DASAR KESELAMATAN ICT

POLITEKNIK SEBERANG PERAI

VERSI 1.2

OKTOBER 2011

ISI KANDUNGAN

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT PSP mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di PSP.

OBJEKTIF

Dasar Keselamatan ICT PSP diwujudkan untuk menjamin kesinambungan urusan PSP dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi PSP. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT PSP ialah seperti berikut:

1. Memastikan kelancaran operasi PSP dan meminimumkan kerosakan atau kemusnahan;

2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

3. Mencegah salah guna atau kecurian aset ICT Kerajaan.

SKOP

Aset ICT PSP terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT PSP menetapkan keperluan-keperluan asas berikut:

(a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT PSP ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan PSP. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian
Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada PSP.

SKOP

(c) Perkhidmatan
Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:
i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat
Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif PSP. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod PSP, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) Manusia
Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian MAMPU bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(f) Premis Komputer Dan Komunikasi
Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

Pelaksanaan dasar ini juga adalah tertakluk kepada semua pekeliling dan arahan kerajaan berkenaan ICT yang sedang berkuatkuasa.

BIDANG 01

PENGURUSAN ASET ICT

Pengurusan Aset ICT adalah bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

1. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;

2. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;

3. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di PSP;

4. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan

5. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

BIDANG 02

KESELAMATAN PERALATAN

0201 PERALATAN ICT

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

1. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;

2. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

3. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

4. Pengguna dilarang membuat instalasi sebarang perisian tambahan;

5. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

6. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

7. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. Penggunaan login *administrator* di komputer hanya boleh digunakan oleh Unit ICT.

8. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

BIDANG 02

KESELAMATAN PERALATAN

0201 PERALATAN ICT

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

9. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);

10. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. -
    - Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci ;
    - Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;
    - Bilik peralatan rangkaian sentiasa berada dalam keadaan yang teratur dan tersusun. Dilarang meletakkan peralatan / barang selain daripada peralatan yang sedia ada.

11. Peralatan ICT yang hendak dibawa keluar dari premis PSP, perlulah mendapat kelulusan Ketua Unit/Pengarah dan direkodkan bagi tujuan pemantauan;

12. Peralatan ICT yang hilang hendaklah dilaporkan kepada Unit ICT dan Pegawai Aset dengan segera;

13. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

14. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Unit ICT;

15. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Unit ICT melalui e-Aduan untuk di baik pulih;

BIDANG 02

KESELAMATAN PERALATAN

0201 PERALATAN ICT

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

16. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

17. Alamat IP tidak boleh dikonfigurasi secara manual tanpa kebenaran Unit ICT;

18. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Unit ICT;

19. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

20. Pengguna hendaklah mematikan semua perkakasan komputer, pencetak dan pengimbas apabila meninggalkan pejabat;

21. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Unit ICT;

22. Memastikan plug dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

BIDANG 02

KESELAMATAN PERALATAN

0202 MEDIA STORAN

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

1. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
2. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
3. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
4. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
5. Akses dan pergerakan media storan yang mengandungi data kritikal hendaklah direkodkan;
6. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;
7. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
8. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
9. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

BIDANG 02

KESELAMATAN PERALATAN

0203 MEDIA PERISIAN DAN APLIKASI

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

1. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan PSP;

2. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Ketua Jabatan/Pengarah;

Perkara-perkara yang perlu dipatuhi oleh Unit ICT adalah seperti berikut:

1. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak;

2. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang tertentu.

BIDANG 02

KESELAMATAN PERALATAN

0204 PENYELENGGARAAN PERKAKASAN

Perkakasan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Perkara-perkara yang perlu dipatuhi oleh Unit ICT dan Pegawai Aset adalah seperti berikut:

1. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar;

2. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

3. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

4. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;

5. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan;

6. Semua penyelenggaraan mestilah mendapat kebenaran daripada Unit ICT.

BIDANG 02

KESELAMATAN PERALATAN

0205 PERALATAN DI LUAR PREMIS

Perkakasan yang dibawa keluar dari premis PSP adalah terdedah kepada pelbagai risiko.

