

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

AMENDMENTS LOG

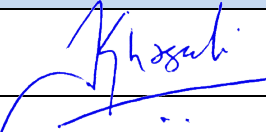
Revision History

Version	Date	Revision Author	Summary of Changes
1.0	10 June 2024	Edwin Soedarta DPO	First Release

Distribution

Name	Location
<i>All employees</i>	<i>Shared Folder</i>

Review & Approval

Name	Position	Signature	Date
Khasali M	Director		10 June 2024

THE SOFTWARE PRACTICE PTE LTD	No of Pages	2 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

TABLE OF CONTENTS

RECORDS FOR DOCUMENT REVIEW 3

PURPOSE 4

SCOPE AND APPLICABILITY 4

RESPONSIBILITIES & AUTHORITIES..... 4

POLICY 01 – ACCEPTABLE USE POLICY 5

POLICY 02 – INFORMATION CLASSIFICATION POLICY..... 6

POLICY 03 – INFORMATION TRANSFER & COMMUNICATIONS SECURITY POLICY 7

POLICY 04 – E-MAIL POLICY 9

POLICY 05 – ACCESS CONTROL POLICY 11

POLICY 06 – PASSWORD POLICY 13

POLICY 07 – POLICY ON SUPPLIER RELATIONSHIPS 15

POLICY 08 – CLOUD COMPUTING POLICY 16

POLICY 09 – IP & COPYRIGHT COMPLIANCE POLICY 17

POLICY 10 – BUSINESS CONTINUITY POLICY 18

POLICY 11 – AVAILABILITY POLICY 19

POLICY 12 – RECORDS MANAGEMENT POLICY 20

POLICY 13 – DATA RETENTION & DESTRUCTION POLICY 21

POLICY 14 – REMOTE WORKING POLICY 22

POLICY 15 – CLEAR DESK & CLEAR SCREEN POLICY 23

POLICY 16 – REMOVABLE STORAGE MEDIA POLICY 24

POLICY 17 – USER ENDPOINT DEVICE POLICY 25

POLICY 18 – POLICY ON VULNERABILITY MANAGEMENT AND DISCLOSURE 26

POLICY 19 – MALWARE PROTECTION POLICY 27

POLICY 20 – BACKUP POLICY 28

POLICY 21 – LOG MANAGEMENT POLICY 29

POLICY 22 – SOFTWARE SECURITY POLICY 30

POLICY 23 – NETWORK SECURITY POLICY 31

POLICY 24 – CRYPTOGRAPHY POLICY..... 32

POLICY 25 – SECURE DEVELOPMENT POLICY 34

POLICY 26 – CHANGE MANAGEMENT POLICY..... 36

THE SOFTWARE PRACTICE PTE LTD	No of Pages	4 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

PURPOSE

The Software Practice Pte Ltd has identified a set of policies in a wide variety of information security areas. These policies and their main objectives have been specified in this document for organization wide implementation.

The purpose of the policies is to provide a high-level framework for:

- Addressing and managing security risk;
- Developing and implementing security standards and guidelines;
- Effective security management practice; and
- Increase customers' confidence in the organisation's dealings.

SCOPE AND APPLICABILITY

The scope of these policies covers all information and applies to all persons working for or on behalf of The Software Practice Pte Ltd.

Any staff who found to have violated any of the policies applicable to them might be subject to disciplinary action. Any third party found to have violated any of the policies applicable to them will be investigated and may be subject to termination of contract and/or contractual claims.

RESPONSIBILITIES & AUTHORITIES

The organisation will keep all these policies current and relevant. Therefore, from time to time, it may be necessary to modify and amend some sections of the policies or to add new ones.

This document shall be reviewed at least once a year and/or if significant changes occur by the DPO and the The Management. The review must ensure that changed requirements are captured and feedback from process owners and other relevant interested parties are considered.

Information security is the responsibility of each and every individual working for or on behalf of the organisation.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 01 – ACCEPTABLE USE POLICY

OVERVIEW

The Software Practice Pte Ltd is committed to ensuring all staff actively address information security and compliance in their roles.

This policy specifies acceptable use of end-user computing devices, and other organisation’s assets and technology. Additionally, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

POLICY STATEMENT

The organisation requires that:

1. Staff must agree and sign terms and conditions of their employment contract, comply with rules of acceptable use and accept their user responsibilities. The same would apply to third-party users, where applicable, and as stipulated in their contracts.
2. Staff will go through an onboarding process that familiarizes them with the environments, systems, and information security requirements, and procedures the organisation has in place.
3. Staff offboarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any organisation’s systems has been removed, as well as ensuring that all organisation owned assets are returned.
4. Use of the organisation’s computing systems is subject to monitoring. A fair disciplinary process will be utilised for employees that are suspected of committing information security breach.

The organisation requires all users to comply with the following acceptable use requirements which include the following:

1. Staff must use either authorized devices or virtual machines for all business related work.
2. Staff may not leave computing devices used for business purposes, unattended in public, and ensure they are not overlooked by unauthorised people when working.
3. Use only those user credentials which they are provided with, and protect their user credentials.
4. Not attempt to bypass or subvert system security controls.
5. All documents and data storage devices must be managed according to the data classification, securely stored, and correctly destroyed or deleted when no longer needed.
6. Staff may not post any confidential information including another individual’s personal data in public forums or chat rooms.
7. The organisation’s internet connection and email should only be used to complete job duties and to seek out information that can be used for work.
8. Staff must fulfil their information security responsibilities on the succeeding policies.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	6 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 02 – INFORMATION CLASSIFICATION POLICY

OVERVIEW

The Software Practice Pte Ltd shall classify and maintain appropriate protection of information. Information classification ensures that individuals who have legitimate right to access a piece of information can do so while also ensuring that the information is protected from those who have no right to access them. This shall also help ensure that correct classification and handling methods are applied to their day-to-day activities and are managed accordingly.

