ARAHAN PENGENDALIAN KOMPUTER BAGI SECURE *DIGITAL COMMUNICATION SYSTEM* (SDCS)

1. Perkembangan teknologi masa kini memungkinkan penghantaran data tanpa *encryption* dengan mudah dapat dibaca oleh pihak yang tidak dikehendaki. Bagi mengatasi masalah tersebut, *Secure Digital Communication System* (SDCS) telah dibangunkan untuk membolehkan pengguna berkomunikasi secara selamat menghantar dan menerima *elektronik mail* (e-mail) dalam bentuk *encryption*. Setiap pengguna sistem ini akan dibekalkan komputer riba yang dilengkapi dengan Kad Pintar (*Smart Card*) dan Pembaca Kad (*Card Reader*).

TUJUAN

2. Tujuan arahan ini dikeluarkan adalah untuk memberi panduan kepada pengguna SDCS bagi memastikan komputer sentiasa berada dalam keadaan selamat dan bebas dari sebarang ancaman penggodam serta virus di samping dapat mengurangkan kesan *negative* keatas maklumat seperti pencerobohan, kecurian dan pengubahsuaian data.

OBJEKTIF

3. Objektif garis panduan penggunaan komputer SDCS adalah seperti berikut :

   a. Menjamin semua perkakasan, perisian dan data SDCS adalah selamat daripada kehilangan, penyalahgunaan atau penyelewengan.

   b. Meminimumkan kerosakan ke atas komputer SDCS.

   c. Memastikan penghantaran dan penerimaan data yang lancar dan berterusan tanpa sebarang masalah.

   d. Melindungi kepentingan dan kerahsiaan maklumat dan data yang dihantar.

POLISI KESELAMATAN

4. Selain daripada garis panduan ini, semua pengguna adalah tertakluk kepada polisi-polisi berikut :

   a. Polisi Keselamatan ICT ATM.

   b. *Malaysian Armed Forces Security Instruction*.

   c. Akta Angkatan Tentera 1972.

d. Akta Rahsia Rasmi 1972.

e. Akta Jenayah Komputer 1997.

f. Akta Tandatangan Digital 1997.

LANGKAH-LANGKAH KESELAMATAN

5. Akaun Pengguna. Pengguna adalah bertanggungjawab atas sistem yang digunakan. Bagi mengenal pasti pengguna dan aktiviti ytang dilakukan, langkah-langkah berikut hendaklah diamalkan :

a. Pengguna yang sah sahaja akan diperuntukkan akaun untuk mencapai sistem ini.

b. Akaun pengguna adalah unik iaitu tidak sama antara satu sama yang lain.

c. Akaun pengguna akan diberikan satu kata laluan yang unik oleh pentadbir sistem dan kata laluan tersebut hendaklah diingati atau disimpan di tempat yang selamat.

d. Akaun pengguna yang diwujudkan akan diberi tahap capaian minimum iaitu untuk membaca, menghantar dan melihat sahaja. Perubahan kepada tahap yang lebih tinggi perlu mendapat kelulusan daripada pentadbir sistem.

e. Pentadbir sistem boleh membekukan atau menamatkan akaun pengguna atas sebab-sebab berikut :

(1). Bertukar bidang tugas kerja.

(2). Bertukar keluar.

(3). Bersara.

(4). Ditamatkan perkhidmatan.

6. Pengesahan Pengguna. Proses pengesahan pengguna akan dijalankan sebelum komputer yang menggunakan sistem ini diberikan kepada pengguna. Ciri-ciri pengguna yang sah adalah seperti berikut :

a. Setiap pengguna akan diberikan satu kad pintar yang dilabelkan dengan nombor siri unik.

b. Kata laluan yang berlainan dan unik akan diberikan kepada pengguna baru semasa penggunaan kali pertama.

c. Pengguna tidak boleh berkongsi kad pintar dengan pengguna lain. Kad pintar hanya dibekalkan kepada seorang pengguna sah sahaja.

d. Akaun pengguna akan disekat selepas tiga kali percubaan pengesahan untuk memasuki sistem gagal. Sekiranya berlaku, pengguna perlu melaporkan kepada pentadbir sistem untuk tindakan mengaktifkan kad pintar dan akaun yang baru.

