*SCAPE Security & PDPA Essentials

Data Handling & Security Basics

Purpose of This Guide

This guide outlines essential data protection and cybersecurity practices at *SCAPE. It aims to help employees handle personal data responsibly and protect organisational information in compliance with Singapore’s Personal Data Protection Act (PDPA).

1. PDPA Basics

1. Personal data must be collected, used, and disclosed only for legitimate purposes.
2. Consent must be obtained before collecting or using personal data.
3. Access to personal data should be limited to authorised personnel only.
4. Personal data should be retained only as long as necessary.

2. Data Handling Guidelines

1. Store personal and confidential data in approved systems only.
2. Do not share personal data via unsecured channels.
3. Verify recipient details before sending emails containing sensitive information.
4. Dispose of physical documents securely (e.g. shredding).

3. Security Basics

1. Use strong passwords and do not share login credentials.
2. Lock your device when unattended.
3. Be alert to phishing emails, suspicious links, or unknown attachments.
4. Install updates and patches as required on work devices.

4. Data Breach & Incident Reporting

Any suspected data breach, loss of device, or security incident must be reported immediately to your supervisor or the designated data protection or IT team. Prompt reporting helps minimise risk and ensures compliance with PDPA requirements.

5. Employee Responsibility

All employees share responsibility for safeguarding personal data and organisational information. Failure to comply with security and PDPA requirements may result in disciplinary action.