








DASAR KESELAMATAN ICT

JABATAN PERHUTANAN SEMENANJUNG MALAYSIA

MAKLUMAT DOKUMEN

Dokumen:	Dasar Keselamatan ICT
Versi:	Versi 3.0
Tarikh Berkuatkuasa:	Jun 2015
Pemilik Dokumen:	Bahagian Pengurusan Maklumat, Jabatan Perhutanan Semenanjung Malaysia

SEJARAH SEMAKAN DAN PINDAAN MAKLUMAT DOKUMEN

Versi	Tarikh	Pindaan Yang Dilakukan
1.0	Mac 2012	Terbitan Pertama
2.0	Ogos 2013	Terbitan DKICT 2.0 Kajian Semula Keseluruhan DKICT JPSM
3.0	Jun 2015	Terbitan DKICT 3.0 -Pengemaskinian Dokumen Disebabkan Perubahan Standard ISO/IEC 27001:2013 -Mengemaskini 6.9 Pertukaran Maklumat -Menambah 8.5 Kawalan Keselamatan Kriptography -Mengemaskini 1.6 Semak dan Pindaan

DASAR KESELAMATAN ICT

JABATAN PERHUTANAN SEMENANJUNG MALAYSIA

KANDUNGAN

DASAR KESELAMATAN

1. DASAR KESELAMATAN

Dasar Keselamatan ICT JPSM adalah hak milik JPSM yang bertujuan memastikan hala tuju pengurusan aset dan keselamatan ICT selaras dengan peruntukan undang-undang. Pelaksanaan dasar-dasar perlindungan ke atas kerahsiaan, integriti dan kebolehsediaan data/ maklumat adalah untuk menjamin kesinambungan urusan serta perkhidmatan dengan meminimumkan kesan insiden keselamatan.

1.1 Tujuan

Dasar Keselamatan ICT JPSM bertujuan menjamin kesinambungan operasi berasaskan rukun kerahsiaan, integriti dan kebolehsediaan seperti berikut :

a) Kerahsiaan bermaksud melindungi kepentingan semua pihak berkaitan keselamatan aset ICT;

b) Integriti bermaksud memastikan sebarang perubahan ke atas aset ICT dilakukan oleh pihak yang dibenarkan sahaja; dan

c) Kebolehsediaan bermaksud aset ICT hendaklah boleh diguna bila diperlukan melalui kelancaran operasi JPSM dan meminimumkan gangguan, kerosakan atau kemusnahan ke atas aset ICT.

1.2 Pendahuluan

Jabatan Perhutanan Semenanjung Malaysia (JPSM) bertanggungjawab memastikan keselamatan aset teknologi maklumat dan komunikasi (ICT) termasuk data/ maklumat, perkakasan, perisian dan rangkaian yang dimiliki atau yang dikawalselia adalah bebas daripada ancaman dan risiko yang tidak boleh diterima.

1.3 Skop

Semua pihak yang menggunakan aset ICT JPSM adalah bertanggungjawab ke atas perkara berikut :

a) Data / maklumat hendaklah boleh dicapai secara berterusan dengan cepat, tepat, mudah dan dengan cara yang diyakini selamat bagi membolehkan keputusan, operasi harian dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

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

Demi memastikan keselamatan berterusan, adalah penting jaminan perlindungan merangkumi perkara-perkara berikut :

a) Data / Maklumat – Dokumentasi dan rekod berkaitan organisasi, sistem, prosedur, pelanggan dan lain-lain;
b) Perkakasan – Aset ICT yang digunakan untuk merekod, memproses dan menyimpan data / maklumat;
c) Perisian – Semua perisian termasuk perisian aplikasi, perisian utiliti, perisian sistem, sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian dan perisian automasi pejabat;
d) Rangkaian – Perkhidmatan yang menghubungkan capaian data / maklumat;
e) Premis – Penempatan kemudahan ICT; dan
f) Manusia – Individu atau kumpulan yang mempunyai pengetahuan dan kemahiran untuk mengendalikan ICT bagi mencapai objektif organisasi.