POLICY STATEMENT

Information must be classified into one of the following categories by those who own / or are responsible for the information e.g., asset owner / record custodian.

Level	Classification	Description	Examples
1	Public (Unclassified)	Freely available outside of the organisation or is intended for public use. No classification mark required, and will not be assigned a formal owner or inventoried.	<ul style="list-style-type: none"> • Online public information • Website information • Public corporate announcements
2	Internal	May be freely shared within and among staff, but must not be shared with third parties unless a non-disclosure agreement has been signed.	<ul style="list-style-type: none"> • Internal policies and operating procedures • Interoffice memorandums • Internal meeting minutes
3	Confidential	Highest level of classification. Highly sensitive information that may be directly or indirectly damaging to the organisation or to the information owner, if disclosed.	<ul style="list-style-type: none"> • Personal data • Information about customer and the business that the company is obliged to protect, with local laws taking precedence • Product or system development information or marketing strategies • Information on mergers, acquisitions, or divestitures, prior to general or public disclosure • Identification and authentication information • Any form of cryptographic key

THE SOFTWARE PRACTICE PTE LTD	No of Pages	7 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 03 – INFORMATION TRANSFER & COMMUNICATIONS SECURITY POLICY

OVERVIEW

This policy lays out the guidelines that need to be applied in undertaking a transfer of information including personal data in and out of the organisation and the supporting communication facilities in The Software Practice Pte Ltd.

POLICY STATEMENT

A. Initial Considerations

Before you undertake any transfer of information, ensure you have the appropriate authorization to do so. Bear in mind any restrictions in place for the sharing or transfer of organisation’s information.

- Never automatically assume someone is entitled to the information just because they have told you they need it, regardless of whether they are an internal or external requester.
- Think about whether a non-disclosure agreement is required to cover security and use of the data.
- Check that you are not providing more information than is necessary for the identified purpose.
- Check if objective / purpose can be met using anonymised data instead of personal data.
- Consider the most appropriate (not necessarily the easiest) transfer or access method.
- For all transfers of confidential information, it is essential that you appropriately establish the identity and authorisation of the recipient.

All exchanges of information classified as confidential information must be conducted on the basis of formal agreements between the sender and receiver based on legal or justifiable business purpose. Specifically, for personal data, disclosure shall only be made if consent for the purpose of disclosure has been obtained, unless an exception in the privacy law / regulation applies.

B. Telephone / Mobile Phone

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, care must be taken as follows:

- Information classified as confidential must not be discussed over the telephone unless you have confirmed the identity and authorisation of the recipient, and no unauthorized personnel is able to overhear.
- When using voice-mail, do not leave confidential information. Only provide a means of contact and wait for the recipient to speak to you personally.
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing.

F. Internet-based Collaborative Sites

THE SOFTWARE PRACTICE PTE LTD	No of Pages	8 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

Only authorized sites shall be allowed for use for file sharing and collaboration with proper access rights set up. To access the authorized file transfer sites, users shall use their company issued e-mail ID for activity tracking purposes.

G. Sending Information by Post

You, as the sender, are responsible for making sure that:

- The postal address is correct.
- The envelope is clearly marked for the attention of the intended recipient.
- No information has been included in error.
- Only approved courier is used for the transfer with appropriate tracking mechanism.

An extra level of protection must be applied when sending confidential information. It is essential that the document or file, whether sent on a media device or in paper form, is kept secure in transit, tracked during transit, and delivered to the correct individual.

- The package is securely and appropriately packed, clearly addressed and has a seal, which must be broken to open the package.
- The package must have a return address and contact details.
- The package must be received and signed for by the addressee e.g., the use of special or recorded delivery.
- Successful delivery / transfer of the item must be checked as soon as possible. Any issues must be reported immediately to The Management.

H. Hand Delivery / Collection

Hand delivery or collection of a document or a media is also an approved method of transfer. Remember however, if you are taking company asset off site or when arranging for an individual to collect information, you must satisfy yourself that the authorized recipients are who they say they are and verify their identification.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	9 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 04 – E-MAIL POLICY

OVERVIEW

E-mail system is designed to improve services to customers, enhance internal communications and reduce paper work. E-mail system has different risks than other forms communications. This policy is developed to ensure establishment of strict and appropriate controls for secured e-mail communications.

POLICY STATEMENT

Due to the importance of e-mail as a communication tool, the following shall be followed for e-mail systems which is intended to be used only for business purposes.

A. E-mail ID

1. There shall be an official e-mail ID provided to authorized employees, and official communication shall be executed only through these e-mail IDs.
2. The organisation's reserves the right to:
 - Decide e-mail IDs to users
 - Deny an e-mail ID to any individual or team or deny access to official e-mail ID to its users for security reasons, such as, to those who try to access it remotely via public computers
 - Access, read, review, monitor, copy, intercept, block or auto forward e-mails and files on its system for legitimate business reasons, without prior notice

B. E-mail Usage

1. All e-mail messages using the company email system are the property of the organisation and the organisation has the right to access and monitor any and all such messages whenever required to present to law enforcement agencies or third party or for legitimate business reasons without consent of the user.
2. Each user is responsible for all e-mail sent from his/her account. Users must use only their own e-mail account.
3. Any use of the company e-mail is easily traceable and therefore these activities must be conducted with the reputation, decency and appropriate content in mind.
4. A standard email confidentiality disclaimer should be mandatory for all e-mail traversing the Internet.

C. E-mail Content

THE SOFTWARE PRACTICE PTE LTD	No of Pages	10 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

1. Messages must not contain any material that may reasonably be considered offensive, disruptive, defamatory, or disparaging towards any employee or to the organisation.
2. Offensive content includes, but not limited to sexual comments or images, racial or religious slurs, and gender-specific comments.