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

1. Peralatan perlu dilindungi dan dikawal sepanjang masa;

2. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

0206 PELUPUSAN PERKAKASAN

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh PSP dan ditempatkan di PSP. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PSP.

Perkara-perkara yang perlu dipatuhi oleh Unit ICT dan Pegawai Aset adalah seperti berikut:

1. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

2. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

3. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

BIDANG 02

KESELAMATAN PERALATAN

0206 PELUPUSAN PERKAKASAN

4. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

5. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

6. Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori;

7. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;

Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

1. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

2. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan sebagainya;

3. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di PSP;

4. Memindah keluar dari PSP mana-mana peralatan ICT yang hendak dilupuskan;

BIDANG 02

KESELAMATAN PERALATAN

0206 PELUPUSAN PERKAKASAN

5. Melupuskan sendiri peralatan ICT;

6. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

BIDANG 03

PENGURUSAN MEL ELEKTRONIK (E-MAIL)

Penggunaan e-mel di PSP hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

1. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh PSP sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

2. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh PSP;

3. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

4. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

5. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

BIDANG 03

PENGURUSAN MEL ELEKTRONIK (E-MAIL)

6. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

7. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

8. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail yang telah ditetapkan;

9. E-mel yang tidak penting, tidak mempunyai nilai arkib, yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

10. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

11. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

12. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan

13. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

BIDANG 04

KAWALAN CAPAIAN

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara-perkara yang perlu diambil kira adalah seperti berikut:

1. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;

2. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

3. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih;

4. Kawalan ke atas kemudahan pemprosesan maklumat.

0401 PENGURUSAN CAPAIAN PENGGUNA

040101 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

1. Akaun yang diperuntukkan oleh PSP sahaja boleh digunakan;

2. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

BIDANG 04

KAWALAN CAPAIAN

0401 PENGURUSAN CAPAIAN PENGGUNA

040101 Akaun Pengguna

3. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;

4. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan PSP. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

5. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan

6. Unit ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:
   - Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu;
   - Bertukar bidang tugas kerja;
   - Bertukar ke agensi lain;
   - Bersara; atau
   - Ditamatkan perkhidmatan.

040102 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

BIDANG 04

KAWALAN CAPAIAN

0401 PENGURUSAN CAPAIAN PENGGUNA

040103 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PSP seperti berikut:

1. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

2. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

3. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus;

4. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

5. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

6. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

7. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;

8. Kata laluan hendaklah berlainan daripada pengenalan identity pengguna;

9. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;

BIDANG 04

KAWALAN CAPAIAN

0401 PENGURUSAN CAPAIAN PENGGUNA

040103 Pengurusan Kata Laluan

10. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian;

11. Mengelakkan penggunaan semula kata laluan yang baru digunakan.

040104 *Clear Desk* dan *Clear Screen*

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:

1. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;

2. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

3. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.

BIDANG 04

KAWALAN CAPAIAN

0402 KAWALAN CAPAIAN RANGKAIAN

040201 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

1. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian PSP, rangkaian agensi lain dan rangkaian awam;

2. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan

3. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

040202 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Penggunaan Internet di PSP hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PSP;

2. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

3. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;

BIDANG 04

KAWALAN CAPAIAN

040202 Capaian Internet

4. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Unit ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

5. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa;

6. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

7. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah sebelum dimuat naik ke Internet;

8. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

9. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PSP;

10. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

11. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali;

BIDANG 04

KAWALAN CAPAIAN

040202 Capaian Internet

12. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:
    - Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan
    - Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

13. Penggunaan peralatan ICT mudah alih milik peribadi bagi tujuan capaian internet menggunakan rangkaian PSP hanya dibenarkan bagi tujuan rasmi sahaja. Pemilik perlu memastikan peralatan berkenaan adalah bebas daripada ancaman virus dan sebagainya.

0403 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

040301 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer.

Kemudahan ini juga perlu bagi:

(a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan

(b) Merekodkan capaian yang berjaya dan gagal.

