PROSEDUR TETAP (PROTAP)
SECURED COMMUNICATION INTERNET MALINDO (SCIM)

PENDAHULUAN

1. SCIM merupakan aplikasi yang membolehkan pengguna berkomunikasi dalam bentuk elektronik terselamat di antara satu sama lain secara langsung dengan menggunakan aplikasi *Video Conferencing* (VC) dan e-mel.

2. Penggunaan internet mudah terdedah kepada ancaman. Justeru penggunaan SCIM mampu mengawal penyebaran maklumat bagi menjamin tahap keselamatan komunikasi untuk mengekalkan kerahsian (confidentiality), integriti (integrity), kesiapsediaan (availability) dan kesahihan (authenticity).

TUJUAN

3. Tujuan garis panduan ini adalah untuk :

   a. Menerangkan tatacara pengendalian SCIM.

   b. Menerangkan tugas dan tanggungjawab pengguna SCIM.

   c. Menerangkan jenis-jenis maklumat yang boleh disebarkan melalui SCIM.

   d. Meningkatkan tahap keselamatan sistem komunikasi.

KEPERLUAN SISTEM

4. **Konfigurasi Perkakasan (Hardware) Pengguna.** Keperluan konfigurasi minima komputer pengguna bagi menggunakan SCIM adalah seperti berikut:

   a. Intel Core 2 Duo Processor/AMD Turion.

   b. HDD – 20 GB.

   c. RAM 1 GB (Windows 2000/XP) atau 2 GB (Windows Vista/7).

   d. CD - Rom.

5. **Aplikasi Sistem.** Keperluan perisian untuk SCIM adalah seperti berikut:

   a. Aplikasi VC terselamat.

   b. Aplikasi e-mel terselamat.

TATACARA PENGENDALIAN SCIM

6. **Akaun SCIM.** Akaun atau alamat e-mel yang digunakan adalah seperti diperuntukan oleh Sekretariat TPK di **Kembaran A.**

7. **Format E-Mel.** Penyampaian maklumat rasmi melalui e-mel hendaklah mengandungi nombor rujukan fail sepertimana yang terdapat dalam prosuder persuratan rasmi biasa. Contoh adalah seperti di **Kembaran B.**

8. **Penghantaran E-Mel.** Elakkan dari menghantar fail-fail e-mel yang terlalu besar. Gunakan kaedah penempatan (compression) untuk megurangkan saiz fail sekiranya perlu.

9. **Aktiviti Yang Dilarang.** Pengguna adalah dilarang:

a. Menghantar e-mel yang berunsur fitnah, hasutan (mail flaming), mel sampah (junk mail), mel bom (mail bombing) dan mel spam (mail spamming).

b. Menerbit semula hak cipta kepunyaan orang lain.

c. Muat turun, menghantar dan memiliki bahan-bahan lucah dan berunsur seks.

d. Melibatkan diri dalam e-mel berantai.

e. Menggunakan e-mel untuk tujuan komersial.

f. E-mel ini tidak boleh digunakan untuk tujuan peribadi.

KESELAMATAN

10. **Keselamatan Komputer Yang Mengendalikan Maklumat Berdarjah.** Keselamatan maklumat berdarjah berkait rapat dengan keselamatan komputer di mana aplikasi SCIM tersebut digunakan. Rujuk kepada tatacara pengendalian komputer negara masing-masing.

11. **Keselamatan E-mel.** Keselamatan e-mel bergantung kepada faktor-faktor berikut:

a. **Darjah Keselamatan.** Penggunaan maklumat yang berdarjah RAHSIA dan ke bawah sahaja dibenarkan melalui SCIM.

b. **Keselamatan Komputer.** Pengguna komputer SCIM hendaklah memastikan keselamatan penggunaan dan penyimpanan perkakasan. Pengguna juga dikehendaki mengaktifkan penggunaan nama pengguna dan kata laluan sebelum memasuki aplikasi *windows* komputer SCIM.

c. **Keselamatan Dokumen.**

(1) **Penggunaan Perisian Anti-Virus dan *Malicious Codes*.**

(a) Pastikan semua fail yang dihantar dan diterima adalah virus dan *malicious codes*. Pengguna perlu melaksanakan

imbasan setiap kali penggunaan media storan selain dari storan komputer SCIM.

(b) Jangan membuka mana-mana e-mel dan fail kepilan yang tidak
diketahui pengirimnya atau pengirim yang tidak boleh dipercayai.
(c) Pastikan perisian anti-virus dan penapis *malicious codes* dikemaskini secara berjadual.

(2) **Penyimpanan Maklumat.** Semua maklumat yang sudah diambil tindakan perlu dimusnahkan (delete). Sekiranya maklumat tersebut masih diperlukan, pengguna perlu menyimpannya dalam media storan yang berasingan.

d. **Keselamatan Kata Laluan**. Kata laluan bagi aplikasi Tandberg Movi akan ditukar oleh Pentadbiran Sistem SCIM negara masing-masing setiap 3 bulan. Penukaran kata laluan bagi e-mel boleh dilakukan oleh pengguna pada sebilang masa. Garis panduan untuk kata laluan adalah seperti berikut di **Kembaran C.**

12. ***Bounce Mail*.** Penggunaan yang menghantar (sender) tidak dibenarkan menghantar semula e-mel yang di kembalikan oleh sistem (bounce mail) sebelum menyiasat punca kejadian penghantar perlu menghubungi Pentadbir Sistem untuk siasatan lanjut.

