



Think IT ~ Think Us

PRO OFFICE TECHNOLOGY SDN BHD

Security Guidelines for Mobile Device Usage

All information is proprietary to PRO OFFICE TECHNOLOGY SDN. BHD. ("PROOFFICE"). The information may not be disseminated, distributed, reproduced, or transmitted in any manner without prior written consent of PROOFFICE.

It is important to protect your devices against cybercrime or theft.

This document outlines the usage and protection of PROOFFICE mobile devices and storage systems, including:

- “Portable computers” i.e., laptops
- “Mobile devices” such as smartphones and tablets
- “Portable media” used for digital storage such as USB Flash Drive/CDs/DVDs, etc.

Portable computers and mobile devices provide convenience and mobility, enabling PROOFFICE staff to work from any location. These devices are, however, a target for theft and may be misplaced or lost by the owner.

If you suspect PROOFFICE data has been breached you are required to report the case to local service desk immediately via telephone, email or face-to-face. Please refer to contact details in Appendix (A).

For any enquiries, please contact your local service desk.

You Should:

1. While at your workplace, keep your portable computer, mobile devices, and portable media in an access-controlled area. Always use a cable lock or U-clamp to secure your laptop to a fixed object such as a desk when you leave it unattended. In public places, keep your portable computer, mobile devices, and portable media under your direct control and never leave them unattended.
2. To collect, use and retain personal data for a legitimate reason you should render your best effort in protecting personal data as required by the law and PROOFFICE requirements.
3. When you leave your workplace for an extended period, either take your portable computer, mobile devices, and portable media with you, or lock them in an enclosed drawer or cabinet. Do not rely on a cable lock to secure your laptop for extended periods of time (e.g., overnight).

4. If using a shared cabinet to lock up your portable computer, mobile devices, and portable media, consider the availability of spare keys and manage these appropriately.
5. Be aware of your surroundings and take precautions to prevent PROOFFICE INTERNAL USE ONLY, CONFIDENTIAL & CONFIDENTIAL RESTRICTED INFORMATION displayed on your screen from being viewed by unauthorized persons. For example, use a privacy screen filter to keep your private data safe from visual hacking.
6. Use a strong password pattern to protect your devices and the PROOFFICE system. Please refer to Appendix (B).
7. Always use the built-in password lock feature to lock your mobile devices when on and not in use.
8. Always upgrade your mobile device with the latest o/s and security updates, and setup anti-virus protection.
9. Logout of the system when you are not using it.
10. When travelling by plane, train, bus, etc., take your portable computer, mobile devices, and portable media on board with you as carry-on luggage, rather than checking them in and/or letting them out of your direct control. Check in laptop cable locks to prevent confiscation by airport security.
11. Delete all PROOFFICE digital programs or apps in all portable media or devices that are no longer needed to access PROOFFICE systems.
12. Only use a recommended device to access PROOFFICE system for enjoying the best view. Please check the Appendix (C) and review the minimal device requirement.

You should never:

Note: For any regulatory and legislation breach, the offender will be subject to potential legal liabilities under relevant local regulations and legislation issued by local authorities and internal disciplinary actions, if needed.

1. Jail-break your mobile device if you use that device for accessing Sun Life Malaysia digital programs or websites, as it may create a security hole for

hackers to reach PROOFFICE INTERNAL USE ONLY, CONFIDENTIAL & CONFIDENTIAL RESTRICTED INFORMATION.

2. Store your ACCESS MECHANISMS and/or ACCESS CREDENTIALS along with your portable computer, mobile devices, or portable media, for example in your laptop bag or device carrying case.
3. Store your IDs or passwords/PINs in the same place as your mobile devices.
4. Share or tell other people about your passwords/PINs.
5. Use personal portable media such as USB Flash Drive, personal cloud storage to store PROOFFICE INTERNAL USE ONLY, CONFIDENTIAL & CONFIDENTIAL RESTRICTED INFORMATION.
6. Store your portable computer, mobile devices or portable media anywhere unattended in your vehicle for extended period of time (e.g. overnight). If you need to leave them in your vehicle for short periods of time, be sure to take the following minimum precautions:
 - Store them out of plain sight and lock the vehicle and make sure all openings are closed.
 - Do not leave spare keys in the vehicle (an experienced thief knows all the hiding places).
 - Exercise due care with respect to environmental issues such as heat or cold.

Appendix:

| | |
|--|---|
| A) Contact details in case you need assistance or escalate the incident | Local service desk support hotline: 1800-88-6858 (Toll Free) 03-8061 7913 weekdays (Mon – Sat) 8am-6pm Local service desk support email: helpdesk.support@prooffice.my Technical Support PIC Support Agent Mobile +6011-28726858 (Mon – Sun) 24/7 |
| B) Strong Password | Minimal 12 characters with Alphanumeric & symbols & CAPITAL characters |
| C) Minimal device requirements | Mobile <ul style="list-style-type: none">• Minimum Android 9 or above• Minimum IOS 9 or above Laptop/PC <ul style="list-style-type: none">• Minimum Windows 10 21H2 or above• 1 Gigahertz (GHz) or faster processor or System on a Chip (SoC)• 32 GB hard disk space or above• 4Gb of RAM or above |