1.4 Prinsip

Prinsip Dasar Keselamatan ICT JPSM adalah seperti berikut:

a) Capaian Atas Dasar Perlu Tahu

Capaian dibenarkan dan dihadkan kepada pengguna tertentu atas dasar "perlu tahu" berdasarkan klasifikasi maklumat dan tahap tapisan keselamatan pengguna.

b) Hak Capaian Minimum

Hak capaian kepada pengguna dimulai pada tahap yang paling minimum. Kelulusan adalah perlu bagi membolehkan capaian pada tahap yang lebih tinggi.

c) Akauntabiliti

Setiap pengguna adalah bertanggungjawab ke atas semua tindakan terhadap kemudahan ICT JPSM yang disediakan. Tanggungjawab pengguna termasuk perkara berikut :

i. Menghalang pendedahan maklumat kepada pihak yang tidak

dibenarkan;

ii. Memeriksa maklumat dan menentukan ianya sentiasa tepat dan lengkap;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan maklumat; dan

v. Mematuhi langkah dan garis panduan keselamatan yang ditetapkan.

d) Pengasingan

Setiap tugasan, proses dan persekitaran pelaksanaan ICT hendaklah dipisah dan diasingkan sebaik mungkin untuk mengekalkan integriti dan perlindungan keselamatan daripada kesilapan dan penyalahgunaan. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut :

i. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan dan pengujian;

ii. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden atau keadaan yang mengancam keselamatan. Pengauditan adalah penting dalam menjamin akauntabiliti seperti berikut :

i. Mengesan pematuhan atau perlanggaran keselamatan;

ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya perlanggaran keselamatan; dan

iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya perlanggaran keselamatan.

f) Pematuhan

Prinsip ini penting untuk mengelak pelanggaran Dasar melalui tindakan berikut :

i. Mewujudkan proses yang sistematik khususnya dalam menjamin

keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;

ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;

iii. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan

iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

g) Pemulihan

Pemulihan adalah untuk memastikan kebolehsediaan dan kebolehcapaian dengan meminimumkan gangguan atau kerugian akibat daripadanya adalah seperti berikut :

i. Merancang dan menguji Pelan Pemulihan Bencana – (Disaster Recovery Plan); dan

ii. Melaksanakan amalan terbaik dalam pelaksanaan ICT.

h) Saling Bergantung

Prinsip keselamatan adalah saling lengkap-melengkapi dan hendaklah dipatuhi bagi jaminan keselamatan yang berkesan. Tindakan mempelbagaikan pendekatan dalam menyusun strategi mekanisme keselamatan mampu meningkatkan tahap keselamatan.

1.5 Pemakaian

Dasar Keselamatan ICT JPSM adalah terpakai kepada semua pengguna aset ICT termasuk pembekal dan pakar runding yang berurusan dengan JPSM.

1.6 Semakan Dan Pindaan

Dasar Keselamatan ICT JPSM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Setiap perubahan hendaklah

mendapat pengesahan ICTSO. Perubahan yang melibatkan penambahan atau pemansuhan yang memberi impak ke atas keselamatan adalah di anggap perubahan utama dan hendaklah mendapat pengesahan JPICT.

Prosedur penyelenggaraan Dasar Keselamatan ICT JPSM adalah seperti berikut :

a) Menyemak dasar ini dua kali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan;
b) Mengemukakan cadangan pindaan atau perubahan secara bertulis; dan
c) Memaklumkan pindaan atau perubahan dasar yang telah dipersetujui kepada semua pengguna.

PENGURUSAN KESELAMATAN ICT

2. PENGURUSAN KESELAMATAN ICT

Objektif :

Memastikan rangka kerja diwujudkan bagi menjamin pelaksanaan pengurusan keselamatan ICT yang sistematik dan berkesan.

2.1 Struktur Pengurusan Keselamatan ICT JPSM

Struktur organisasi formal diwujudkan untuk mengurus keselamatan ICT JPSM melalui Jawatankuasa Pemandu ICT (JPICT) JPSM dan mematuhi termasuk yang berikut :

a. Komitmen pengurusan atasan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus;

b. Tanggungjawab yang jelas dan jalinan komunikasi dengan semua pengguna dalam pengurusan keselamatan ICT;

c. Memastikan kerahsiaan maklumat sentiasa terkawal;

d. Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan; dan

e. Memastikan keperluan sumber bagi keselamatan ICT JPSM adalah mencukupi.

