Pep & Co Pte Ltd

Data Protection & Cybersecurity Policy

Version 2026

Document Control

Document Title: Data Protection & Cybersecurity Policy
Organisation: Pep & Co Pte Ltd
Version: 2026
Effective Date: 2026
Review Cycle: Annual
Policy Owner: Data Protection Officer
Approved By: Managing Director
Next Review Date: 2027

Document Version History

Version: 2026
Date: 2026
Description: Initial release

1. Corporate Commitment to Data Protection

Pep & Co Pte Ltd ("Pep & Co") is committed to protecting personal data and maintaining robust cybersecurity practices across all systems and services operated by the organisation.

The company recognises the importance of safeguarding personal data in accordance with Singapore's Personal Data Protection Act (PDPA) and implementing security practices aligned with industry standards.

Pep & Co adopts administrative, technical and organisational safeguards designed to protect personal data against unauthorised access, disclosure, alteration or loss. These safeguards include secure system architecture, encryption standards, controlled infrastructure access, monitoring systems and internal governance policies.

This document outlines Pep & Co's general approach to data protection and cybersecurity. Certain operational security controls are not publicly disclosed for security reasons.

2. Scope of Policy

This policy applies to:
• systems developed and maintained by Pep & Co
• infrastructure used to host client platforms
• internal development environments

• employees and contractors handling company systems
• personal data processed through systems operated by Pep & Co

This document provides a high-level overview of Pep & Co's cybersecurity and data protection practices.

3. Appointment of Data Protection Officer

Pep & Co Pte Ltd has appointed a Data Protection Officer (DPO) responsible for overseeing compliance with Singapore's Personal Data Protection Act (PDPA) and internal data protection policies.

Designated Data Protection Officer:
Name: Vanessa Tan
Position: Data Protection Officer
Organisation: Pep & Co Pte Ltd
Email: vanessatan@pepnco.com.sg
Telephone: +65 6908 6577

The DPO oversees internal data protection governance and works with management and technical teams to ensure appropriate safeguards are implemented.

4. Data Protection Contact & Enquiries

Pep & Co welcomes enquiries and feedback regarding the handling of personal data.

Individuals who wish to submit requests relating to personal data access, correction or data protection matters may contact the organisation through the following channels:

General Enquiries Email: enquiry@pepnco.com.sg
Telephone: +65 6908 6577

Requests will be reviewed by the Data Protection Officer and responded to within a reasonable timeframe in accordance with PDPA obligations. Where necessary, the organisation may request additional verification to confirm the identity of the requester.

5. Personal Data Protection Policy

Pep & Co collects and processes personal data only where necessary for legitimate business purposes including service delivery, technical support and contractual obligations.

Pep & Co adheres to the following principles:
• personal data is collected only for legitimate purposes
• only necessary personal data is collected (data minimisation)
• personal data will not be disclosed to unauthorised third parties
• reasonable efforts are made to maintain data accuracy
• personal data is protected using appropriate security safeguards

6. Data Classification

Pep & Co classifies information and data according to sensitivity levels to ensure appropriate protection measures are applied.

Information may generally be categorised as follows:

Public — Information that may be publicly disclosed without risk.
Internal — Information intended for internal use within the organisation.
Confidential — Sensitive business information that should only be accessed by authorised personnel.
Restricted — Highly sensitive information including personal data or security-sensitive system information that requires strict access control.

Security controls and access permissions are applied based on the classification of the data.

7. Information Security & Cybersecurity Framework

Pep & Co maintains an internal cybersecurity framework designed to protect systems against cyber threats, unauthorised access and operational disruption.

Security practices include:
- controlled access to systems and infrastructure
- regular system patching and security updates
- protection against common web application threats
- authentication controls for administrative systems
- monitoring of infrastructure and application environments

These practices are reviewed periodically to ensure alignment with evolving cybersecurity threats.

8. Cloud Infrastructure Security

Pep & Co deploys systems on reputable cloud infrastructure providers that provide enterprise-grade security capabilities.

Production workloads for Singapore-based projects are typically hosted within cloud infrastructure located in Singapore, ensuring that personal data remains within Singapore's jurisdiction.

Infrastructure environments may utilise services provided by major cloud providers such as Amazon Web Services (AWS).

9. Network Security

Pep & Co implements network-level protections to safeguard systems against external threats.

Security protections may include:
- Web Application Firewalls (WAF)

• Distributed Denial-of-Service (DDoS) protection
• traffic filtering and monitoring
• bot protection mechanisms

Where appropriate, platforms such as Cloudflare may be deployed. All web applications enforce secure HTTPS connections to protect data transmitted over the internet.

10. Endpoint Security

Pep & Co deploys endpoint protection mechanisms to monitor production infrastructure.

Endpoint Detection and Response (EDR) platforms may be used to detect suspicious activity. Industry-standard platforms such as CrowdStrike Falcon may be deployed for threat monitoring.

