AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

NetGain Systems has identified a set of policies in a wide variety of information security areas which are directly derived and aligned with the controls in ISO/IEC 27001 Standard. 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. These policies apply to all staff and to all other individuals who directly or indirectly use or support the products and services of the organisation.

Any employee 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.

REFERENCE

- ISO/IEC 27001 Information technology – Information security, cybersecurity and privacy protection – Information security management systems requirements

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 Management Representative (MR) and the Top 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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

POLICY 01 – ACCEPTABLE USE POLICY

OVERVIEW

NetGain Systems 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. Employees 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. Employees 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. Employee 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:

1. Employees may not leave computing devices used for business purposes, unattended in public, and ensure they are not overlooked by unauthorised people when working.
2. Use only those user credentials which they are provided with, and protect their user credentials.
3. Not attempt to bypass or subvert system security controls.
4. 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.
5. Employees may not post any confidential information including another individual's personal data in public forums or chat rooms.
6. 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.

POLICY 02 – INFORMATION CLASSIFICATION POLICY

OVERVIEW

NetGain Systems 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 owner. The classification category can change during the lifecycle of information or can result in non-classified information. The accountability for such "de-classification" always remains with the designated owner.

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.	• 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.	• Internal policies and operating procedures • Interoffice memorandums • Internal meeting minutes
3	Confidential	Highest level of classification. Sensitive information that may be directly or indirectly damaging to the organisation or to the information owner, if disclosed.	• 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

POLICY 03 – INFORMATION TRANSFER & COMMUNICATIONS SECURITY POLICY

OVERVIEW

This policy sets out how information, including personal and confidential data, should be securely transferred and communicated within and outside the organisation. It applies to all staff and covers all methods of transfer (digital, physical, or verbal).

POLICY STATEMENT

A. Key Principles

- All information transfers must be authorised, justified, and secure.
- Only share the minimum necessary information for the intended purpose.
- Confirm the recipient's identity and authorisation before any transfer.
- Where appropriate, ensure a legal basis exists (e.g. data sharing agreement, NDA, consent, or lawful exemption).

B. Approved Transfer Methods

Method	**Key Requirements**
Email	Use email disclaimers. Avoid confidential info in subject lines. Follow Email Policy.
File Transfers	Use approved tools and encrypt/password-protect confidential data.
Postal Mail / Courier	Use tracked delivery. Seal, label correctly, confirm recipient identity.
Removable Media	Only with business need. Must be encrypted. Report any loss or issues.
Phone / Voicemail	Confirm recipient identity. Don't share confidential info via voicemail.
In-person / Hand Delivery	Verify identity. Use secure packaging. Track collection or delivery.
Collaboration Tools	Only use authorised tools. Access must be restricted and logged.

C. Email Use Guidelines

- Include a confidentiality disclaimer in outgoing messages.
- Be cautious with subject lines and filenames—avoid revealing confidential content.
- Double-check recipients before sending.

D. Removable Storage Devices

Use of media devices 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 use must be authorized by management.

- The media must be encrypted.
- Lost or malfunctioning devices must be reported immediately to the MR.

E. Phone and Voicemail

- Don't discuss sensitive info unless the recipient's identity is confirmed and the conversation is private.
- Never leave confidential data in voicemail messages.
- Avoid discussing confidential information in open spaces.

F. Internet-based File Sharing

- Only use authorised cloud or collaboration platforms.
- Access must be via company credentials for traceability.
- Ensure appropriate permissions are set (e.g., read-only, limited access).

G. Sending Information by Post

- Verify postal address.
- Use secure, sealed packaging with clear recipient and return details.
- Use tracked delivery services and confirm receipt.
- Report any issues or delivery failures immediately to the MR.

H. In-Person Transfers

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 that the authorized recipients are who they say they are and verify their identification.

POLICY 04 – E-MAIL POLICY

OVERVIEW

This policy outlines how to use email securely, responsibly, and in compliance with legal and business requirements.

POLICY STATEMENT

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

A. E-mail Accounts

1. All official communication must be conducted using company-issued email accounts.
2. Email access may be restricted or revoked for security reasons (e.g., use from untrusted devices).
3. The organisation's reserves the right to assign and revoke email accounts, and monitor, access, or manage email data without prior notice, for legal, security, or business purposes.