BIDANG 04

KAWALAN CAPAIAN

040301 Capaian Sistem Pengoperasian

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

(a) Mengesahkan pengguna yang dibenarkan;

(b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan

(c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;

(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;

(c) Mengehadkan dan mengawal penggunaan program; dan

(d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

BIDANG 04

KAWALAN CAPAIAN

040302 Kad Pintar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;

(b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;

(c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan

(d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Unit ICT.

BIDANG 04

KAWALAN CAPAIAN

0404 KAWALAN CAPAIAN APPLIKASI DAN MAKLUMAT

040401 Capaian Applikasi dan Maklumat

Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkaraperkara berikut hendaklah dipatuhi:

(a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;

(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);

(c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

(d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan

(e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

BIDANG 05

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Unit ICT dengan kadar segera:

1. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;

2. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

3. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

4. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

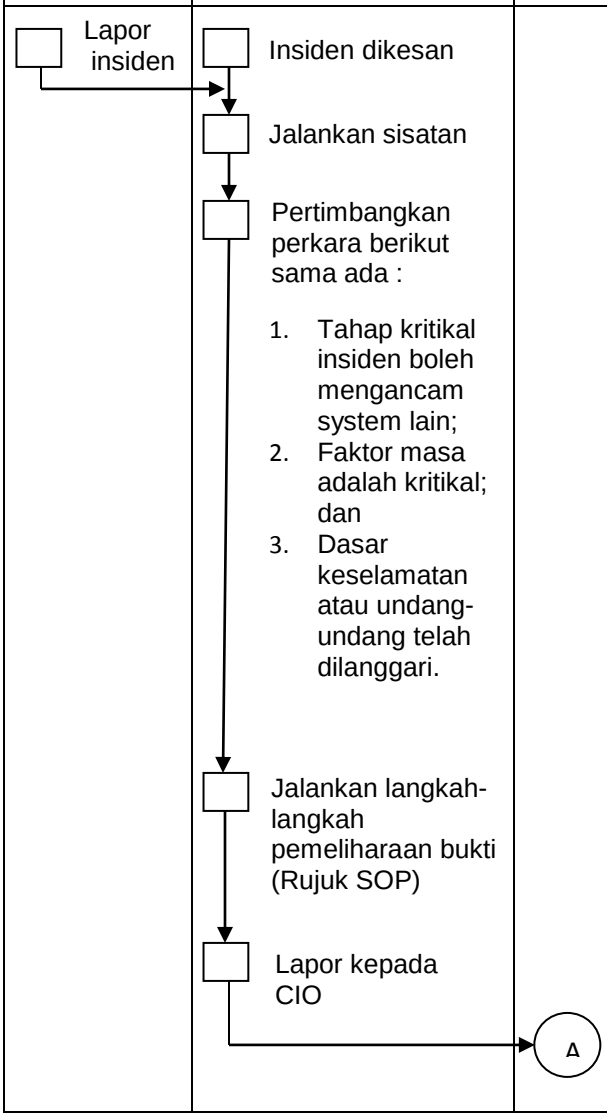
5. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

