Guidance on

Data Security Measures for Information and Communications Technology

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Introduction

The Guidance Note on Data Security Measures for Information and Communications Technology (Guidance) provides data users with recommended data security measures for information and communications technology to facilitate their compliance with the requirements under the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO), as well as good practices in strengthening their data security systems. This pamphlet highlights the core recommendations of the Guidance.

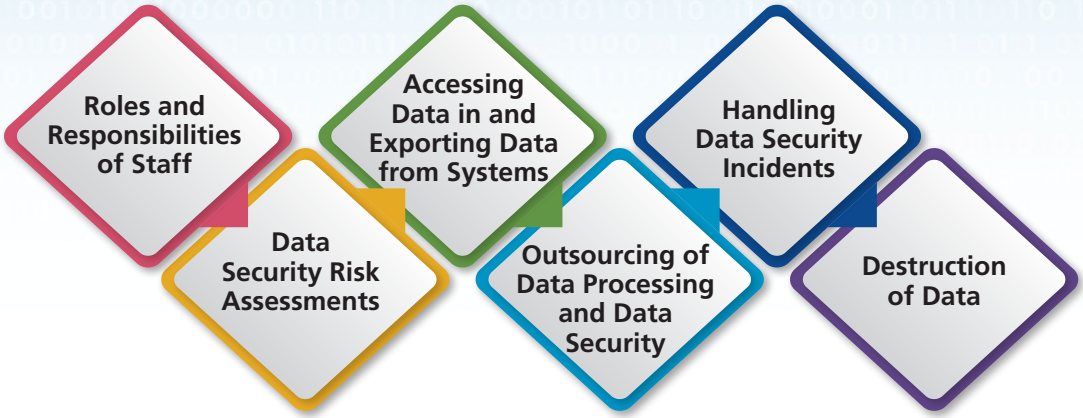
Recommended Data Security Measures for Data Users are Grouped into 7 Key Areas:

- Data Governance and Organisational Measures
- Risk Assessments
- Technical and Operational Security Measures
- Data Processor Management
- Remedial Actions in the Event of Data Security Incidents
- Monitoring, Evaluation and Improvement
- Other Considerations

Data Governance and Organisational Measures

- **Policies and Procedures**

  A data user should establish policies and procedures on data governance and data security covering:



- **Manpower**

  Appoint suitable personnel in a leadership role to bear specific responsibilities for data security.

  The number, seniority and technical competence of staff members allocated for data security should be proportional to the nature, scale and complexity of data processing activities, as well as the data security risks.

- **Training**

  Training should be provided for staff members at induction and at regular intervals:

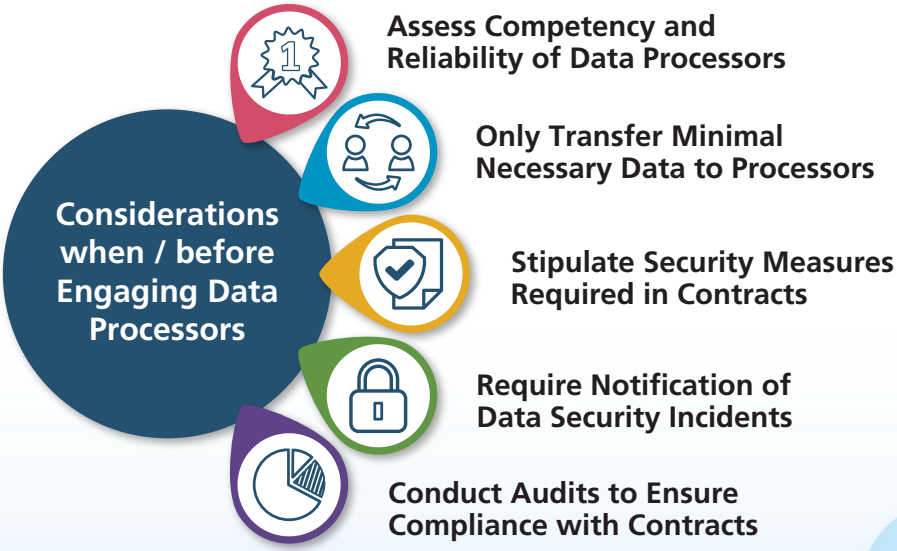
Risk Assessments

- Conduct risk assessments on data security for new systems and applications before launch — engage third party specialists where necessary
- Report results of risk assessments to senior management regularly
- Address the security risks identified promptly

Technical and Operational Security Measures

Data Processor Management

Pursuant to Data Protection Principle 4(2) under the PDPO, a data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the personal data transferred to its data processors for processing.