B. Acceptance Use of Email

1. Users are responsible for all emails sent from their account.
2. Use only your own assigned email account and never share or use someone else's credentials.
3. All emails should reflect professional conduct, as they are traceable and considered the property of the organisation.
4. Include the standard email confidentiality disclaimer in all external communications.

C. E-mail Content Guidelines

1. Do not send content that could be considered offensive, disruptive, defamatory, or discriminatory.
2. Avoid any messages that include: sexual, racial, religious, or political commentary, harassing or threatening language.

D. Prohibited E-mail Activities

Prohibited Activity	**Description**
Spam & Junk Mail	No bulk or unsolicited messages (e.g. commercial ads)
Chain Letters / Pyramid Schemes	Do not forward or participate in these types of messages.
Malicious Emails	Avoid mail bombing or intentionally disrupting others' email use.
Impersonation	Do not send messages pretending to be someone else.
Unsecured Personal Data	Personal data must be encrypted or password-protected before sending. Passwords should be shared via a separate email or channel.

POLICY 05 – ACCESS CONTROL POLICY

OVERVIEW

This policy ensures access to information systems and resources is tightly controlled to:

- Minimise risk to information assets
- Enforce least privilege and need-to-have principles
- Ensure that only authorised users can access systems
- Enable traceability and secure authentication mechanisms

POLICY STATEMENT

1. Access is granted only to authorised individuals based on job responsibilities and must be formally requested and approved by senior management.
2. All users must have a unique account to enable accountability and activity tracking.
3. Shared accounts are not allowed unless explicitly approved for operational reasons.
4. External users (vendors, consultants, etc.) must have expiry dates aligned with the end of their engagement.
5. Passwords must comply with the organisation's password policy and must be securely communicated.
6. Two-Factor Authentication (2FA) is mandatory for system and application administrators.
7. After 5 failed login attempts, the account will be locked and can only be reactivated by an administrator.
8. Use of administrative privileges is tightly controlled.
9. Privileged IDs (admin, root, etc.) must be separate from regular user accounts, and use of these accounts should be minimised, logged, and reviewed.
10. Utility programs that bypass controls must be tightly controlled and only used when necessary.
11. All access and usage of systems must be logged and monitored. Logs must also capture new, modified, and deleted accounts.
12. Access rights must be regularly reviewed to ensure they are still required.
13. Excess or outdated access must be removed promptly. Accounts must be suspended:
    a. After 60 days of inactivity
    b. When a user is on leave exceeding 60 days
    c. Within 1 working day of employee resignation or termination
    d. Immediately upon notification of termination (e.g., unfriendly exits)

POLICY 06 – PASSWORD POLICY

OVERVIEW

This policy sets requirements for the creation, use, storage, and management of passwords to prevent unauthorized access to systems and data.

POLICY STATEMENT

We categorize access points as:

- Endpoints: Endpoints (e.g., laptops): Require passwords or biometric login.
- Cloud Systems: Must enforce passwords and Multi-Factor Authentication (MFA).

Password Requirements:

1. Complexity, Expiration and History
    - Be at least 8 characters long.
    - Contain characters from at least three of the following: Uppercase letters (A–Z), Lowercase letters (a–z), Numbers (0–9), Special characters (!, @, #, $, etc.)
    - Avoid dictionary words, usernames, or easily guessable phrases.
    - Use of passphrases is encouraged (e.g., “BlueHorse!42Tree”).
    - Passwords must be changed at least once per year.
    - The last 5 passwords cannot be reused.

2. Account Lockout
    - Accounts will be locked after 5 failed login attempts.
    - Locked accounts must be manually unlocked by an administrator.

3. Cloud Systems
    - MFA is mandatory for all cloud platforms and internet-facing systems.
    - Passwords must be checked against lists of commonly used or breached passwords, with user-friendly rejection messages.

4. Secure Password Handling
    - Passwords must never be stored or transmitted in plain text.
    - Only hashed and salted passwords should be stored.
    - Secure password managers must be used where applicable.
    - Do not share passwords under any circumstance.
    - Any suspected or actual password leak is treated as a security incident and must be reported immediately to the MR.

5. Password Reset and Assignment
    - Default/vendor-supplied passwords must be changed immediately after deployment.
    - Initial/reset passwords must be changed by users on first login
    - Identity verification is required before any password reset.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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 regarding milestones, payments, 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 call for independently audited compliance acceptable to the customer, and 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.