7. Komputer Yang Ditinggalkan Sementara. Komputer yang ditinggalkan untuk seketika mestilah dilindungi daripada sebarang bentuk penyalahgunaan. Berikut adalah beberapa prosedur keselamatan yang perlu dipatuhi :

a. Menarik keluar kad pintar daripada pembaca kad supaya membolehkan sistem terkunci secara automatik.

b. Membawa bersama kad pintar semasa meninggalkan komputer tanpa membiarkan kad pintar pada pembaca kad.

8. Kad Pintar. Kad Pintar yang diberikan kepada pengguna sistem mempunyai cip berteknologi tinggi. Oleh itu, adalah menjadi kewajipan kepada pengguna untuk menjaga Kad Pintar ini daripada rosak atau hilang. Berikut adalah beberapa langkah yang perlu dipatuhi oleh pengguna di dalam menjaga keselamatan Kad Pintar :

a. Tidak mendedahkan Kad Pintar kepada kepanasan yang melampau.

b. Tidak terdedah kepada *electromagnet* kerana ini boleh merosakkan cip Kad Pintar.

c. Menghindarkan cip Kad Pintar dari terguris atau terkena sebarang bentuk fizikal yang boleh merosakkannya.

d. Pengguna adalah bertanggungjawab ke atas keselamatan Kad Pintar. Sebarang bentuk kerosakan atau kehilangan hendaklah dimaklumkan dengan segera kepada pentadbir sistem.

e. Tindakan disiplin akan dikenakan kepada pengguna sekiranya Kad Pintar disalahgunakan.

9. Perisian Berbahaya (*Malicious*). Pengguna hendaklah memastikan semua pembangunan perisian adalah bebas daripada program yang berbahaya atau kerosakan yang boleh mengganggu sistem operasi atau mengakibatkan maklumat terdedah kepada ancaman. Untuk memastikan perkara tersebut tidak berlaku, perkara-perkara berikut perlu dipatuhi :

a. Tidak memuat turun perisian yang tidak diketahui tahap keselamatannya.

b. Memasang komputer dengan sistem pertahanan (*Anti Virus*) untuk mempertahankan sistem daripada sebarang serangan virus dan penggodam.

c. Sentiasa mengemaskinikan sistem pengoperasian dengan *service pack patches* yang telah dikeluarkan oleh Microsoft dan sentiasa melakukan pembersihan komputer (*computer scan*).

10. Penggunaan Disket dan *Thumb Drive.* Virus boleh disebarkan dengan pelbagai cara. Terdapat berbagai jenis virus yang boleh mengakibatkan kerosakan kepada sistem dan perisisan. Oleh itu, perkara-perkara berikut perlu dititikberatkan semasa menggunakan komputer untuk mencapai sistem :

a. Sebarang disket yang akan digunakan pada komputer SDCS hendaklah dilakukan penapisan terlebih dahulu sebelum ianya boleh digunakan. *Thumb drive* hendaklah ditapis *(scan*) terlebih dahulu sebelum digunakan bersama-sama komputer SDCS.

b. Komputer yang dijangkiti oleh virus hendaklah dilaporkan segera kepada pentadbir sistem dan usaha untuk membersihkan komputer tersebut hendaklah dilaksanakan.

c. Pengguna hendaklah memaklumkan kepada pentadbir sistem jenis virus yang telah dijangkiti dan nama virus tersebut hendaklah dicatatkan untuk memudahkan pentadbir sistem mendapatkan jalan penyelesaian untuk membersihkan virus tersebut.

11. Kemudahan Penggunaan Internet. Pengguna sistem adalah diperuntukkan dengan kemudahan Internet sebagai media penghantaran data melalui perisian yang dipasang. Oleh yang demikian penyalahgunaan Internet boleh memberikan kesan kepada sistem.