2.2 Jawatankuasa Teknikal Dan Keselamatan ICT

Peranan dan tanggungjawab ahli Jawatankuasa Teknikal dan Keselamatan ICT JPSM adalah seperti berikut :

a) Pengurus ICT (*ICT Manager*)

i. Membantu Ketua Pegawai Maklumat (*CIO*) dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;

ii. Menentukan keperluan dan bertanggungjawab ke atas perkara-perkara berkaitan dengan keselamatan ICT JPSM; dan

iii. Membangun dan menyelaras pelaksanaan program kesedaran dan latihan keselamatan ICT.

b) Pegawai Keselamatan ICT (ICTSO - *ICT Security Officer*)

i. Merancang, melaksana, mengurus dan memantau program keselamatan ICT JPSM;

ii. Menguatkuasakan Dasar Keselamatan ICT JPSM;

iii. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JPSM

iv. Memberikan penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JPSM kepada pengguna;

v. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT JPSM;

vi. Melaksanakan pengurusan risiko keselamatan ICT;

vii. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

viii. Memberikan amaran kepada JPN terhadap kemungkinan berlakunya ancaman keselamatan ICT seperti virus dan penggodam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah perlindungan yang bersesuaian;

ix. Melaporkan insiden keselamatan ICT kepada CERT NRE;

x. Memastikan penyimpanan rekod, bahan bukti dan laporan ancaman atau insiden keselamatan ICT JPSM dilaksanakan dengan berkesan.

xi. Bekerjasama dengan semua pihak yang berkaitan dalam menangani ancaman atau insiden keselamatan ICT dan memperakukan langkah penyelesaian atau pencegahan; dan

xii. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JPSM.

c) Pentadbir Sistem ICT

i. Menjaga kerahsiaan maklumat keselamatan ICT;

ii. Mengambil tindakan segera apabila dimaklumkan mengenai sebarang perubahan pengguna dalaman / luaran / asing berkaitan pengurusan ICT;

iii. Menentukan pelaksanaan tahap capaian kemudahan ICT adalah bertepatan dengan arahan pemilik maklumat;

iv. Memantau dan menyediakan laporan aktiviti penggunaan dan capaian pengguna;

v. Mengenal pasti dan melaporkan aktiviti tidak normal berkaitan

vi. ICT kepada Pengurus ICT; dan

vii. Menyimpan dan menganalisis rekod jejak audit.

2.3 Penasihat Undang-Undang

a) Menyediakan khidmat nasihat perundangan bagi memastikan aktiviti ICT JPSM dapat dijalankan sepenuhnya berdasarkan undang-undang dan peraturan yang berkuat kuasa;

b) Menyediakan khidmat nasihat perundangan bagi melindungi aset, sumber dan warga JPSM terhadap pelbagai risiko perundangan;

c) Memberi khidmat nasihat dan bantuan perundangan dalam pengurusan kontrak termasuk urusan penyediaan, kajian semula, penyelesaian pertikaian, melaksanakan tindakan perundangan ke atas pihak yang berkenaan dan menyelaras urusan tindakan perundangan ke atas JPSM (sekiranya ada);

2.4 Pengurus Sumber Manusia

Memaklumkan sebarang pengambilan, pertukaran, perpindahan, persaraan dan / atau penamatan perkhidmatan kakitangan kepada pentadbir sistem ICT;

2.5 Pengguna Dalaman

a) Mematuhi dan melaksanakan Dasar Keselamatan ICT JPSM;

b) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;

c) Mengikuti dan menghayati program kesedaran keselamatan ICT; dan

d) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Bahagian Pengurusan Maklumat JPSM.

2.6 Pengguna Luaran, Pembekal Dan Pakar Runding

a) Menandatangani akuan pematuhan Dasar Keselamatan ICT JPSM atau lain-lain dokumen atau borang yang berkaitan;

b) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Bahagian Pengurusan Maklumat JPSM; dan

c) Mendapatkan kelulusan untuk menggunakan kemudahan ICT JPSM.

PENGURUSAN ASET

3. PENGURUSAN ASET

Objektif :

Memastikan setiap aset hendaklah dikenal pasti, dikelas, direkod dan diselenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

3.1 Pengurusan Aset

Semua aset ICT di JPSM mestilah diuruskan mengikut tatacara yang telah ditetapkan dalam Pekeliling Perbendaharaan Bil. 5 Tahun 2007 - Tatacara Pengurusan Aset Alih Kerajaan. Setiap aset ICT hendaklah didaftarkan dalam Sistem Pengurusan Aset (SPA). Ketua Jabatan atau Pengarah Bahagian / Ketua Unit adalah bertanggungjawab mengenalpasti pemilik aset ICT tersebut. Setiap pegawai adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset ICT di bawah tanggungannya.