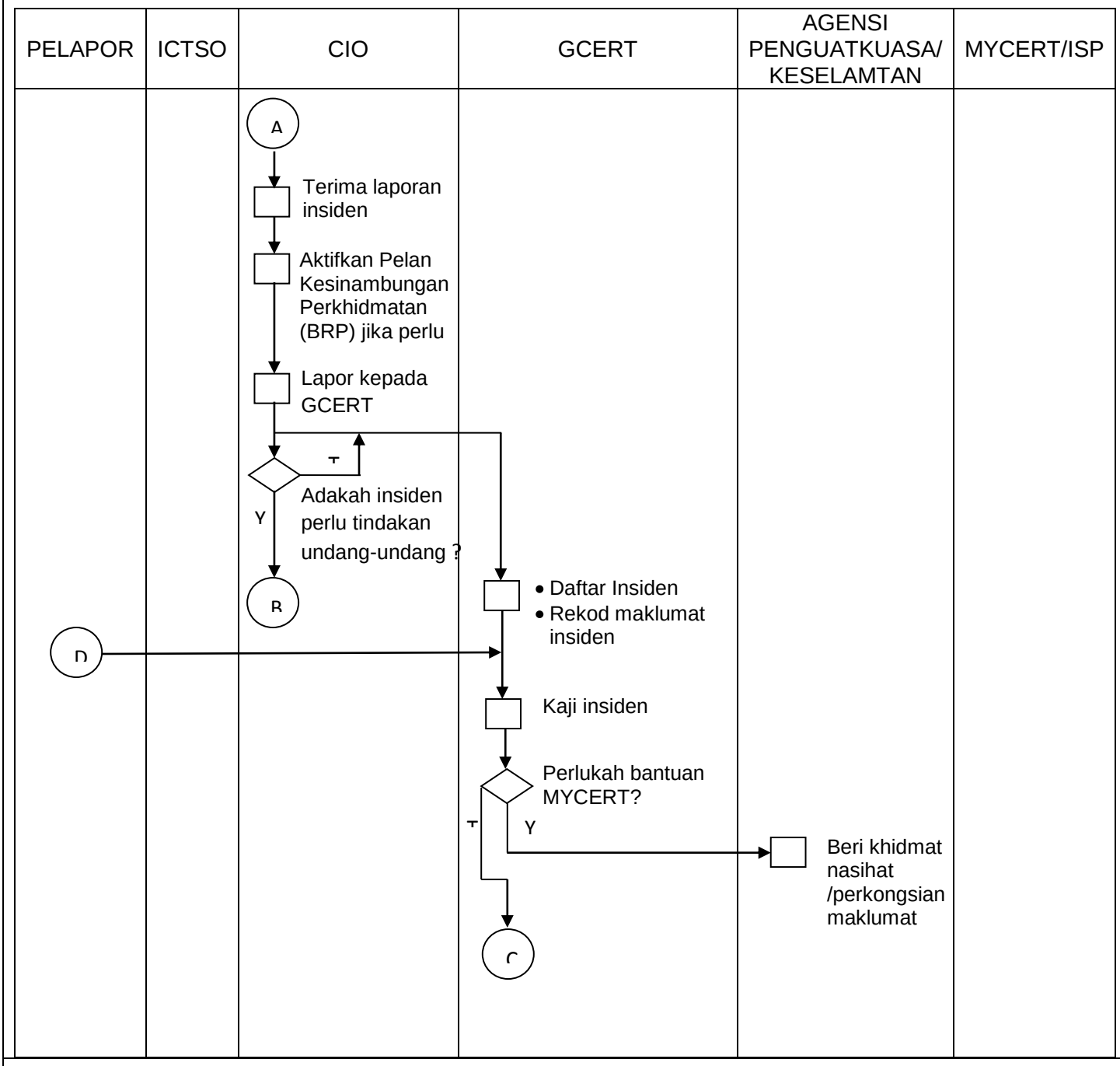
Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di PSP sepertimana **Lampiran 1**.