12. Larangan Penggunaan Internet. Pengguna Internet adalah sama sekali dilarang melakukan perkara-perkara berikut :

a. Menghantar, menyimpan atau mengetahui penerimaan sebarang bahan yang menyalahi undang-undang.

b. Menyalin atau memuat turun program atau perisian yang tidak dikenali yang boleh memudaratkan sistem.

c. Menghantar mesej yang mengandungi maklumat yang tidak benar, berbentuk hasutan, fitnah dan ancaman yang boleh menjatuhkan imej mana-mana pihak.

d. Menggunakan perkhidmatan *chatting* melalui Internet.

e. Menjalankan aktiviti-aktiviti politik dan sebarang bentuk perniagaan.

f. Memuat turun atau melayari laman-laman web yang tidak sihat seperti laman wab lucah dan yang seumpamanya.

g. Penggunaan Internet adalah dibenarkan untuk tujuan penyelidikan, pengumpulan maklumat dan pengendalian urusan rasmi sahaja.

h. Pentadbir sistem berkeupayaan untuk mengesan pengguna yang melayari laman web yang tidak sepatutnya dilayari dan berhak untuk memaklumkan perkara berkenaan kepada pihak yang bertanggungjawab.

TATACARA PENGGUNAAN SECURED SOFT MAIL

13. *Secured Soft Mail* adalah merupakan perisian aplikasi yang membolehkan pengguna membuat capaian komunikasi antara dua pihak atau lebih dalam bentuk *data encryption*. Pengguna adalah dilarang sama sekali menghantar mesej atau data menggunakan aplikasi email selain daripada S*ecured Soft Mail*. Prosedur yang perlu dipatuhi apabila ingin membuat penghantaran maklumat melalui S*ecured Soft Mail* adalah seperti berikut :

a. Pengguna hendaklah menghidupkan aplikasi *Virtual Private Network* (VPN) untuk membolehkan penghantaran data lebih selamat.

b. Segala dokumen berdarjah hendaklah dienkripkan terlebih dahulu sebelum dihantar melalui S*ecured Soft Mail*.

c. Pengguna tidak dibenarkan membiarkan pengguna lain menghantar email menggunakan akaunnya. Tindakan tatatertib akan diambil ke atas pengguna dan akaunnya akan ditamatkan serta disenaraihitamkan.

14. Pangkalan Data / Fail-fail Elektronik. Semua pangkalan data hendaklah dikategorikan sebagai bahan berdarjah dan dikawal dari sebarang capaian, perubahan dan pemusnahan yang tidak sah. Oleh demikian, adalah penting bagi pengguna mengikuti langkah-langkah berikut :

a. Pengguna boleh membuat satu fail elektronik yang baru dan menyimpan segala data atau dokumen berdarjah di dalamnya.

b. Pengguna boleh mengenkripkan segala data atau dokumen yang berdarjah rahsia menggunakan aplikasi SDCS.

c. *Encryption* tidak terhad kepada data yang hendak dihantar sahaja, malah keseluruhan komputer yang menggunakan sistem ini boleh dienkripkan menggunakan perisian SDCS.

KHIDMAT NASIHAT

15. Sebarang kemusykilan berkaitan dengan sistem atau kerosakan sistem hendaklah dirujuk atau dimaklumkan kepada pentadbir sistem melalui alamat atau email berikut :

Markas Angkatan Tentera Malaysia
Bahagian Komunikasi dan Elektronik Pertahanan
(Sel Komputer)
Wisma Pertahanan
Jalan Padang Tembak
50634 KUALA LUMPUR
(Untuk Perhatian : PS 2 Rangkaian A)

Tel : 03 – 2071 5398
Faks : 03 – 2059 8397

PENUTUP

16. Oleh kerana penggunaan komputer kini berkembang dengan pesat dan meluas di dalam ATM maka keselamatan komputer dan maklumat perlu dititikberatkan. Selain daripada langkah-langkah penggunaan yang disebutkan di atas setiap pengguna perlu mendisiplinkan diri bagi menentukan tiada maklumat penting dikeluarkan atau jatuh ke tangan pihak yang tidak bertanggungjawab.

17. Penggunaan perisian SDCS ini diharapkan dapat meningkatkan tahap kerahsiaan sesuatu dokumen atau data semasa penghantaran maklumat melalui media Internet.