AI Management Programme

Justin Law, June 2024

Background

To fulfill the Personal Data Protection requirements suggested by the Hong Kong Personal Data (Privacy) Commission Officer in June 2024, I made reference to the current Privacy Management Programme (PMP) to fit the AI technology. It aims to provide the company with a management framework to adopt AI technology in a secure and responsible way.

Overview

1. Organisational Commitment

1. Organisational Commitment

1.1 Appointment of AI Personal Data Protection Officer (ADPO)

- Top-down approach
- Assign a senior management to be the role of ADPO
- In charge all related AI issues
- Reviewing the effectiveness
- Reporting to the top management periodically

1.2 Establish AI Governance Committee

A cross-functional team

- business and operational personnel,
- procurement teams,
- system analysts,
- system architects,
- data scientists,
- Cybersecurity professionals,
- legal and compliance professionals (including data protection officer(s)),
- internal audit personnel,
- human resources personnel customer service personnel.

1.3 Establish reporting mechanism

- Establish internal reporting mechanisms
- Clearly state the reporting structure
- procedures for reporting organisation's overall compliance situation
- Report to PDPO

2. Programme Controls

2.1 AI Inventory

Establishing an AI inventory

- How to collecting personal data
- What kinds of personal data collected
- Where the data stored
- The duration of retention,
- the ways of using

2.2 Develop MTR CGI on the Use of AI and data policy

- Develop MTR CGI to provide direction in the use of AI technology
- Privacy-by-design principle
- Ethical use
- Min. Bias/Variance
- Prevent Hallucinations

2.3 Establish AI Security Task Force
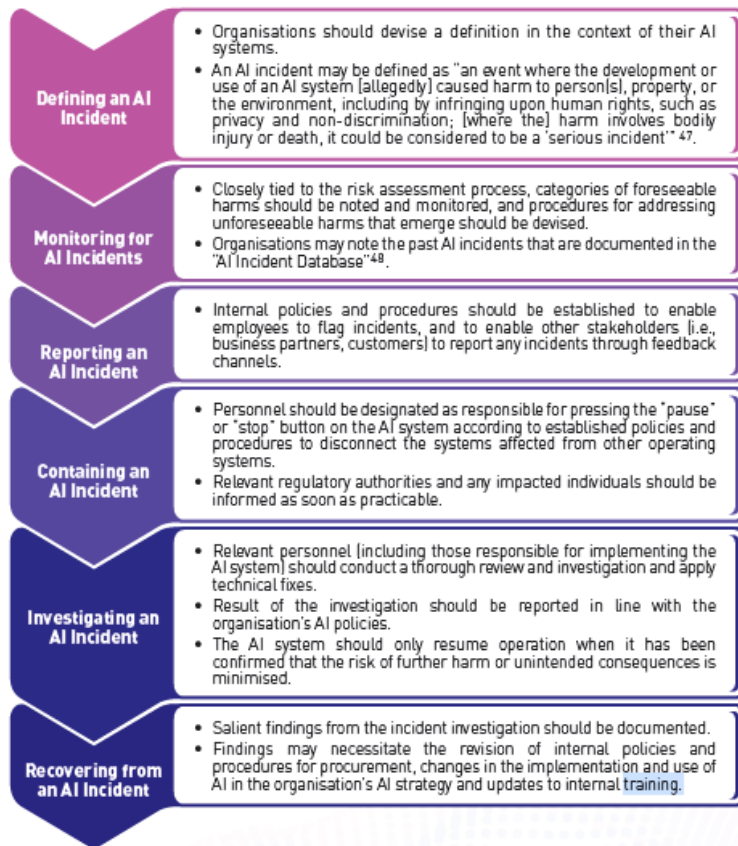
Establish Task force for operations

- Conduct Risk and Security Assessment

2.4 Training and Communication

- Internal training and education
- Communication with stakeholders

Establishing an AI incident plan

Stage	Details
Defining an AI Incident	• Organisations should devise a definition in the context of their AI systems. • An AI incident may be defined as "an event where the development or use of an AI system [allegedly] caused harm to person(s), property, or the environment, including by infringing upon human rights, such as privacy and non-discrimination; [where the] harm involves bodily injury or death, it could be considered to be a 'serious incident'" [47].
Monitoring for AI Incidents	• Closely tied to the risk assessment process, categories of foreseeable harms should be noted and monitored, and procedures for addressing unforeseeable harms that emerge should be devised. • Organisations may note the past AI incidents that are documented in the "AI Incident Database" [48].
Reporting an AI Incident	• Internal policies and procedures should be established to enable employees to flag incidents, and to enable other stakeholders (i.e., business partners, customers) to report any incidents through feedback channels.
Containing an AI Incident	• Personnel should be designated as responsible for pressing the "pause" or "stop" button on the AI system according to established policies and procedures to disconnect the systems affected from other operating systems. • Relevant regulatory authorities and any impacted individuals should be informed as soon as practicable.
Investigating an AI Incident	• Relevant personnel (including those responsible for implementing the AI system) should conduct a thorough review and investigation and apply technical fixes. • Result of the investigation should be reported in line with the organisation's AI policies. • The AI system should only resume operation when it has been confirmed that the risk of further harm or unintended consequences is minimised.
Recovering from an AI Incident	• Salient findings from the incident investigation should be documented. • Findings may necessitate the revision of internal policies and procedures for procurement, changes in the implementation and use of AI in the organisation's AI strategy and updates to internal training.

- A risk-based approach should be adopted in the procurement

3. Ongoing Assessment and Revision

3.1 Regular review and audit

- Regular review
  - Update AI inventory
  - Conduct risk assessment
  - Update training content
  - Revise operation manual
- Annual audit and International certificate (e.g. ISO)