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 the ISO/IEC 27001 Standard or any other equivalent information security / data protection compliance certification relevant to cloud computing.

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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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 intellectual property 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, standards (e.g., ISO/IEC International 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).

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. 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. The DRP must be documented to provide guidance when hardware, software, or services become critically dysfunctional or cease to function (short- and long-term outages).

3. The DRP must include an explanation of the magnitude of information or system unavailability in the event of an outage and the process that would be implemented to continue business operations during the outage.

4. The DRP must include a recovery plan for returning business functions and services to normal operations and procedures for periodic testing, review, and revisions of the DRP.

5. The organisation must verify the established plans, response and recovery procedures in order to ensure that they are valid and effective during adverse situations. The test plan and test report shall be maintained by the MR for this.

6. 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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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 have 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.*

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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. The organisation shall publish a list of records with the following minimum details:
    - Record Name
    - Record Classification
    - Record Owner
    - Retention Time
    - Storage Location
    - Disposal Method

4. All record owners shall store and retain relevant records in accordance with laid down asset classification and handling guidelines of the organisation.

5. All records shall be protected from loss, damage, fabrication, and falsification in accordance with business and statutory requirements.

6. 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.

7. 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.*

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

POLICY 13 – DATA RETENTION & DESTRUCTION POLICY

OVERVIEW

NetGain Systems 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:

1 Retains data based on legal, regulatory and business requirement, including maintaining the continuity and its availability in the event of a disaster.
2 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. Hammer storage media to physically destroy it if it will be disposed of. If 3rd 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.

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 fully 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. 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 for remote access.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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.*

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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 after 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 MR immediately.
- Delete all organisation's data for all allowed personally owned devices upon termination of employment or relationship with the organisation.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

POLICY 18 – POLICY ON VULNERABILITY MANAGEMENT AND DISCLOSURE

OVERVIEW

This policy outlines the organisation's approach to identifying, managing, and disclosing vulnerabilities to reduce security risks and support a secure IT environment.

POLICY STATEMENT

1. The organisation shall actively monitor and assess systems for technical vulnerabilities using automated tools and manual reviews.

2. Vulnerability assessments shall be conducted at least once a year or after significant system changes (e.g., patches, upgrades).

3. Identified vulnerabilities shall be:
   - Assessed for severity and potential impact.
   - Tracked and remediated based on priority.
   - Assigned timelines for resolution based on risk level.

4. All systems must be updated with security patches and firmware updates based on criticality.

5. Unsupported or end-of-life systems must be either decommissioned or appropriately isolated with risk acceptance by management.

6. The organisation encourages responsible disclosure of vulnerabilities by internal or external parties. Secure channels (e.g., designated email) shall be available for reporting vulnerabilities.

7. Reports of security vulnerabilities from external sources shall be acknowledged and evaluated promptly. If valid, mitigation steps must be taken without unnecessary delay.

8. Exploiting known vulnerabilities in organisation systems without permission is strictly prohibited and will result in disciplinary action or legal consequences.

9. Periodic reports on vulnerability status and remediation efforts shall be presented during regular information security meetings.

10. A vulnerability management log shall be maintained.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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 company-managed endpoints must have approved anti-malware software installed and configured to:
   - Run real-time protection at all times
   - Perform scheduled scans at least weekly
   - Automatically update virus signatures and engines daily
   - Prevent users from disabling or modifying protection settings
   - Log all malware-related events to a centralised log management system

2. Users must not install unauthorised software or disable malware protection controls on their devices.

3. Any removable media must be automatically scanned upon connection to endpoint devices.

4. Malware scanning must be enabled at the email platform level using integrated or third-party security services. All attachments and links received via email must be scanned for malicious content using built-in email security features (e.g., safe attachments, link protection).

5. Files downloaded via browsers or collaboration tools (e.g., file sharing sites, cloud storage) must be scanned at the endpoint level upon access.

6. All cloud-hosted workloads must use cloud-native malware protection tools that:
   - Detect and prevent malware or anomalous behaviour
   - Integrate with security monitoring platforms (e.g., SIEM)
   - Log and alert relevant teams in real-time

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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, 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 restoration 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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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, 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.

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 designated Department Head for approval, and the copies of the installation media, instructions, license key and license terms must be maintained. 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.