D. Prohibited E-mail Activities

1. Users must not forward or otherwise propagate chain letters or pyramid schemes to lists or individuals, and any other types of use, which may unnecessarily consume system resources or otherwise interfere with the work of others.
2. Users are explicitly prohibited from sending unsolicited bulk mail messages (“junk mail” or “Spam”). This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, and political tracts.
3. Malicious e-mail, including but not limited to “Mail bombing” (flooding a user or site with a very large or numerous pieces of e-mail), is prohibited.
4. Users must not post server configuration information about any company machine. This includes internal TCP/IP addresses, server names, server types, or software version numbers. Use Bitwarden if required.
5. Impersonation is not permitted. Users must identify themselves by their real name; pseudonyms that are not readily attributable to actual users are not allowed. Users may not represent themselves as another user.
6. Personal data must be encrypted or password-protected (and password must be sent via a different channel), if to be sent through e-mail.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	11 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 05 – ACCESS CONTROL POLICY

OVERVIEW

This policy is designed to minimize risk to organizational resources and information by establishing the privileges of users to the minimum allowable while still allowing them to perform job functions without undue inconvenience.

The objective of the policy is to ensure that:

- An authentication mechanism, commensurate with the sensitivity and criticality of the information asset, is set up.
- Access of information system assets is by authorized users only.
- All actions of users are logged.

POLICY STATEMENT

1. A formal procedure for logical access control granting and revoking access to all information systems and services shall be documented, implemented and maintained.
2. All users shall have a unique identifier (user ID) for their own use so that activities can be traced to the responsible individual for all types of users.
3. Access to information and information processing facilities shall be granted only to authorized users in accordance with the least privilege and "need-to-have" principle based on the need for business and security requirements.
4. Request for granting any access shall be accepted only with approvals from the authorised approver(s).
5. The System Administrator shall create user ID for access to information asset after receiving approved requests from the competent authority.
6. All users of the information systems shall be responsible for taking due care in the use and operation of the information systems through their user ID. Users shall be responsible for any activity carried out through their user IDs.
7. Password policy shall be enforced technically and adequate mechanism be placed to create and communicate user password to ensure password security.
8. Users with system or application administrative roles shall be authenticated with 2 factor authentication especially for Google, Microsoft and Bitwarden accounts.
9. An account shall be locked out at a maximum of 5 failed login attempts, and a locked account shall remain as locked until an administrator explicitly unlocks it.
10. All access to the servers, infrastructure and database systems shall be done through a secure channel (such as SSH), and all access shall be logged to facilitate independent reviews of the access and transactions completed.
11. All servers, infrastructure and database systems shall be configured with timeout and automatic logout feature for non-active sessions.
12. Privileged IDs shall be different from those that are to be used for normal business use. Special care shall be taken in allocating and reviewing privileged IDs.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	12 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

13. Use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
14. For all external users (contract employees, consultants, vendors, temporary staff etc.), all user IDs, on creation and renewal, shall require written approval from The Management, and have an expiry date that coincides with the conclusion of the contracted project.
15. An account shall be suspended under the following conditions:
 - a. inactive for more than 60 days;
 - b. when a user is on leave for more than 60 days;
 - c. on the last day of exiting staff; and
 - d. immediately (within the same day) when notification is received upon unfriendly terminations and termination of vendors.
16. Single user logon session must be implemented if the ICT system is able to support this feature, to ensure that users cannot log on to multiple sessions at any given time using the same user credentials. Multiple logon sessions are allowed only if there is a business requirement to do so.
17. A log should be maintained of new, modified, and revoked accounts.
18. Appropriate consistency checks should be deployed for ensuring acceptable changes in access control system.
19. All major events relating to use and access of information system assets shall be logged / monitored. It shall be ensured that all access is granted on a need-to-have basis and strictly controlled to reduce the exposure of unauthorized activities. Such access shall be reviewed on a quarterly basis and removed promptly when not required.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	13 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 06 – PASSWORD POLICY

OVERVIEW

Passwords are the most commonly used authentication mechanism. This policy shall govern the creation and protection of passwords to prevent their compromise.

POLICY STATEMENT

General

We identify all our access points in three categories:

- Endpoints: User endpoints (Laptops) have password-based login subject to yearly rotation.
- Cloud Systems: All cloud systems must require passwords and MFA must be enabled.

Note: All passwords must conform to the guidelines described below:

1. All systems and application shall adhere to this password policy.
2. System Administrators shall determine and enforce appropriate controls to
 - Ensure use of complex passwords:
 - i. At least 16 characters long
 - ii. Contain characters from at least 3 of the 4 categories: uppercase (A through Z), lowercase (a through z), digits (0-9), special characters (symbols)
 - Lock out an account at a maximum of 5 failed login attempts. A locked account shall remain as locked until an administrator explicitly unlocks it.
 - Enable Multi-Factor Authenticator for cloud systems
3. The use of passphrases (concatenation of words or text or special character) is encouraged.
4. Passwords shall not be stored displayed in clear text, and unprotected (plaintext) electronic mail messages must be avoided.
5. Password must not be transmitted or stored in plaintext.
6. Only password hashes and salts are stored.
7. Password shall be stored on Company prescribed secure password manager to protect against dictionary or brute-force attack.
8. Initial or reset password shall be changed by user upon first use. Users shall be allowed to select and change their own password.
9. Password shall not be the same as the account ID or user ID.
10. User identity shall be verified before performing password reset.
11. System Administrators shall ensure to change all default passwords provided by vendors.
12. Use of Group user-ID/password shall be limited to situations dictated by operational necessity and approved by The Management.
13. Passwords of generic user ID administrative must be changed frequently and as soon as possible when a privileged user leaves or changes job.
14. Password leakage shall be treated as a serious information security incident and dealt with a disciplinary action.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	14 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

15. Passwords and other forms of user credentials shall not be shared with anybody. The breach of this practice is a serious act of indiscipline.
- Using the credentials of another user is prohibited.
 - Disclosing password to anyone is not allowed.
 - Privileged/administrative access should be used only for purposes authorized for / originally intended. Abuse of entitlements is a serious act of indiscipline.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	15 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 07 – POLICY ON SUPPLIER RELATIONSHIPS

OVERVIEW

The purpose of this policy is to ensure appropriate control over security exposures and risks on services provided by suppliers.

