appropriate security measures to prevent unauthorised copying or exporting of the Company's data via the USB ports of the desktop and laptop computers being used by Employees. Employees can only copy Prosec's data to the Company's servers based on technical settings by IT Department.

Users are responsible for ensuring that their own laptop computers and authorised portable storage devices containing personal data 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 data are easily and widely transmitted and shared among Prosec's employees and even third-parties, one of the main threats is the infection by malicious code, viruses, Trojans, worms, malware, spyware, ransomware, etc introduced via shared thumbdrives, web browsing or downloading of apps. Therefore it is extremely important for Prosec 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, ransomware, etc, the entire computer network, computer systems and databases within Prosec 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, ransomware, etc and to report suspicious infection or incidents to the responsible parties.

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 share personal data. These could be sited within Prosec or hosted in the cloud through external cloud service providers (e.g. Dropbox, Google Drive, iCloud). There should be proper control mechanisms to protect the personal data and to restrict access to authorised persons only.

Risk/Exposure
Shared drives and folders could be easily hacked into and the personal 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, iCloud).

When using local shared folders within departments, the shared folders should be password-protected at a minimum (even if it is a shared password). In addition, the shared files within the shared folders that contain more sensitive personal data should be individually password-protected, and where practical, be encrypted.

Protection of Electronic Document

Description/Rationale
Within Prosec, and between Prosec and third-party organisations, a lot of electronic documents containing personal 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 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 documents containing personal data should be password protected or encrypted. Transmission of such documents should be done over secure and encrypted networks (e.g. via virtual private networks (VPN)).

Personal 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 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 data on the computer screens, whether accidentally or deliberately, resulting in information leakage and exposure.

Preventive Measure/Action
All users should enable the screen lock function or screen saver with password/PIN feature on their computers and mobile devices. As a good practice, the IT Department should implement automatic screen lock functions on all computers within Prosec.

Protection of Mobile Devices

Description/Rationale
Mobile computing devices (e.g. tablets, smart phones) used by Prosec's employees could contain personal data, which must be adequately protected.

Risk/Exposure
When mobile devices are misplaced, lost or stolen, the personal 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.

Public Areas with WiFi

Description/Rationale
Prosec's employees may need to connect to public WiFi networks using mobile devices while on the move or outside Prosec's premises. The personal data stored in their mobile devices could be compromised when connecting to such networks, especially the unprotected WiFi networks.

Risk/Exposure
Main areas of risk/exposure include malware downloaded to the mobile devices without the user's knowledge. The mobile devices may also be subject to virus attacks or hacking. The user could also be susceptible to identity theft.

Preventive Measure/Action
To minimise risks from public WiFi networks, it is best to avoid connecting to unsecured networks (i.e. those that do not require passwords to connect). As a minimum, all mobile devices should have firewalls and anti-virus software installed. Personal data should be encrypted as far as practicable.

Safeguard Against Phishing

Description/Rationale
There are bogus websites and emails that masquerade as originating from bona fide organisations to trick the unsuspecting user into revealing personal data such as NRIC number, credit card details or passwords ("Phishing"). All Prosec staff must guard against this.

Risk/Exposure
If the Prosec staff is not vigilant, he/she may inadvertently give away personal data on phishing websites or click on URL links or file attachments in emails that contain malware. Worse, the user could be susceptible to identity theft or he/she be held ransom by ransomware that encrypts his/her data and render it unreadable.

Preventive Measure/Action
All staff must be vigilant and be on the lookout for websites and emails that look suspicious. Some precautions to take are:

- Do not click on the URL link or file attachment in emails where the content looks dubious. For example, asking you to update the password to your banking account when you have not been using Internet banking for years. The more likely scenario is that you have forgotten your password and you request the bank to reset your password.
- Check the actual source of the email or website posting by hovering your mouse over the sender's email address or the website's URL or the embedded URL. You may discover that the source is not what you expect it to be. This 'mouse' check, however, cannot be done on a mobile device.
- Be careful when using unsecured websites asking for personal data. Avoid websites whose URLs do not have the *https* prefix or the symbol of a 'lock'.
- Watch out for impersonal messages (e.g. "Hello" without addressing you by name) in emails purportedly from official government or Prosec sources dealing with a personal matter. Other giveaways include lots of grammatical errors in the messages.

Safeguard Against Social Engineering

Description/Rationale
People with malicious intent use social, non-technical means to trick the unsuspecting individual to part with his/her personal data ("Social Engineering"). All Prosec staff must guard against this.

Risk/Exposure
If the Prosec staff is not vigilant, he/she may inadvertently give away personal data to people with malicious intent via the telephone, other communications media or even in face-to-face interactions.

Preventive Measure/Action
All staff must be vigilant and not fall victim to so-called 'social engineers'. Some precautions to take are:

- Always verify and authenticate the identity of the person who is asking you to disclose personal data. You should do this even for someone who claims that he/she has been referred to you by a friend or colleague. You should verify with your friend or colleague to ensure this is indeed the case.

- Always ask the requester for the purpose of wanting access to the information.
- Always ask the requester to write in to Prosec officially.

Safeguard Against Website Attacks

Description/Rationale
People with malicious intent can modify online websites to 'steal' personal data from unsuspecting users by tricking them into believing that they are providing information to access the website's services. All Prosec staff must guard against this.

Two common techniques used by the malicious 'attacker' are SQL injection and cross-site scripting. The 'attacker' carries out the malicious act by injecting software codes or scripts into the website's input screens (where the user inputs the User ID and Password) or online forms (where the user inputs certain personal data), and redirecting the 'stolen' data to their own databases.

Risk/Exposure
If the Prosec staff is not vigilant, he/she may inadvertently be tricked into giving away his/her log-in credentials or personal data, resulting in identity theft. Worse, the injected software code could insert inappropriate data into Prosec's database, delete data from the database or shut a database down.

Preventive Measure/Action
Prosec should carry out regular vulnerability assessments and penetration tests of their websites and online applications. IT Department should ensure that databases are properly configured and that the database codes on the websites are written with tighter controls to minimise the risks from website attacks.

Use of Social Media

Description/Rationale
The use of social media platforms such as Facebook enables Prosec to do mass promotion or marketing of its products and services. It can also serve as an alternative channel for customers to share with their friends or the general Facebook user population what they like or dislike about Prosec's products and services. So it is like a 'double-edge' sword that may enhance or harm Prosec's reputation.

Risk/Exposure
On social media platforms, users tend to be more casual in their conversations and more open in sharing personal data. Prosec staff, thinking that they are acting in their personal capacity, may inadvertently disclose personal data which they are not supposed to, without realising the consequences. With powerful search engines and Big Data analytics tools it is easy to trace the individual staff's association or relationship with Prosec.

Preventive Measure/Action
A Social Media Policy spelling out rules on what information can or cannot be posted on social media should be implemented so that all Prosec staff are aware of their 'boundaries' in sharing information on social media platforms.

A5) Third Party Outsourcing

Prosec 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 Prosec's
- 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 the Data Protection Officer or Head, IT Department.

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