POLICY 23 – NETWORK SECURITY POLICY

OVERVIEW

This policy defines how the organisation protects its digital assets, systems, and cloud-based environments from network-related threats. As the company operates from a shared office space and does not manage the physical office network infrastructure, this policy applies to cloud networks, secure access to services and platforms, and use of trusted internet connections.

POLICY STATEMENT

1. All company services hosted in the cloud must be deployed in logically segmented networks (e.g., VPCs, subnets) and protected using:
    - Security groups and network ACLs
    - Identity-based access control
    - Cloud-native firewalls or Web Application Firewalls (WAF), where applicable

2. Users must:
    - Connect only to trusted, encrypted networks (e.g., company VPN, secured Wi-Fi)
    - Avoid transmitting sensitive information over public or untrusted networks without encryption
    - Use endpoint protection tools (e.g., anti-malware, DNS filtering, personal firewall) to secure their devices while on shared networks

3. Remote access to cloud platforms and administrative systems must use VPN, SSO with MFA, or bastion hosts with time-based access controls.

4. Default-deny network access policies should be applied for all cloud workloads.

5. Network access to cloud applications and APIs must be restricted using firewalls, IP allow-lists, and geo-restrictions as required.

6. Network traffic in cloud environments must be monitored using cloud-native tools.

7. Cloud network configurations (e.g., routing, security groups) must be version-controlled and reviewed for misconfigurations.

8. Any remote or API access granted to external vendors or partners must follow principle of least privilege and be time-limited, logged, and reviewed regularly.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

POLICY 24 – CRYPTOGRAPHY POLICY

OVERVIEW

This policy defines how cryptographic controls are applied across the organisation to protect the confidentiality, integrity, and authenticity of information at rest and in transit. Cryptography is a critical control in safeguarding sensitive data, especially in a cloud-based service environment.

POLICY STATEMENT

A. Use of Encryption

1. All confidential data must be protected using approved encryption methods during:
   - Transmission over public or untrusted networks
   - Storage on cloud platforms, databases, or local devices
2. Encryption must be applied to:
   - Customer and company data stored in cloud environments
   - User credentials and authentication tokens
   - Backups, logs, and system configuration files containing sensitive data
   - End-user devices (e.g., full-disk encryption on laptops)
3. All communications (e.g., HTTPS, API calls, remote access) must use TLS 1.2 or higher.

B. Approved Algorithms and Standards

1. Only industry-standard, strong cryptographic algorithms must be used. Approved algorithms include:
   - AES with 256-bit keys (for data encryption)
   - RSA with 2048-bit keys or higher (for digital signatures and key exchange)
   - SHA-256 or higher (for hashing)
   - Elliptic Curve Cryptography (ECC), where appropriate
2. Use of outdated, weak algorithms (e.g., MD5, SHA-1, DES, RC4) is strictly prohibited.

C. Cryptographic Key and Certificate Management

1. All cryptographic keys must be:
   - Generated securely using approved methods
   - Stored securely, such as in a cloud-based key management system
   - Access-controlled, with minimal privilege
   - Rotated periodically (e.g., annually or on compromise)
   - Destroyed securely when no longer needed
2. All digital certificates (e.g., SSL/TLS) must be:
   - Issued by trusted Certificate Authorities (CAs)
   - Renewed before expiration
   - Revoked if compromised or no longer in use

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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. 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.
7. 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.
8. Testing of security functionality shall be carried out during development. No code shall be deployed to production systems without documented, successful test results.
9. Test data shall be selected carefully, protected and controlled.
10. Changes within the development lifecycle shall be controlled by the use of formal change control procedure and shall use version control.
11. Ensure that the latest security patches are applied prior to system commissioning.
12. Securely archive the necessary files and retain supporting data for each release.
13. 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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

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: Develop a plan 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.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

POLICY 27 – PRIVACY GOVERNANCE POLICY

1. Policy Statement

1.1. All persons involved in the processing of personal data are responsible for ensuring compliance with this document, and to clarify any of its provision with the Data Protection Officer (DPO).

1.2. The organisation provides a framework for processing of personal data in compliance with Singapore Personal Data Protection Act (PDPA) and other applicable privacy laws and regulations.