POLICY STATEMENT

1. Selection / appointment of a supplier shall be made in accordance with the organisation’s purchasing requirements.
2. Due diligence assessment will be conducted prior to selection to assess information security practices of the supplier.
3. Service level agreement shall be defined with the supplier and contracts shall be signed with clearly defined clauses on information security and personal data protection (if applicable). Agreements with supplier shall specify whether personal data is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and data protection obligations.
4. Supplier agreements shall clearly spell out their responsibilities taking into account the type of personal data processed. The organisation shall specify in contracts with the supplier that personal data is only processed on the organisation’s instructions.
5. All information technology related activities performed by supplier shall be assessed for security and personal data exposures and risks while providing access to them.
6. An agreement to comply with all applicable policies and procedures of the organisation concerning information security and personal data handling and protection during exchange of information or information asset shall be signed with the supplier including confidentiality or non-disclosure agreements and data processing agreement covering data protection obligations where personal data processing is involved.
7. Service assessment and review of outsourced services shall be carried out. The supplier agreement should state that the organisation has the right to audit the supplier’s compliance with applicable legislation and/or regulation relating to personal data, where needed.
8. Supplier shall bring to the notice of the organisation any weakness, incident relating to information security during their period of contract immediately upon their detection without undue delay.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	16 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 08 – CLOUD COMPUTING POLICY

OVERVIEW

This policy outlines best practices in relation to the use of cloud computing services provided by cloud service provider (CSP) to support the processing, sharing, storage and management of information.

POLICY STATEMENT

It is the organisation’s policy in the area of cloud computing that:

1. Appropriate assessment must be carried regarding the use of cloud services including a full understanding of the information security controls implemented by the CSP.
2. Due diligence must be conducted prior to sign up to a cloud service to ensure that appropriate controls will be in place to protect confidential information. Preference will be given to CSP who are certified to information security / data protection compliance certification such as DPTM, APEC-CBPR or APEC-PRP, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017, ISO/IEC 27018, Tier 3 of the Multi-Tiered Cloud Security (MTCS).
3. Activities such as backup and recovery, patching, encryption, log management, malware protection and incident management must be clearly determined prior to the commencement of the cloud service.
4. Only approved features and functionality from CSP shall be used to ensure information security.
5. Sufficient logs monitoring must be available to allow the organisation to understand the ways in which data is being accessed and to identify whether any unauthorized access has occurred.
6. For cloud provider network products used by the organisation, the organisation shall rely on the certifications of the cloud provider to ascertain network services and components and to ensure technical compliance.
7. Information stored in cloud services must be encrypted at rest and in transit.
8. All organisation’s data must be removed from cloud services in the event of the subscription is coming to an end. Data must not be stored in the cloud for longer than is necessary to meet legal or justifiable business reasons.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	17 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 09 – IP & COPYRIGHT COMPLIANCE POLICY

OVERVIEW

This policy addresses intellectual property and copyright compliance.

POLICY STATEMENT

- We respect the intellectual property (IP) and conduct our business in compliance with the IP-related laws as applicable and agreements with other companies, and take into account any relevant IP-protection risks in our risk assessment.
- We protect any material that can be considered IP or proprietary products through the following:
 - Acquiring software only through known and reputable sources, to ensure that copyright is not infringed upon;
 - Maintaining proof and evidence of ownership of licenses, manuals, etc.
 - Ensuring that any maximum number of users or resources permitted within the license is not exceeded;
 - Carrying out reviews to ensure that only authorized software and licensed products are installed;
 - Complying with terms and conditions for software and information obtained from public networks and outside sources;
 - Not duplicating, converting to another format or extracting from commercial recordings (video, audio) other than permitted by copyright law or the applicable licenses;
 - Not copying, in full or in part, copyrighted standards, books, articles, reports, or other documents, other than permitted by copyright law or the applicable licenses.
- We actively protect our own IP. All intellectual property created in the course of employment or during contracted work belongs to the organisation by default, unless different arrangements between the author and the organisation were made prior to performing the work.
- Knowledge or possession of IP and other proprietary information shall be strictly limited on a “need to know” basis, and we execute written confidential or non-disclosure agreements prior to sharing the information.
- We do not infringe a third party’s intellectual property in our products, services, or components, or disclose or use a third-party’s intellectual property without the express or explicit consent of the owner or as permitted by law or license(s).
- We do not purchase or use counterfeit or other infringing goods and services in running our business, including counterfeit trademark goods or infringing copyright material (such as software, publications, video, audio, or other content).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	18 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 10 – BUSINESS CONTINUITY POLICY

OVERVIEW

This policy is designed to embed information security continuity in the organisation’s business continuity management and to ensure availability of information systems and data.

POLICY STATEMENT

The organisation must implement plans, processes, and procedures in order to ensure the reconstitution of the various components of the business systems in case of catastrophic systems failure.

1. The Management must ensure that the continuity of information security is captured within the business continuity management and disaster recovery plan (DRP) of the organisation with the following elements:
 - An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
 - Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security safeguards are nominated; and
 - Documented plans, response and recovery procedures are developed and approved.
2. Documented plans, response and recovery procedures must provide guidance when hardware, software, or services become critically dysfunctional or cease to function (short- and long-term outages).
3. The organisation must verify the established plans, response and recovery procedures in order to ensure that they are valid and effective during adverse situations.
4. The organisation shall review the validity and effectiveness of information security continuity measures when information systems, information security processes and controls, or business continuity / disaster recovery management and solutions change.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	19 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 11 – AVAILABILITY POLICY

OVERVIEW

This policy is designed to define requirements for proper controls to protect the availability of the organisation’s information systems.