Aset ICT didefinisikan sebagai semua yang mempunyai nilai kepada agensi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan juga sumber manusia.

3.2 Tanggungjawab Pengurus Aset

Semua aset ICT yang dimiliki atau digunakan oleh setiap Bahagian / Unit hendaklah diberikan kawalan dan tahap perlindungan yang sesuai oleh Pengarah Bahagian / Ketua Unit mengikut peraturan yang berkuat kuasa seperti berikut :

a) Pemilik aset hendaklah menentukan tahap sensitiviti (terperingkat) yang bersesuaian bagi setiap maklumat aset di JPSM. Pemilik aset juga hendaklah membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut. Pemilik aset hendaklah mematuhi *Information Classification and Handling Guideline* dengan sewajarnya;

b) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya, kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset; dan

c) Semua pengguna aset ICT di JPSM mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. Pengguna adalah terdiri daripada kakitangan JPSM (lantikan tetap, kontrak dan sambilan), konsultan, kontraktor atau pihak ketiga yang terlibat secara langsung.

3.3 Pengelasan, Pelabelan dan Pengendalian Maklumat

a) Pengelasan maklumat

Pengelasan maklumat bertujuan memastikan setiap maklumat diberi perlindungan oleh pemilik aset untuk menentukan keperluan, keutamaan dan tahap keselamatan berdasarkan peraturan yang berkuatkuasa seperti berikut:

i. Rahsia Besar;
ii. Rahsia;
iii. Sulit;
iv. Terhad; dan
v. Terbuka.

b) Pelabelan dan Pengendalian Maklumat

Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 3.3 (a).

Aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran (sama ada dari segi lisan, pos, faksimile dan mel elektronik) dan pemusnahan maklumat mestilah mengikut standard,

prosedur, langkah dan garis panduan keselamatan yang ditetapkan dalam Buku Arahan Keselamatan.

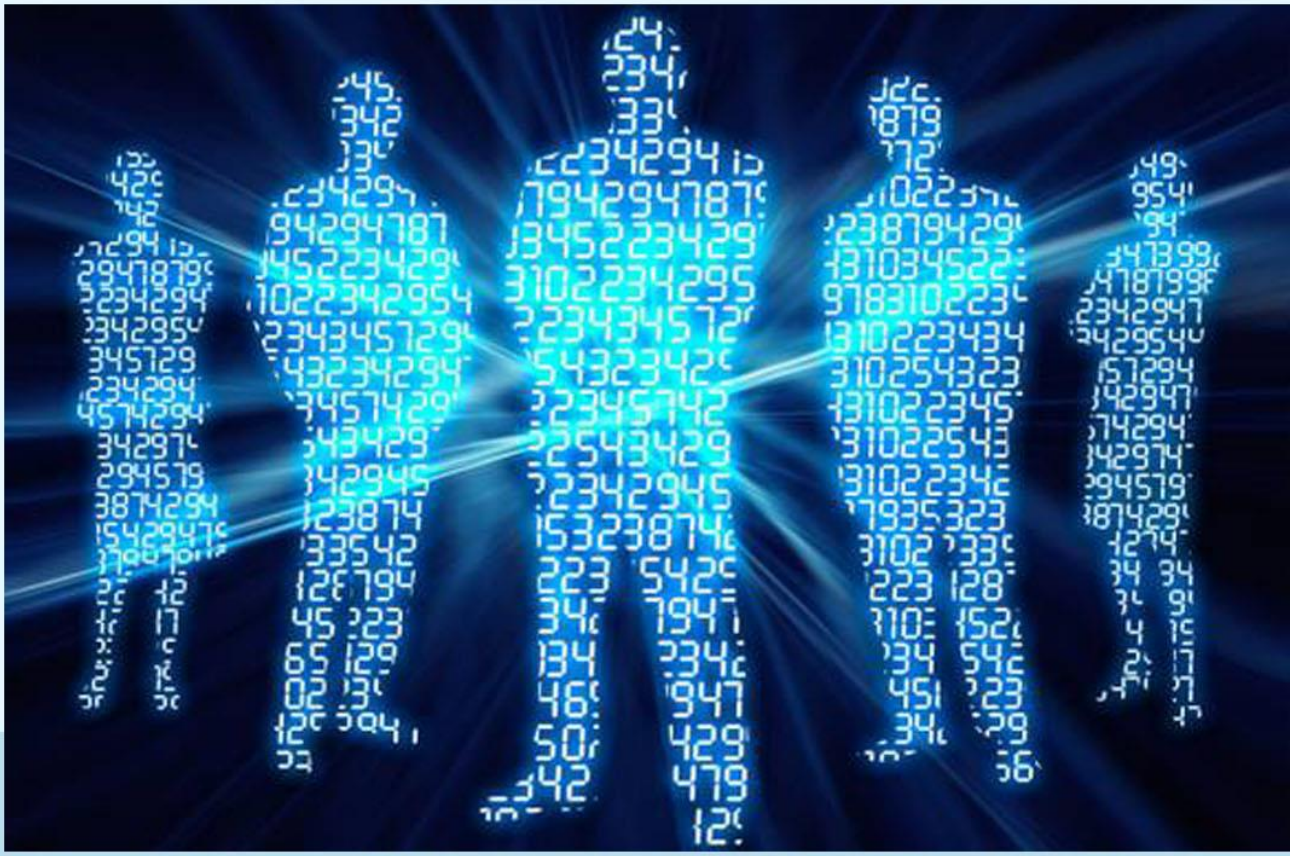
Maklumat yang diklasifikasikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad perlu dilindungi daripada didedahkan kepada pihak ketiga atau awam. Pihak ketiga jika perlu boleh diberi kebenaran capaian maklumat JPSM atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran pemilik aset atau pentadbir sistem.

