AI ACCEPTABLE USE POLICY

Organisation:	Nexus Corporate Services Sdn Bhd
Document Type:	Policy
Policy ID:	NCS-POL-003
Version:	2.1
Effective Date:	1 January 2024
Review Date:	31 December 2025
Owner:	Human Resources and IT Governance Department
Classification:	Internal Use Only

1. Purpose and Scope

This policy establishes the obligations and responsibilities of Nexus Corporate Services Sdn Bhd (hereinafter "the Company") and its employees in relation to the protection of personal data and the acceptable use of artificial intelligence (AI) tools in the workplace.

This policy is developed in accordance with the **Personal Data Protection Act 2010 (PDPA)** and aligned with Malaysia's **National Guidelines on AI Governance and Ethics (AIGE)** published by the Ministry of Science, Technology and Innovation (MOSTI). It applies to all permanent employees, contract staff, interns, and third-party vendors who process personal data or use AI tools on behalf of the Company.

> This policy does not cover AI tools used for personal, non-work purposes on personal devices outside of working hours. It applies strictly to the use of any AI tool in connection with Company data, systems, or business activities.

2. Data Privacy Obligations Under PDPA 2010

2.1 Seven Principles

All employees who handle personal data must comply with the seven data protection principles under the PDPA 2010:

- **General Principle:** Personal data may only be processed with the data subject's consent and for purposes that have been disclosed.
- **Notice and Choice Principle:** Data subjects must be informed of the purpose of data collection and given the option to withdraw consent.
- **Disclosure Principle:** Personal data must not be disclosed to any third party without the consent of the data subject, except as permitted by law.
- **Security Principle:** Practical steps must be taken to protect personal data from any loss, misuse, modification, unauthorised or accidental access, disclosure, alteration, or destruction.

- **Retention Principle:** Personal data must not be kept longer than is necessary for the fulfillment of its purpose.
- **Data Integrity Principle:** Personal data must be accurate, complete, not misleading, and kept up to date.
- **Access Principle:** Data subjects have the right to access and correct their personal data held by the Company.

2.2 Categories of Personal Data

The following categories of personal data are collected and processed by the Company and are subject to PDPA protections:

- Employee information: name, IC number, address, date of birth, bank details, employment records
- Customer and client information: contact details, transaction records, correspondence
- Vendor and supplier information: business registration details, contact persons, financial data
- Sensitive personal data: health and medical information, biometric data (requires explicit consent)

2.3 Employee Responsibilities

- Employees must only access personal data that is necessary for their job function.
- Personal data must not be transferred outside of approved Company systems without written approval from the IT Governance department.
- Employees must report any suspected data breach or unauthorised disclosure immediately to their line manager and the IT Governance department.
- Printed documents containing personal data must be stored securely and disposed of through approved shredding methods.

3. Acceptable Use of AI Tools

3.1 Approved AI Tools

Employees may only use AI tools that have been formally approved by the IT Governance department. The approved tools list is maintained on the Company intranet and reviewed quarterly. Using unapproved AI tools for work-related tasks is a breach of this policy.

At the time of publication, the following categories of AI tools have been assessed and may be approved for specific use cases subject to departmental approval:

- AI writing and summarisation assistants integrated within approved productivity suites
- AI translation tools for internal communications (not for legal or regulatory documents)
- AI data analysis tools that operate within approved cloud environments

3.2 Permitted Uses of AI Tools

Employees may use approved AI tools for the following purposes:

- Drafting internal communications, reports, and non-sensitive documentation

- Summarising lengthy documents or meeting notes for internal use
- Generating ideas, outlines, or templates that are reviewed and edited by a human before use
- Analysing anonymised or non-personal datasets to identify trends
- Translation of general internal communications (not legally binding documents)

3.3 Prohibited Uses of AI Tools

> Employees must not use any AI tool, approved or otherwise, for the following activities. Violations may result in disciplinary action.

- Inputting, uploading, or pasting personal data of employees, customers, or any individual into any AI tool without written authorisation from the IT Governance department
- Using AI tools to make or assist in making employment decisions including hiring, performance reviews, promotions, or redundancy without human oversight and HR approval
- Submitting confidential company information, trade secrets, financial projections, or unreleased product details to any external AI service
- Using AI-generated content in any external-facing document, proposal, or communication without human review, editing, and approval by a relevant manager
- Representing AI-generated output as the employee's own original work in any formal submission, assessment, or professional certification
- Using AI tools to create, distribute, or amplify false, misleading, or harmful content about any person, organisation, or product

4. Alignment with Malaysia's AI Governance and Ethics Guidelines (AIGE)

The Company's approach to AI governance is guided by the principles set out in Malaysia's National Guidelines on AI Governance and Ethics (AIGE). The following principles are embedded in this policy:

- **Human Oversight:** AI tools are used to assist employees, not to replace human judgement. All AI-generated outputs used in business decisions must be reviewed and approved by a responsible person.
- **Transparency:** Employees must be transparent with colleagues and clients when AI tools have been used to produce content or recommendations that are shared externally.
- **Fairness and Non-discrimination:** AI tools must not be used in ways that could produce discriminatory outcomes. Any AI-assisted process involving employees or customers must be monitored for bias.
- **Privacy by Design:** Personal data protection is considered at the point of selecting and configuring AI tools, not as an afterthought. Tools that require personal data inputs must undergo a privacy impact assessment before deployment.
- **Accountability:** Department heads are responsible for ensuring their teams comply with this policy. Employees remain personally accountable for the outputs they submit or act upon, regardless of whether AI was used.
- **Security:** AI tools must only be accessed through secure, Company-approved networks. Employees must not access AI tools through public or unsecured networks when handling work-related tasks.

5. Data Classification and AI Tool Restrictions

Not all company information may be used with AI tools. The following classification framework determines what may and may not be processed by AI tools:

Classification	Description	AI Tool Use
Public	Information approved for external publication	Permitted
Internal	General business information for employee use only	Permitted with approved tools
Confidential	Sensitive business, client, or financial data	Requires written IT approval
Restricted	Personal data, legal documents, trade secrets	Prohibited without special authorisation

6. Breach Reporting and Non-Compliance

Any suspected or confirmed breach of this policy, including unauthorised disclosure of personal data or misuse of AI tools, must be reported within 24 hours to:

- The employee's direct line manager
- The IT Governance department via the internal helpdesk portal
- The Data Protection Officer (DPO) if personal data is involved

Under the PDPA 2010, the Company is required to notify the Personal Data Protection Commissioner in cases of significant data breaches. Employees who fail to report a known breach may be subject to disciplinary action in addition to any action taken by regulatory authorities.

> Non-compliance with this policy may result in disciplinary action up to and including termination of employment, and in cases involving personal data breaches, potential legal liability under the PDPA 2010.

7. Policy Review and Updates

This policy is reviewed annually by the IT Governance department in consultation with Human Resources and Legal. Updates may also be triggered by significant changes in Malaysian law, new regulatory guidance, or the introduction of new AI tools or technologies within the Company.

Employees are responsible for reading and acknowledging the latest version of this policy. Acknowledgement is recorded in the HR system and must be completed within 14 days of any updated version being published.

Prepared by:	IT Governance Department	**Approved by:**	Chief Executive Officer
Date:	1 January 2024	**Date:**	1 January 2024
Signature:	_____	**Signature:**	_____