Within this policy, an availability is defined as a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed.

POLICY STATEMENT

1. Information systems must be consistently available to conduct and support business operations.
2. Information systems must have defined availability requirements, and appropriate redundancy and failover plan that meets these requirements.
3. System failures must be reported promptly to the Incident Response Team.
4. Users must be notified of scheduled outages (e.g., system maintenance) that require periods of downtime. This notification must specify the date and time of the system maintenance, expected duration, and anticipated system or service resumption time.
5. Prior to use, each new or significantly modified application must have a completed risk assessment that includes availability risks.
6. Capacity management and load balancing techniques must be used, as deemed necessary, to help minimize the risk and impact of system failures.
7. Information systems must have an appropriate data backup plan that ensures:
 - All sensitive data can be restored within a reasonable time period.
 - Full backups of critical resources are performed as per the organisation’s [Backup Policy](#).
 - Test of backup data and configurations must be conducted at least once a year.
8. Information systems must have an appropriate disaster recovery plan in line with the organisation’s [Business Continuity Policy](#).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	20 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 12 – RECORDS MANAGEMENT POLICY

OVERVIEW

This policy ensures the identification and protection of records that are of significant value to the business, and those that are required for compliance with the organisation’s policies, legal and regulatory requirements.

POLICY STATEMENT

1. The organisation shall ensure that records of significant value are identified and retained securely over a specified retention period.
2. Identification of such records will be based on their value to the business and to applicable legal, statutory and contractual requirements.
3. All record owners shall store and retain relevant records in accordance with laid down asset classification and handling guidelines of the organisation.
4. All records shall be protected from loss, damage, fabrication, and falsification in accordance with business and statutory requirements.
5. Record owners shall cease the retention of the records at the end of the specified retention periods and when it has been determined that it no longer serves the legal or business retention purpose.
6. At the end of the retention period, record owners shall ensure that records are disposed of securely and non-retrievable as required by its data classification. For more details, refer to the organisation’s [Data Retention and Destruction Policy](#).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	21 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 13 – DATA RETENTION & DESTRUCTION POLICY

OVERVIEW

The Software Practice Pte Ltd commits to protecting the data provided by employees, customers and external providers or partners. The organization is committed to the protection of this data while under its responsibility, and its destruction when the organization determines that the legal or business purpose for retaining them is no longer necessary.

POLICY STATEMENT

A. Data Retention

The organization has implemented a data retention policy designed such that data are retained in a uniform format for a specified period based on a defined retention schedule. Data owners/custodians shall be responsible for the following:

- Retains data based on legal, regulatory and business requirement, including maintaining the continuity and its availability in the event of a disaster.
- Retains data relevant to pending or reasonably anticipated legal proceedings, consistent with the organization’s legal obligations.

B. Data Destruction

The organization has implemented a data destruction policy that specifies guidelines related to the destruction of documents that are no longer required for business or legal reasons. The method for proper document destruction and disposal shall in line with the table below:

Data Classification	Method of Destruction	Recyclable?
Public	Hardcopy: Dispose Softcopy: Delete	Yes.
Internal	Hardcopy: Shred off and Dispose Softcopy: Delete	Yes. Recycle for internal doc reference only
Confidential	Hardcopy: Shred off (using at least P-3 security cross cut shredder) and dispose Softcopy: Delete from storage media and reformat before reuse of the media. Sanitise or physically destroy the media if it will be disposed of. If 3 rd party is engaged, a due diligence assessment is to be conducted, a data processing agreement shall be prepared and a certificate of destruction shall be requested.	No.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	22 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 14 – REMOTE WORKING POLICY

OVERVIEW

This policy sets out the key information security related elements that must be considered in agreeing a teleworking or remote working arrangement. It ensures that all of the necessary issues are addressed and that the organization's information and associated assets are protected.

POLICY STATEMENT

The organisation embraces remote working to drive its workforce mobility. However, remote working arrangements must take into account several factors such as confidentiality, integrity and availability of information being handled, and suitability of the teleworking technology and security measures.

A. Equipment

1. Arrangements must be in place to ensure that any remote working solutions that must be provided are fully supported and maintained.
2. Remote working solution must support adequate data backup and teleworkers must understand the backup procedure.
3. Any equipment which provides remote access to the organisation's systems, and the authentication method that it uses to access organization's resources, must be verifiable.
4. Where a teleworker handles confidential information, they must be provided with file encryption tools.

B. Security of Information in Remote Working Arrangements

1. Staff must not put the organisation information at risk by using other less secure equipment.
2. If remote administration to server or applications is needed, adequate technologies must be used to guarantee that no risk is placed in implementing remote access. In particular, the following must be followed:
 - All remote access sessions shall only be done from specific systems and filtering based on IP address shall be implemented.
 - Security controls to protect against malware spread originating from remote connections must be implemented.
 - All remote access sessions must be authenticated using two-factor authentication mechanism.
 - Split tunnelling shall not be used for remote access.
 - Logging of the date time, IP addresses of the source and destination systems, user information as well as the type of action performed shall be enabled on the servers that allow remote access.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	23 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 15 – CLEAR DESK & CLEAR SCREEN POLICY

OVERVIEW

The purpose of this policy is to establish a culture of clear desk and clear screen. This is to ensure that all work stations are clear of information, whether in electronic or paper form, to reduce the risks of unauthorized access, loss of and damage to information.