1.3. This Privacy Governance Policy is based on the following:

- To process, store, and disclose personal data only for legitimate business purposes;
- To provide notice (unless an exception applies) to individuals, advising them of the purpose for which the organisation is processing their personal data;
- To contain terms in contracts with third party suppliers to help ensure that personal data disclosed / shared / transferred to them is managed according to the same standards the organisation implements and comparable to PDPA or other applicable privacy laws and regulations;
- To give additional attention and care to sensitive personal data according to the requirements of Personal Data Protection Act (PDPA) and other applicable privacy laws and regulations.
- To identify appropriate measures to maintain personal data as accurate, complete, current, adequate, reliable; and
- To protect personal data using appropriate physical, technical and organizational security measures.

2. Data Protection Officer (DPO)

A DPO has been appointed to champion data protection initiatives and be primarily responsible for monitoring the organisation's compliance to relevant data protection requirements. The Appointment Letter for the DPO contains the details of the duties that the DPO must perform. The business contact information of the DPO will be made publicly available.

3. Collection, Use and Disclosure of Personal Data

3.1. Collection of Personal Data

The organisation shall not collect personal data unless the information is reasonably necessary for, or directly related to, one or more processing activities. Personal data will only be collected by lawful and fair means, and not in an intrusive way, and reasonable steps will be taken to ensure that the individual is aware of the following:

- The identity and contact details of NetGain Systems as the organization collecting and storing the information;
- The purpose for which the information is collected;
- The intended recipients to which the organisation usually discloses information of that kind;
- Any law that requires the particular information to be collected;

- The main consequences (if any) for the individual if all or part of the information is not provided; and
- How to exercise their rights over their personal data.

Where it is reasonable and practical to do so, we will collect personal data about an individual only from that individual. If, however, this information is collected from a person other than the individual, we must act reasonably to ensure that the individual is or has been made aware of the matters listed above.

3.2. Use and Disclosure of Personal Data

As a general rule, the organisation must only use or disclose personal data in a manner consistent with any data protection notice provided to the individual. We must not use or disclose personal data about the individual other than for its primary purpose of collection, unless:

- The individual has consented to the use or disclosure; or
- The individual would reasonably expect the organisation to use or disclose non-sensitive personal data for a secondary purpose and the secondary purpose is related to the primary purpose (e.g., fulfilment of the contract); or
- We have reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal data as a necessary part of its investigation of the matter or in reporting its concerns to relevant authorities; or
- The use or disclosure is required or authorized by or under law, rule or regulation; or
- We reasonably believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of an individual

3.3. Collection, Use and Disclosure of Sensitive Personal Data

The organisation will only collect sensitive personal data if the collection is required by any written law or where the personal data is reasonably necessary for the purpose and with the individual's consent.

Sensitive personal data is defined as any personal data which is considered likely to result in significant harm to an affected individual when compromised. Examples are:

- NRIC, FIN, Passport Details and other government-issued identifications;
- Financial, medical, life/health insurance, vulnerable person, private key to authenticate or authorize a record or transaction;
- Individual's account information combined with any of the following: biometric data, security/access code, password or answer to security question used to permit access to or use of an account

The organisation must not use and/or disclose sensitive data such unless such use or disclosure is required or authorized under law or applicable regulation.

3.4. Receiving Unsolicited Personal Data

Where the organisation receives unsolicited personal data about an individual, it must either destroy (e.g., shredding if hardcopy) or permanently delete (e.g., deletion of email and deleted items bin) the personal data immediately upon detection. If the personal data is part of a document that needs to be kept, the unsolicited personal data shall be masked off or the document shall be anonymised, if reasonably practicable.

3.5. Obligation to Inform Third Parties on any Modification or Withdrawal of Consent, or Objections Pertaining to the Shared Personal Data
Communication of modifications, withdrawals or objections to relevant third parties shall be done by the DPO and recorded to maintain an audit trail. The DPO shall monitor the acknowledgment of receipt of the information.

4. Access and Correction of Personal Data

As a general rule, the organisation will, on the request by an individual, provide him or her with access to their personal data, and will consider a request from the individual for correction of that information. We shall verify the identity of the requestor to ensure legitimacy of the request and shall reply within the prescribed timeline. For any request that will be denied, we shall provide the individual with justifiable reasons that are permitted under the PDPA or other applicable laws and regulations.

5. Maintaining Personal Data Accuracy and Quality

The organisation will take reasonable steps to make sure that the personal data they collect, use, or disclose is accurate, complete, up to date, and not misleading.