3.4 Akauntabiliti Terhadap Aset ICT

Senarai maklumat aset di JPSM hendaklah diwujudkan. Setiap aset perlu ditentukan dengan jelas dan pemilikan aset mestilah dipersetujui dan didokumenkan berserta lokasi semasa aset tersebut. Senarai aset hendaklah disimpan oleh Ketua Jabatan atau Pengarah Bahagian / Ketua Unit.

Rekod aset di JPSM adalah terdiri daripada kategori yang berikut :

a) Data atau maklumat – dokumentasi sistem, panduan pengguna, maklumat yang telah diarkibkan, pangkalan data, fail-fail data, bahan pembelajaran / latihan, prosedur operasi dan sokongan;
b) Sumber manusia – semua warga JPSM;
c) Perisian – semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi perisian sistem, perisian utiliti, perisian rangkaian, sistem aplikasi, pangkalan data; dan
d) Perkakasan ICT – semua perkakasan komputer seperti komputer peribadi, pelayan, pencetak, pengimbas, *plotter* dan lain-lain perkakasan ICT.



PENGURUSAN SUMBER MANUSIA

4. PENGURUSAN SUMBER MANUSIA

Objektif :

Memastikan semua pihak yang terlibat dalam pengurusan dan penggunaan ICT hendaklah bertanggungjawab dan memahami peranan masing-masing mengikut peraturan berkaitan keselamatan ICT yang berkuat kuasa.

4.1 Sebelum Berkhidmat

Semua pihak terlibat di dalam pengurusan dan / atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut :

a) Melaksanakan peranan dan tanggungjawab dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;

b) Menjalankan tapisan keselamatan selaras dengan keperluan perkhidmatan mengikut peraturan sedia ada; dan

c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.

4.2 Dalam Perkhidmatan

Semua pihak yang terlibat dalam pengurusan dan / atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut :

a) Mengurus keselamatan aset ICT yang dibenarkan mengikut peraturan yang ditetapkan;

b) Memastikan tindakan disiplin dan / atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan;

c) Memastikan tanggungjawab dan peranan dalam pengurusan keselamatan ICT dinyatakan dalam senarai tugas; dan

d) Mengikuti program kesedaran keselamatan ICT berdasarkan

keperluan;

4.3 Keselamatan ICT Dalam Senarai Tugas

Peranan dan tanggungjawab dalam keselamatan ICT hendaklah didokumenkan di dalam senarai tugas.

Senarai tugas mesti mengandungi perkara berikut :

a) Tanggungjawab kakitangan;
b) Hubungan dengan pegawai atasan; dan
c) Tanggungjawab kakitangan dalam keselamatan ICT.