POLICY STATEMENT

1. Whenever unattended or not in use (e.g., if you leave your desk for any reason), all workstations must be left logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism.
2. A password-protected screen saver must be enabled on workstations and automatically activated after 10 minutes of inactivity.
3. When viewing confidential information on a screen, users must be aware of their surroundings and must ensure that unauthorized parties are not permitted to view the information.
4. Passwords must not be posted on or under a computer / desk or in any other accessible location.
5. The organisation shall restrict the creation of hardcopy material and use of removable storage media to the minimum needed to fulfil the identified processing purpose. All hardcopies of confidential information must be kept in a locked storage and must be secured until the time that they can be shredded or their retention period ends.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	24 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 16 – REMOVABLE STORAGE MEDIA POLICY

OVERVIEW

This policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

Removable media devices that may be allowed in the organisation include, but are not restricted to the following:

- External hard drives
- USB memory sticks (flash drives)
- External SD memory cards

POLICY STATEMENT

- Removable media should only be used to store or transfer information as a last resort. Under normal circumstances, information should be stored on corporate systems and exchanged using appropriately protected and approved information exchange connections.
- Use of media devices for information classified as confidential shall only be allowed if there's a business need for it. The following shall be enforced for the use of media devices, when allowed.
 - The media must be encrypted or password protected. The password itself must be conveyed to the recipient in a separate communication from that covering the information itself.
 - Report any issues to Incident Response Team and in the case of missing removable storage device or corrupted data immediately.
- Should access to, and use of, removable media be approved, the user is responsible for the appropriate use and security of data and for not allowing removable media, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.
- Virus and malware checking software must be operational on the company devices from which the data is taken and on to which the data is to be loaded.
- Special care must be taken to physically protect the removable media and stored data from loss, theft or damage.
- Any removable media for reuse must have their contents erased prior to reuse. All removal media that are no longer required, or have become damaged, must be securely disposed in line with the organisation's [Data Retention and Destruction Policy](#).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	25 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 17 – USER ENDPOINT DEVICE POLICY

OVERVIEW

The use of desktops, laptops, mobile, and other endpoint devices (hereafter referred to as user endpoint devices) are integral to the working environment. Many user endpoint devices are increasingly mobile, which significantly increases the risk to the security of information both contained on and accessed by these devices. This policy addresses that risk by establishing the responsibilities of users to maintain the security of data that is stored, accessed, or transmitted via user endpoint devices.

POLICY STATEMENT

A. Guiding Principles

- Everyone who uses a user endpoint device to access organisation data or resources are responsible for securing such devices, regardless of ownership (company-issued or allowed personal devices), against data compromise according to this policy.
- All software installed on company-issued endpoint devices must be suitably licensed for use. Installation or use of any software in violation of its license, or of pirated software, is not allowed.
- The organisation reserves the right to access and review any company-issued endpoint devices, without advance notice. For allowed personal devices, the user agrees that the organisation has the right to audit the device as and where needed (e.g., for the purposes of incident investigation).

B. User Responsibilities

When using an endpoint device, whether personally or company-owned, to access the organisation’s data or resources, all users must be aware of, and agree to, and adhere to the following:

- Comply with the organisation’s [Acceptable Use Policy](#).
- Meet minimum security standards for endpoint devices:
 - Uses operating systems for which updates are available when security vulnerabilities are discovered.
 - Third-party authorized applications are updated and patched when patches become available.
 - Must require password authentication in line with the organisation’s [Password Policy](#).
 - Anti-virus software is installed.
 - Enable inactivity timeout of no more than 10 minutes to prevent unauthorized access to an unattended device. Password authentication must be required to unlock the device.
- Report a known or suspected compromise, including theft or loss of any endpoint device that may contain organisation’s data or has stored credentials providing access to the data to IT immediately.
- Delete all organisation’s data for all allowed personally owned devices upon termination of employment or relationship with the organisation.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	26 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 18 – POLICY ON VULNERABILITY MANAGEMENT AND DISCLOSURE

OVERVIEW

A vulnerability is commonly defined as “an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.”

The organisation policy with respect to technical vulnerabilities is to be aware of them and timely address them.

POLICY STATEMENT

A. Sources of Information

Information about vulnerabilities is generally available from the vendor who will issue updates and patches to fix those that it becomes aware of.

For cloud services, the responsibilities of the organisation as the customer, and the cloud service provider (CSP) must be defined. This may involve the CSP being responsible for vulnerability assessment and patching for some or all aspects of the service, depending on the cloud service model adopted (e.g., IaaS, PaaS or SaaS or similar service definitions).

B. Security Tests

In addition to monitoring vulnerabilities via intrusion detection or prevention system, the organisation will conduct regular technical security tests.

IT is responsible for ensuring that technical security test happens at least once a year and/or after any significant change in the platform.

All vulnerabilities identified will be communicated to appropriate personnel for assessment and remediation. Follow-up security tests must be performed to confirm effectiveness of actions taken within 1 year.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	27 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 19 – MALWARE PROTECTION POLICY

OVERVIEW

The objective of this policy is to protect information and underlying systems from potential damages caused by malicious codes. Malicious code includes all and any programs (including macros and scripts, viruses, worms, logic bombs, Trojan horses, web bugs, and in some cases “spy ware”) that are deliberately coded to cause an unexpected, and unwanted, event on a user’s workstation.