Security alerts are reviewed by the development and infrastructure teams.

11. Access Control & Identity Management

Access to systems and infrastructure is restricted to authorised personnel.

Pep & Co implements:
• secure development repositories
• restricted access to development environments
• role-based infrastructure access
• controlled administrative server access
• Multi-Factor Authentication (MFA) for privileged accounts

Access privileges are granted based on operational necessity and are reviewed periodically.

12. Password Security Policy

Pep & Co enforces secure password standards.

Password requirements include:
• minimum 12 characters
• uppercase and lowercase letters
• numbers and special characters
• avoidance of easily guessable words or patterns

Systems may implement account lockout or rate limiting mechanisms to prevent repeated login attempts.

Passwords are stored using secure hashing mechanisms such as bcrypt or Argon2 and are never stored in plain text.

13. Encryption & Data Protection Measures

Pep & Co implements encryption measures to protect sensitive data.

These protections include:
• TLS encryption for data transmitted over the internet (data in transit)
• AES-256 encryption for stored data (data at rest)
• encryption of system backups and storage services

Where required by project scope, additional protections such as field-level encryption may be implemented for highly sensitive data fields.

14. Monitoring & Logging

Pep & Co monitors its infrastructure environments to detect abnormal activity and operational issues.

Monitoring mechanisms may include:
• infrastructure monitoring platforms
• server event logs
• application logs
• cloud monitoring services such as AWS CloudWatch

Logs may be reviewed periodically to identify anomalies or potential security incidents.

15. Backup & Disaster Recovery

Pep & Co maintains backup procedures to support system recovery in the event of operational incidents.

Backup processes may include:
• automated database backups
• system snapshots
• secure storage of backup data in cloud storage services such as Amazon S3

Backup retention periods are determined based on project requirements and contractual obligations.

16. Data Retention & Secure Disposal

Pep & Co retains personal data only for as long as necessary to fulfil the purposes for which the data was collected, or as required by applicable laws and contractual obligations.

When personal data is no longer required for business or legal purposes, Pep & Co will take reasonable steps to ensure that such data is securely deleted, anonymised, or disposed of in a manner that prevents unauthorised access or recovery.

Secure disposal methods may include:
• permanent deletion of electronic records
• secure destruction of physical records where applicable
• removal of data from active systems and backups in accordance with system retention policies

These practices support compliance with the PDPA retention limitation obligation.

17. Third-Party Service Providers

Pep & Co may utilise reputable third-party technology providers to support system development, infrastructure hosting and cybersecurity protection.

Examples may include cloud infrastructure providers, web security platforms and monitoring services.

Third-party providers are selected based on reliability, reputation and security standards. Where applicable, Pep & Co relies on the security controls and compliance frameworks provided by these technology partners.

18. Security Awareness & Training

Pep & Co recognises that cybersecurity risks can arise not only from technical vulnerabilities but also from human factors.

Pep & Co conducts annual cybersecurity awareness and data protection training for employees to ensure they remain informed about:

- current cybersecurity threats and attack methods
- phishing and social engineering risks
- responsible handling of personal data
- secure development and operational practices
- relevant technology trends and security considerations

Employees are expected to follow internal security policies and report any suspected security incidents or vulnerabilities.

19. Data Breach Response

If a potential data breach is detected, Pep & Co will initiate an internal incident response process.

The organisation will:

- investigate the incident
- contain affected systems
- assess the scope and potential impact of the breach
- implement remediation measures to prevent further exposure

Where required under applicable laws and regulations, Pep & Co will notify relevant authorities and affected individuals in accordance with Singapore's Personal Data Protection Act (PDPA).

The Data Protection Officer oversees the breach response process and coordinates any necessary notifications.

20. Security Governance & Risk Management

Pep & Co recognises that cybersecurity risks evolve continuously and therefore adopts a governance-based approach to managing information security.

Security governance activities may include:
• periodic review of internal cybersecurity policies
• assessment of infrastructure security controls
• monitoring of emerging cybersecurity threats
• review of system access privileges
• review of monitoring alerts and security logs

These activities help ensure that cybersecurity practices remain aligned with industry standards and regulatory expectations.

21. Responsible Disclosure and Security Vulnerability Reporting

Pep & Co encourages responsible disclosure of security vulnerabilities.

Security researchers or members of the public who discover potential vulnerabilities may report them through the following email address:
security@pepnco.com.sg

Pep & Co will acknowledge and investigate vulnerability reports and implement remediation measures where necessary.

22. Policy Review

This policy will be reviewed periodically to ensure alignment with regulatory requirements and industry best practices.

Policy Approval

Document Title: Pep & Co Pte Ltd – Data Protection & Cybersecurity Policy
Version: 2026
Effective Date: 2026
Review Cycle: Annual Review

Approved By:
Managing Director
Pep & Co Pte Ltd