LAMPIRAN 1

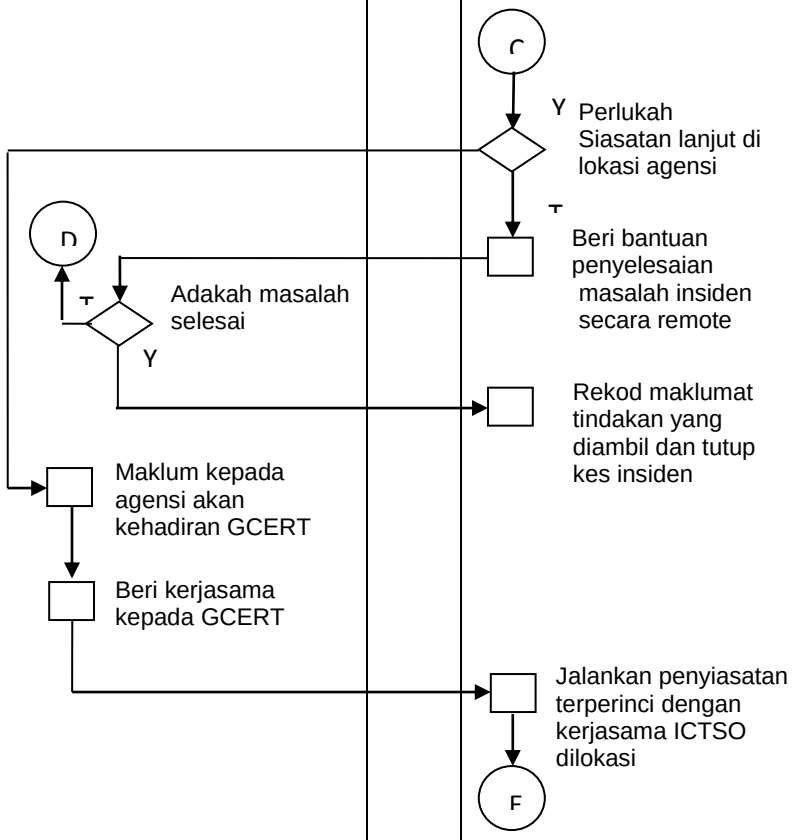
DASAR KESELAMATAN ICT PSP

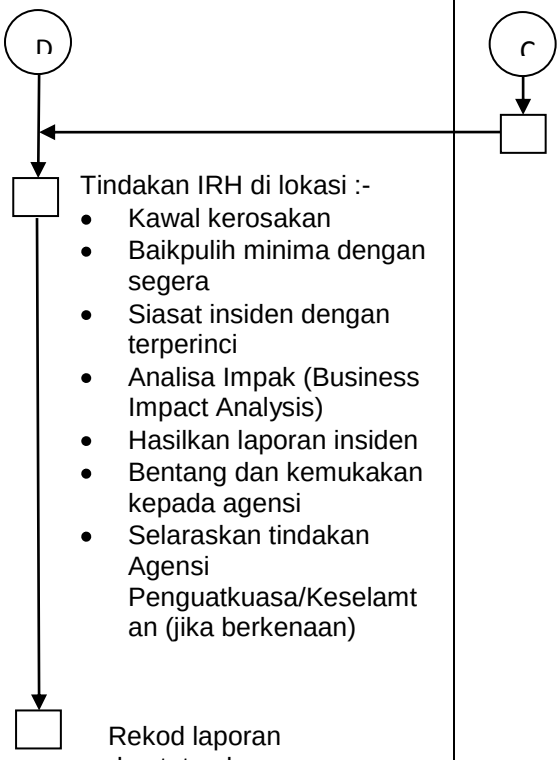
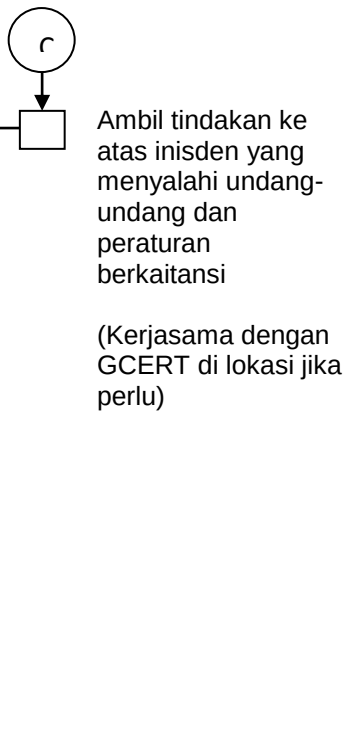
Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT PSP




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMTAN
MYCERT/ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Adakah insiden perlu tindakan undang-undang ?
Y
B
D
Daftar Insiden
Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MYCERT?
T
Y
Beri khidmat nasihat /perkongsian maklumat
C

PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUATKUASA/ KESELAMTAN	MYCERT/ ISP



PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUATKUASA/ KESELAMTAN	MYCERT/ ISP
					

Penunjuk :
SOP – *Standard Operating Procedure*

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT PSP	1.0	12/2010	33/33

Rujukan :
Dasar Keselamatan ICT, MAMPU versi 5.2