13. **Memajukan (Forwarding).** Segala e-mel hanya boleh dimajukan semula kepada pihak yang berdaftar dan layak sahaja.

PELANGGARAN KESELAMATAN (SECURITY BREACHES)

14. Pelanggaran keselamtan merupakan insiden di mana tahap keselamatan telah dikompromi dan bertentangan dengan peraturan-peraturan keselamatan, samada disebabkan kecuaian atau perbuatan yang tidak disengajakan. Pelanggaran Keselamatan merangkumi, dan tidak terhad kepada perkara berikut:

a. Kompromi maklumat berdarjah.

b. Kehilangan maklumat berdarjah.

c. Kecurian.

d. Kerosakan kepada material dan aset.

e. Penyebaran virus.

f. Pendedahan nama pengguna dan kata laluan kepada orang yang tidak berkenaan.

g. Mengubah perisian tanpa kelulusan.

KEMBARAN A

AKAUN *SECURED COMMUNICATION INTERNET* MALINDO (SCIM) MALAYSIA

Bil	Nama	Jawatan	Akaun VC	Akaun e-mel
1	Ketua TPK Malaysia	AKS KOMLEK	ptpkm	pkpkm@malindo.mil.my
2	Pengarah Rancang	Pengarah Rancang KOMLEK	prk	prk@malindo.mil.my
3	Ahli TPK MK ATM	PS 1 Op – KOMLEK	tpkmatm	tpkmatm@malindo.mil.my
4	Ahli TPK Darat	Pegawai Memerintah 1 RSD	tpkdarat	tpkdarat@malindo.mil.my
5	Ahli TPK Laut	Pegawai Memerintah SKTLDM Lumut	tpklaut	tpklaut@malindo.mil.my
6	Ahli TPK Udara	PS 2 Analisa – MTU JTMK	tpkudara	tpkudara@malindo.mil.my
7	Pentadbir Sistem	PS 2 Kripto – KOMLEK	cps	cps@malindo.mil.my
8	PS 2 Op A	PS 2 Op A – Komlek	opa	opa@malindo.mil.my
9	PS 2 Op B	PS 2 Op B – Komlek	opb	opb@malindo.mil.my
10	Sekretariat MALINDO	Majlis Keselamatan Negara	mkn	mkn@malindo.mil.my
11	Sekretariat COCC	PS 1 A/PS 2 A – BOLP	skcocc	skcocc@malindo.mil.my
12	Sekretariat TPK	PS 2 Op C – KOMLEK	sktpk	sktpk@malindo.mil.my
13	Sekretariat TPI	PS 2 Darat - BSPP	sktpi	sktpi@malindo.mil.my
14	Sekretariat TPOD	PS 2 Gerak – MK 1 Div Inf	sktpod	sktpod@malindo.mil.my
15	Sekretariat TPOL	PS 2 OPS A – MTL RANOP	sktpol	sktpol@malindo.mil.my
16	Sekretariat TPOU	PS 2 K & L – MOU RANOP	sktpou	sktpou@malindo.mil.my
17	MK ATM – KOMLEK	Bilik Mesyuarat Mat Kilau	bmmk	
18	MABES	Sekretariat TPK	mabes	mabes@malindo.mil.my

KEMBARAN B

FORMAT E-MEL

To (Kepada) :
CC (Salinan Kepada) :
BCC (Salinan Karbon Buta):
Subject (Perkara) :
Rujuk Fail: TEKS   Tarikh: Nama dan Jawatan Pengirim: No. Tel:

KEMBARAN C

GARIS PANDUAN KESELAMATAN KATA LALUAN

1. Rahsiakan kata laluan anda dari pengetahuan orang lain.

2. Sekiranya kata laluan telah dikompromi atau disyaki dikompromi, hendaklah diubah dengan serta merta dan dilaporkan kepada Pentadbir Sistem.

3. Kata laluan Tandberg Movi akan dikemaskinikan oleh Pentadbir Sistem negara masing-masing setiap 3 bulan sekali.

4. Kata laluan bagi e-mel dan sistem operasi komputer pengguna adalah atas urusan pengguna.

5. Kata laluan hendaklah mengandungi campuran *alphanumeric* dan simbol khas yang terdiri daripada sekurang-kurangnya 8 aksara. Contoh kata laluan yang baik adalah “rahm@n3204”. (Amaran: Jangan guna kata laluan ini kerana ianya telah diketahui umum).

6. Jangan menggunakan semula kata laluan yang lama.

7. Jangan sekali-kali menyalin kata laluan di mana-mana media. Ianya hendaklah dihafal.