Company Registration No.: 201101014489 (Malaysia)
Headquarters: B-12-01, Atria Damansara, Jalan SS 22/23, Damansara Jaya, 47400, Petaling Jaya, Selangor, Malaysia.
Website: https://www.trides.com.my
Contact: info@trides.com.my

TRIDES SDN BHD — Information Security Policy

1. Introduction

At TRIDES Sdn Bhd ("TRIDES"), information is one of our most valuable assets. As a provider of Identity, Security, and Access Management solutions, TRIDES is committed to safeguarding the confidentiality, integrity, and availability of all information under our control — whether belonging to our company, our clients, or our business partners.

This Information Security Policy (ISP) defines our approach to protecting data, managing access, and ensuring compliance with applicable laws and standards, including the Personal Data Protection Act (PDPA) 2010 and the ISO/IEC 27001 Information Security Management Framework.

2. Purpose

The purpose of this policy is to:

- Protect TRIDES's and clients' information assets against all internal and external threats.
- Ensure business continuity through effective security risk management.
- Provide a framework for the secure management of information systems and resources.
- Promote a culture of security awareness and accountability across the organization.

3. Scope

This policy applies to:

- All employees, contractors, consultants, and third parties with authorized access to TRIDES's systems or information.
- All data, documents, systems, networks, and software owned or managed by TRIDES.
- All physical and digital information, including emails, records, backups, and client data.

4. Information Security Objectives

TRIDES aims to:

- Maintain confidentiality — ensuring that only authorized individuals have access to information.
- Maintain integrity — ensuring information is accurate and protected from unauthorized modification.
- Maintain availability — ensuring systems and data are accessible to authorized users when required.
- Comply with all relevant legal, regulatory, and contractual obligations.

5. Information Classification

All information within TRIDES shall be classified based on sensitivity and business value:

- Public: Information intended for public disclosure (e.g., marketing materials).
- Internal: Operational information restricted to TRIDES personnel.
- Confidential: Sensitive company or client information requiring controlled access.
- Restricted: Critical or privileged data requiring explicit authorization and monitoring.

Each classification level must determine appropriate handling, storage, and transmission controls.

6. Access Control

- Access to systems, applications, and data is granted on a least privilege and need-to-know basis.
- All user accounts must be uniquely identifiable and protected by secure authentication mechanisms (passwords, MFA, or SSO).
- Access rights shall be reviewed periodically and revoked immediately upon employee resignation, role change, or contract termination.
- Administrative or privileged access must be approved by authorized management and logged for audit purposes.

7. Data Protection and Privacy

TRIDES adheres to the principles of the Personal Data Protection Act (PDPA) 2010 and global privacy standards. We commit to:

- Collecting only necessary personal data for legitimate business purposes.
- Storing and processing data securely using encryption and access controls.
- Prohibiting the transfer or disclosure of client data without authorization.
- Retaining data only as long as required by business or legal obligations.

- Ensuring all staff handle personal data responsibly and complete regular data protection training.

8. Physical and Network Security

- Office premises, server rooms, and network facilities must be physically secured and accessible only to authorized personnel.
- Network systems must be protected using firewalls, antivirus, intrusion detection, and regular patching.
- Portable devices and removable media must be encrypted and safeguarded at all times.
- Wi-Fi and VPN access must use secure authentication and encryption protocols.

9. Incident Response and Management

- All employees must report suspected or confirmed security incidents immediately to the IT Security Team or Compliance Office.
- Incidents include data breaches, malware infections, unauthorized access, or loss of devices.
- The Incident Response Plan (IRP) defines containment, investigation, reporting, and recovery procedures.
- Post-incident reviews will be conducted to identify root causes and implement preventive measures.

10. Business Continuity and Backup

- Regular backups of critical data and systems must be performed and tested periodically.
- Backup data must be securely stored and protected from unauthorized access.
- Business continuity procedures ensure minimal disruption during system outages, cyberattacks, or disasters.

11. Employee Responsibilities

All TRIDES employees must:

- Protect company and client information assets.
- Use company devices and systems responsibly.
- Refrain from sharing credentials, sensitive data, or confidential documents without authorization.
- Report any suspicious activities, phishing attempts, or potential risks immediately.

Violation of this policy may result in disciplinary action, including termination or legal proceedings.

12. Compliance and Review

This policy shall be reviewed periodically by the Compliance Office and IT Security Team to ensure alignment with:

- Current legal and regulatory requirements.
- Emerging cyber threats and technological advancements.
- Client contractual obligations and industry best practices.

13. Endorsement

This Information Security Policy has been reviewed and approved by the Board of Directors of TRIDES Sdn Bhd and is effective as of January 2025.

TRIDES SDN BHD
Driving Digital Identity, Securely and Responsibly.