POLICY STATEMENT

This policy describes malware controls for user end point devices and information systems. The following minimum requirements shall be enforced:

1. All anti-virus product shall be operated in real time on all end-user computers, workstations and servers. The product shall be configured/updated for real time protection.
2. Each removable storage media placed into a computer must be scanned locally and automatically.
3. Files downloaded from the Internet via the firewall must be scanned for viruses.
4. No one should be able to stop anti-virus definition updates and anti-virus scans except for administrators.
5. All incoming and outgoing email must be scanned to ensure that no virus infected emails or attachments are sent or received.
6. No emails or attachment may be delivered to a user that could not successfully be scanned and disinfected if necessary.
7. A virus control mechanism, with appropriate notification of the user, must quarantine all messages that could not be inspected for virus.
8. All applicable systems must be configured with approved antivirus software. The software must be configured to receive automatic updates and virus signatures, perform periodic scan, log anti-virus events with routing to a central logging solution, and end users must not be able to configure or disable the software.
9. Anti-virus software must be configured to update virus signatures and scan engines on at least a daily basis.
10. VM servers will be protected by AWS Inspector (or an equivalent product for non-AWS environment).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	28 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 20 – BACKUP POLICY

OVERVIEW

This policy aims to ensure that backup, recovery and restoration of information are in place and tested for effectiveness.

POLICY STATEMENT

The policy below applies to the organisation’s overall information backup including the requirements for backup, recovery and restoration and any further requirements (e.g., contractual and/or legal) for the erasure of information.

1. Owners of the information assets like operating systems, databases, applications, network components and other information assets shall identify the data to be backed up.
2. The backup arrangements shall include:
 - List of directories and files to be backed up
 - Types of backups to be performed e.g., incremental backup, full backup etc.
 - Backup location for taking and restoring the concerned backup.
 - Timing of start and completion of backup
 - Retention period
3. The backup schedule shall be available for reference and verification with the information asset owner and the team responsible for the execution of the backup schedule.
4. Backup shall be tested for readability and restorability at least once a year. Recovery procedures for the restoration of data must be kept up to date.
5. Where the organisation explicitly provides backup and restore services to customers, they will be provided with clear information about the capabilities of the organisation with respect to backup and restoration of information particularly personal data, and the limits of the service regarding backup.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	29 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 21 – LOG MANAGEMENT POLICY

OVERVIEW

This policy defines specific requirements for information systems to generate, store, process, and aggregate appropriate audit logs across the organisation’s entire environment in order to provide key information and detect indicators of potential compromise.

POLICY STATEMENT

1. All critical systems, applications, and services within the organisation shall record and retain audit-logging information that includes the following information.
 - Activities performed on the system.
 - The user or entity (i.e., system account) that performed the activity, including the system that the activity was performed from.
 - The file, application, or other object that the activity was performed on.
 - The time that the activity occurred.
 - The device that the activity was performed with.
 - The outcome (e.g., success or failure) of the activity.

2. Specific activities to be logged must include, at a minimum:
 - Information (including authentication information such as usernames or passwords) is created, read, updated, or deleted.
 - User authentication and authorization to systems.
 - Granting, modification, or revocation of access rights, including adding a new user or group; changing user privileges, file permissions, database object permissions, firewall rules, and passwords.
 - System or services configuration changes, including software installation, patches, updates, or other installed software changes.
 - Start-up, shutdown, or restart of an application.
 - Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold or hardware fault.
 - Detection of suspicious and/or malicious activity from a security system such as an intrusion detection system or anti-virus system

3. Unless technically impractical or infeasible, all logs must be aggregated in a central system so that activities across different systems can be correlated, analysed, and tracked for similarities, trends, and cascading effects. Log aggregation systems must have automatic and timely log ingest, event and anomaly tagging and alerting, and ability for manual review.

4. When using a cloud environment, logs must be kept for all administrators and operators performing activities in cloud environments.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	30 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 22 – SOFTWARE SECURITY POLICY

OVERVIEW

This policy aims to control the use of software to ensure that only secure and authorized software is used and to prevent violation of copyright, confidentiality and license agreements.

POLICY STATEMENT

1. The organisation recognizes its legal obligation to the holders of copyright on computer software. To this end, the organisation does not permit unlicensed software on company-owned computers and requires documentation of the appropriate licenses for all installed software. Unless specifically allowed by the license agreement, no copies of software shall be made.
2. A list of authorized/approved software and license details will be maintained. Only approved software shall be used, and if a software requires a license, only licensed copy shall be used.
3. Asset audit shall be conducted at least once a year to determine that only approved software is installed, and the validity of software licenses installed on all laptops, and any information systems.
4. All requests for new software installations must be made to the The Management which will approve and forward it to IT for installation. The copies of the installation media, instructions, license key and license terms must be maintained by IT. Requests may be denied in the following conditions:
 - An insufficient number of licenses supplied
 - In case software/patch interferes with another application
 - The requesting staff member will not be available to test the software before distribution
5. Capacity management shall be carried out for all critical software, to analyse existing and future capacity requirements.
6. Ensure that latest security patches are applied.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	31 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 23 – NETWORK SECURITY POLICY

OVERVIEW

The objective of this policy is to secure network and resources from intrusions and to provide / maintain security of data. The controls under this policy include all aspects of network security from network management to monitoring.

POLICY STATEMENT

1. The number of entry points to the company's network shall be restricted and secured through firewall, web content filtering and intrusion detection system. All connections to the critical system/application servers shall route through the firewall.
2. A firewall system has to be installed at all connections from an internal to any other internal or external network. Firewall systems are categorized into un-trusted relations firewall systems or trusted relations firewall systems.
3. All access through the firewalls shall be justified and supported by business and/or operational requirements.
4. Network and security components used for communication and network security shall be appropriately configured, maintained and secured.
5. Current configuration information about network infrastructure and critical network devices like firewall, routers, switches etc. shall be stored and backed up securely.
6. Key network activities shall be monitored to assess the performance of the network, reduce the likelihood of network overload and detect potential or actual malicious intrusions.
7. Capacity planning activities shall be undertaken to allow extra network capacity to be commissioned before projected bottlenecks / overloads materialize.
8. Third party agreements related to network services shall include but may not be limited to a clear description of security features, service levels, vendor escalation details and terms of non-disclosure of information.
9. For cloud provider network products, the company shall rely on the certifications of the cloud provider to ascertain network services and components and to ensure technical compliance and capability to enable geo-location restriction.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	32 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 24 – CRYPTOGRAPHY POLICY

OVERVIEW

The objective of this policy is to protect the confidentiality, authenticity or integrity of information by cryptographic means.