6. Storage and Transmission

6.1. The organisation shall implement approved security measures to all personal data in line with established information security policies and processes.
6.2. Access to personal data shall be limited only to authorized and appropriate employees.
6.3. The organisation allows outside transmission of information to the effect that encryption or password-protection is employed to personal data, whichever of the two controls is efficiently feasible for the transmission activity, and that the transmission is over an encrypted channel.

7. International Personal Data Transfers

7.1. The organisation may need to transfer personal data to recipients outside Singapore which may include outsourcing of services to suppliers located overseas and/or processing the personal data outside Singapore (e.g., cloud computing, web services).
7.2. The above transfers may take place when there is an adequate level of protection to the fundamental right of individuals to data privacy, and that the personal data receives a comparable standard of protection as that which it would receive under the PDPA. We will ensure that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.
7.3. Personal data may be transferred to recipients to other countries under certain conditions:
- The recipient can implement all necessary controls to fulfil all applicable obligations regarding the processing of personal data taking account of security risks and the scope of processing; and
- The recipient can demonstrate evidence of compliance with the instructions and/or agreements/contracts (Note: We may rely on applicable data protection / privacy

certifications such as (ISO/IEC 27701, APEC CBPR, APEC PRP, EU-GDPR Compliance, etc.) where available to satisfy this requirement).

8. Retention

8.1. The organisation shall retain personal data only for the duration necessary to fulfil the identified lawful business purpose. All personal data shall be retained only for as long as necessary:
- For the fulfilment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or
- The establishment, exercise, or defence of legal claims; or
- As prescribed by law.

8.2. Retention periods, modes of storage and disposal method shall be documented for the personal data involved in each processing activity.

8.3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

9. Disposal and Destruction

9.1. Upon the expiration of identified legal, lawful business purposes or withdrawal of consent, The organisation must take reasonable steps to securely destroy or permanently de-identify or anonymize the personal data if it is no longer needed.

9.2. Disposal should be in a manner that the personal data shall be unreadable (for paper) or irretrievable (for digital records).

9.3. All hard, system, soft, and electronic copies will be disposed appropriately following the organisation's *Data Retention and Destruction Policy*.

9.4. Alternatively, where it applies, we may decide to anonymize the personal data. If we consider this option, a risk assessment shall be conducted to address re-identification risks.

10. Maintaining Personal Data Security

10.1. The organisation must take reasonable steps to protect the personal data that it holds from misuse, interference, and loss, and from unauthorized access, modification, or disclosure.

10.2. We shall ensure that appropriate physical, technical, and organizational security measures in line with the established Information Security Management System are implemented on personal data in whatever form it takes.

11. Enquiries and Complaints

The organisation shall receive enquiries and complaints related to personal data, or related to the contents of this governance policy, as well as entertain and institute an investigation in relation thereof. The Data Protection Officer business contact information (BCI) is made available publicly for this purpose.

12. Data Breach Notification

12.1. Data breach notification protocols are established and maintained in order to deal with a data breach concerning personal data including critical timelines and notification requirements.

12.2. Employees and other personnel working for or on our behalf must immediately notify the DPO if they become aware of a data breach to enable the appropriate assessment, investigation and remediation measures to be taken in a timely manner, including possible notification to Singapore Personal Data Protection Commission (PDPC), other relevant authorities and the individuals (where the organisation is the Data Controller for the concerned processing activity), or notification to our clients (where the organisation is the Data Processor and the client is the Data Controller for the concerned processing activity).

13. Data Protection Clause in Contract with Customers

In light of the organisation's obligations under applicable data privacy laws and regulations, contract terms with clients shall include data protection wording to cover instances where the engagement involves collecting and processing personal data, and the client's instructions for such. All draft contracts must be reviewed by the DPO for the possible inclusion of data protection terms applicable for each engagement.

14. Data Processing Agreement with a Supplier

In light of the organisation's obligations under applicable data privacy laws and regulations, we must ensure that appropriate wording is included in a supplier contract where the supplier will receive, or have access to any personal data that we hold.

15. Compliance Monitoring and Reporting

15.1. Noncompliance with this policy may result in a breach of Personal Data Protection Act (PDPA) and other applicable privacy laws and regulations.
15.2. The organisation shall perform regular review (at least once a year and as when significant changes occur) of its policies and relevant procedures to ensure compliance.
15.3. Any non-compliance by an employee with this shall subject the employee to appropriate disciplinary actions.
15.4. Any third party found to have violated this policy will be investigated and may be subject to termination of contract and/or contractual claims.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.