Mandatory PDPA Compliance & Cybersecurity Essentials – Course Outline and Schedule

2 days training

Introduction

In 2026, data protection is no longer optional; it is a legal mandate. This program is designed to align with the **Personal Data Protection Act (PDPA) 2024 Amendments** and the **Cyber Security Act 2024 (Act 854)**. Awareness of mandatory breach notifications, the role of the Data Protection Officer (DPO), and digital defense mechanisms enable organizations to reduce **legal and reputational risks** while ensuring audit readiness in an increasingly regulated landscape.

Learning Objectives

- **Understand** the legal implications of the **Cyber Security Act 2024** and the new mandatory **PDPA breach notification** requirements.
- **Identify and Mitigate** risks of data leaks, ransomware, and AI-driven cyber threats in daily business operations.
- **Apply** a practical framework to conduct internal **Data Protection Impact Assessments (DPIA)** and security audits.
- **Navigate** the official reporting mechanisms for data breaches to the Commissioner within the mandatory **72-hour window**.
- **Demonstrate** commitment to digital ethics and **Social Responsibility (ESG)** by protecting client and employee privacy.

Target Participants

To ensure the organization meets its legal obligations under the **Cyber Security Act 2024** and the **PDPA 2024 Amendments**, this program is designed for the following roles:

- **Business Owners & Directors**: To understand their personal and corporate liability regarding the new fine structures and potential imprisonment for non-compliance.
- **Appointed Data Protection Officers (DPOs)**: Essential training for those legally mandated to oversee data privacy, manage the Breach Register, and communicate with the Commissioner.
- **HR & Administrative Managers**: Professionals handling sensitive employee data, biometric records, and payroll information that must satisfy the "Security Principle".
- **IT Managers & System Administrators**: Staff responsible for implementing technical safeguards like encryption and MFA to defend against AI-driven threats.
- **Compliance & Risk Officers**: Individuals tasked with ensuring the company is "Audit Ready" and maintaining the internal T.R.U.S.T. framework for digital ethics.
- **Legal & Operations Heads**: To align internal policies with mandatory 72-hour breach notification rules and manage third-party vendor risks.

© Knowledge Tree PLT
www.cadtraining.com.my

Methodology

The program uses a **Practical Awareness Approach**. Instead of heavy technical workshops, we utilize **Scenario-Based Discussions**, **Real-World Case Studies** (including recent 2025/2026 breaches), and **Interactive Q&A**. The session concludes with a **Competency Assessment** and the drafting of an **Incident Response Plan** to ensure a documented commitment to compliance.

© Knowledge Tree PLT
www.cadtraining.com.my

Course Outline and Schedule

Day 1: The Legal Mandate & PDPA 2026 Compliance

Time	Topic / Activity
9.00 a.m. – 9.30 a.m.	**Foundation: Data Privacy & The Regulatory Framework** * Trainer & participant introduction; Expectation setting; Why PDPA and the Cyber Security Act matter in 2026.
9.30 a.m. – 10.30 a.m.	**The New Landscape of Malaysian Law** * Overview of **Act 854** and **PDPA 2024 Amendments**; Legal risks & liabilities for "Associated Persons" and Directors.
10.30 a.m. – 12.15 p.m.	**The Mandatory Data Protection Officer & Audit Readiness** * Who must appoint a DPO?; Duties and personal liability; Registration process with the Commissioner.
12.15 p.m. – 1.15 p.m.	**Lunch Break**
1.15 p.m. – 2.30 p.m.	**Mandatory Breach Notifications** * The 72-hour rule; Documentation and maintaining a Breach Register; When and how to notify the Commissioner.

© Knowledge Tree PLT
www.cadtraining.com.my

2.30 p.m. – 3.45 p.m.	**Data Protection Impact Assessments (DPIA)** * Conducting risk audits; Updating privacy notices for 2026 standards; Managing data portability.
3.45 p.m. – 4.30 p.m.	**Internal Reporting & Data Rights** * Overview of internal control mechanisms; Managing individual "Right to be Forgotten" requests; Reporting misconduct basics.
4.30 p.m. – 5.00 p.m.	**Day 1 Summary & Compliance Reflections** * Key legal takeaways; Q&A session; Building a "Privacy-First" mindset.

© Knowledge Tree PLT
www.cadtraining.com.my

Day 2: Cybersecurity Defense & Audit Readiness

Focus: Practical Security Measures to Satisfy the "Security Principle".

Time	Topic / Activity
9.00 a.m. – 10.30 a.m.	**Anatomy of 2026 Cyber Threats** * AI-enhanced phishing, deepfake scams, and ransomware evolution.
10.30 a.m. – 12.15 p.m.	**Technical Safeguards & Access Control** * MFA, Encryption, and "Least Privilege" for satisfying security audits.
12.15 p.m. – 1.15 p.m.	**Lunch Break**
1.15 p.m. – 3.00 p.m.	**Developing an Incident Response Plan (IRP)** * **Workshop:** Drafting a 1-page Emergency Response protocol.
3.00 p.m. – 5.00 p.m.	**Final Audit Preparation & Summary** * Preparing for NACSA/PDPC visits; Building "Cyber Hygiene".

© Knowledge Tree PLT
www.cadtraining.com.my