POLICY STATEMENT

A. General Cryptographic Rules

1. Cryptography must be considered in the following scenarios:
 - To protect confidentiality of data in the inter-connections of networks across the internet, intranet, virtual private networks (VPNs) and wireless networks
 - Where personal data and other confidential data are at rest or stored in data storage
 - Electronic mail messages and attachments
 - Information used for authentication
 - Remote connections
 - Where cloud services are used, regardless of the type of cloud service
2. When exporting encryption internationally, the recipient is responsible for ensuring that encryption laws in the receiving country is not violated.
3. Where applicable, the company will provide information to customer regarding the circumstances in which it uses cryptography to protect the personal data it processes. The company will also provide information to them about any capabilities it provides that can assist the customer in applying their own cryptographic protection.

B. Encryption Techniques

In general, the cryptography policy of the company is to use the following techniques for the relevant business process or situation:

Process/Situation	Technique	Specific Guidance
Storage of data in the cloud at rest	Use encryption as defined by the cloud provider	AES-256 encryption to be used for confidential information
Any web page allowing access to assets	HTTPS with strong encryption cipher (AES-128 or stronger)	RSA to be used for public key cryptography. Certificates to be obtained from a reputable certificate authority. AWS, Comodo and Let's Encrypt are examples of suitable certificate authorities.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	33 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

Process/Situation	Technique	Specific Guidance
Protection of data on storage media	Symmetric encryption	AES-256 encryption to be used where available e.g. Bitlocker
Protection of passwords on systems	All passwords must be hashed	BCRYPT hashing to be used where available and raw password retrieval is not necessary. Otherwise, symmetric encryption.
Email Security	Transmission via SMTP or HTTPS with TLS	Features available in the relevant email client should be used to simplify the process
Remote Access	HTTPS access to web systems using TLS or Virtual Private Network (VPN) using TLS	An IPSec VPN may be used where permitted

THE SOFTWARE PRACTICE PTE LTD	No of Pages	34 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 25 – SECURE DEVELOPMENT POLICY

OVERVIEW

This policy defines the high-level requirements to ensure that information security is designed and implemented within the development lifecycle for application and information systems.

POLICY STATEMENT

1. The organisation shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
 - Development, test and production environments are separated and do not share common components.
 - There is a segregation of administrative duties between development and test, and products.
 - Endpoints to perform development-related tasks are secured and hardened.
2. It shall be ensured that security requirements are known at all times so that they can be taken into account throughout the development lifecycle. This includes requirements from internal sources (e.g., organisation policies, objectives and risk management strategy) and external sources (e.g., customer requirements and applicable laws and regulations).
3. Systems shall be designed and developed based on industry secure coding guidelines for the coding technology and the Open Web Application Security Project (OWASP).
4. Store all forms of code (including source code, executable code, and configuration-as-code) based on the principle of least privilege so that only authorized personnel, tools, services etc. have access.
5. Developers are expected to adhere to the coding guidelines throughout the development lifecycle, including standards for quality and security.
6. Outsourced development (if any) shall adhere to the organisation’s policies and guidelines all throughout the development lifecycle, and their activities shall be supervised and monitored by the organisation.
7. Perform a code review / code analysis based on secure coding standards and record all discovered issues and recommended remediations in the development team’s issue tracking system.
8. Scope the testing, design the tests, perform the testing and document the results, including recording all discovered issues and recommended remediations in the development team’s issue tracking system.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	35 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

9. Testing of security functionality shall be carried out during development. No code shall be deployed to production systems without documented, successful test results.
10. Test data shall be selected carefully, protected and controlled.
11. Changes within the development lifecycle shall be controlled by the use of formal change control procedure and shall use version control.
12. Ensure that the latest security patches are applied prior to system commissioning.
13. Securely archive the necessary files and retain supporting data for each release.
14. Gather information from system acquirers, users, and public sources on potential vulnerabilities in the system and third-party components that it uses, for planning and implementing risk responses for vulnerabilities.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	36 of 36
	Document Classification:	Internal
	Effective Date	10 June 2024
POLICIES FOR INFORMATION SECURITY	Doc No	DPMP-POL-02
	Revision	1.0

POLICY 26 – CHANGE MANAGEMENT POLICY

OVERVIEW

Information security incidents leading to loss of information and reliability can result from poorly managed changes in business environment. This policy is designed to control changes to information processing facilities and information systems to preserve information security when executing changes.

POLICY STATEMENT

For all changes to systems, applications and infrastructure managed by the organisation, security requirements must be determined prior to the development and implementation phase.

Requirements include, but not limited to the following:

1. **Business Impact:** Evaluate the impact that a change will have on business operations, including the potential downtime or disruption.
2. **Security:** Ensure that changes do not compromise information security.
3. **Compliance:** Ensure that changes are in compliance with relevant laws, regulations and standards
4. **Testing:** Verify that changes have been thoroughly tested and will not negatively impact existing systems or application.
5. **Access Control and Authorisation:** Consider who shall be granted access to the system and ensure proper approval.
6. **Documentation:** Update technical and operational documentation to reflect changes and ensure that they are easily accessible.
7. **Rollback plan:** Ensure steps are defined to roll back changes if they result in unexpected problems or negative impacts.
8. **Approvals:** Obtain necessary approvals for changes from relevant stakeholders.
9. **Deployment:** Implementation of changes including deployment plans.

Changes shall follow documented change control procedure with version control to ensure confidentiality, integrity and availability of information in information processing facilities and information systems. Records of changes shall be maintained.