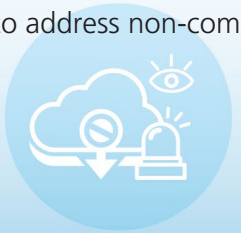
Common Remedial Actions in the Event of Data Security Incidents

Timely and effective remedial actions taken by a data user after the occurrence of a data security incident may reduce the risks of unauthorised or accidental access, processing or use of the personal data affected and gravity of harm that may be caused to the affected individuals.

- Stopping and Disconnecting the Affected Systems
- Changing Passwords or Ceasing Access
- Changing System Configurations
- Notifying and Advising the Affected Individuals
- Reporting to the PCPD and Other Law Enforcement Agencies / Regulators
- Fixing the Security Weakness
- Scanning the Systems if Feasible
- Following Up on the Lessons Learnt

Monitoring, Evaluation and Improvement

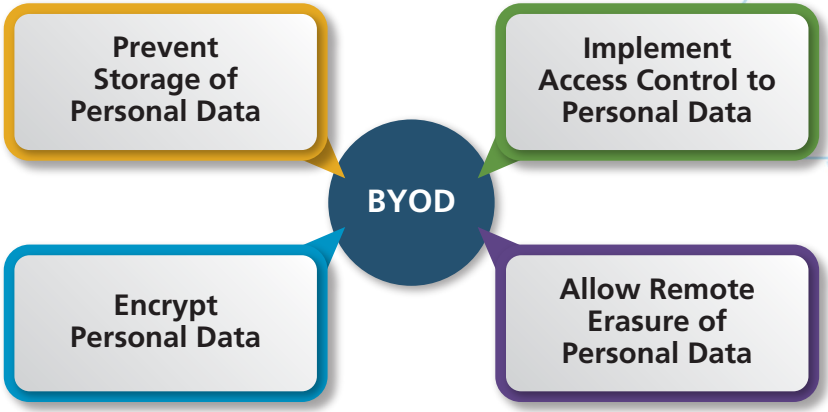
- Commission an independent task force (e.g. internal or external audit team) to monitor compliance with the data security policy and evaluate the effectiveness of data security measures periodically
- Take steps to address non-compliant practices and ineffective measures



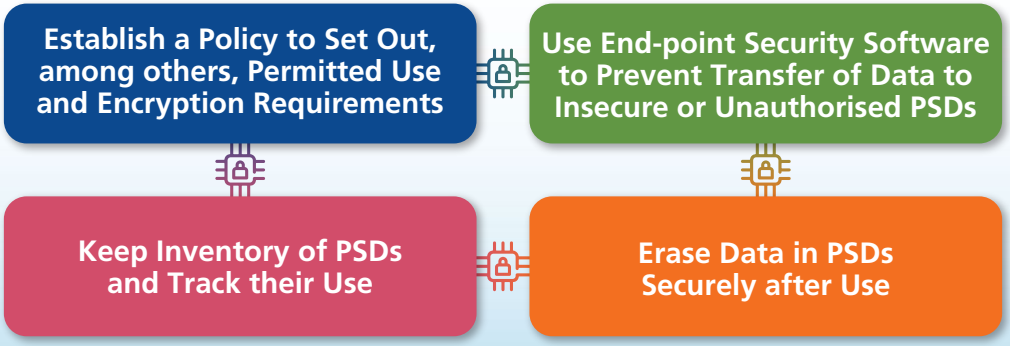
Other Considerations

- **Considerations when Using Cloud Services**

- **Security Measures when Implementing Bring Your Own Device (BYOD) Policy**



- **Security Measures for the Use of Portable Storage Devices (PSDs)**



PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Download this Publication

Download the Guidance Note

Unit 1303, 13/F., Dah Sing Financial Centre,
248 Queen's Road East, Wanchai, Hong Kong

Tel : 2827 2827
Fax : 2877 7026
E-mail : communications@pcpd.org.hk
Website : www.pcpd.org.hk

First published in February 2023

Printed on recycled paper