4.4 Bertukar atau Tamat Perkhidmatan

Semua pihak yang telah terlibat dalam pengurusan dan / atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut :

a) Memastikan semua aset ICT dikembalikan kepada JPSM mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; dan
b) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.

KESELAMATAN FIZIKAL & PERSEKITARAN

5. KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif :

Memastikan premis dan kemudahan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang ancaman fizikal dan persekitaran.

5.1 Tanggungjawab Keselamatan Fizikal dan Persekitaran

Ketua Jabatan adalah bertanggungjawab untuk melaksanakan langkah-langkah keselamatan yang perlu bagi mengesan, mencegah dan menghalang pencerobohan ke atas premis dan kawasan yang menempatkan kemudahan ICT berdasarkan peraturan yang berkuatkuasa.

5.2 Kawalan Kawasan Terperingkat

Kawasan terperingkat adalah premis yang dilengkapi dengan sistem keluar masuk.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
b) Melindungi kawasan terhad melalui kawalan keluar masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
c) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk semua yang bekerja di dalam kawasan terhad;
d) Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya;
e) Pusat Data yang tiada pengawal (*unmanned*) mestilah dikunci. Kakitangan sokongan teknikal dari pihak ketiga hanya dibenarkan memasuki Pusat Data sekiranya perlu dan kehadiran mereka mestilah direkodkan, disahkan, diiringi dan diawasi oleh pentadbir sistem;

f) Aktiviti mengambil gambar, merakam video, merekod suara atau penggunaan peralatan yang seumpamanya tidak dibenarkan di dalam Pusat Data kecuali dengan kebenaran ICTSO; dan

g) Individu yang tidak mempunyai pengenalan diri, pengenalan diri terlindung atau gagal mengemukakan pengenalan diri yang sah perlu diiringi ke kaunter khidmat pelanggan dengan segera.

5.3 Keselamatan Peralatan

Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian atau kompromi ke atas aset ICT dan gangguan ke atas sistem penyampaian agensi.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Perkakasan

i. Menempatkan dan mengawal peralatan ICT supaya risiko ancaman dan bencana dari persekitaran serta percubaan menceroboh oleh pihak yang tidak diberi kebenaran dapat dikurangkan; dan
ii. Semua cadangan pengubahsuaian, pembelian, penempatan dan pemindahan peralatan-peralatan ICT hendaklah dirujuk terlebih dahulu kepada Pengurus ICT.

b) Dokumen

i. Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi :
ii. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
iii. Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen; dan
iv. Satu sistem pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan dan menghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat;

c) Media Storan (cakera keras, *CD-ROM, DVD-ROM, thumb drive* dan media storan lain). Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Langkah-langkah pencegahan yang perlu diambil adalah seperti berikut :

i. Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
ii. Mengehadkan capaian kepada pengguna yang dibenarkan sahaja;
iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan; dan
iv. Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup* / *restore*.

5.4 Prasarana Sokongan

a) Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan perolehan dan pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pihak-pihak yang berkaitan.

Perkara yang perlu dipatuhi adalah seperti berikut :

i. Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat;
ii. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
iii. Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
iv. Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT;
v. Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT khususnya di dalam Pusat Data;
vi. Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;
vii. Menyemak dan menguji semua peralatan perlindungan sekurang kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian perlu direkodkan bagi tujuan rujukan dan tindakan;

viii. Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti bomba, JKR dan sebagainya; dan

ix. Melengkapkan premis dengan sistem penggera kebakaran automatik. Pemasangan sistem pengesan kebakaran perlu mendapat kelulusan pihak berkuasa tempatan serta perlu diperiksa dan diselenggara secara berkala sekurang-kurangnya sekali setahun. Alat pemadam api mudah alih perlu diletakkan di tempat yang strategik dan tidak terlindung. Langkah-langkah penggunaan peralatan juga perlu dipaparkan.

b) Bekalan Kuasa

i. Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dengan menyalurkan bekalan kuasa yang bersesuaian;

ii. Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan

iii. Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

c) Prosedur Kecemasan

i. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan JPSM;

ii. Melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan JPSM;

iii. Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa.

d) Keselamatan Rangkaian

i. Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan.

ii. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut :

iii. Melabel dan menggunakan kabel mengikut spesifikasi yang telah ditetapkan;

iv. Melindungi kabel daripada kerosakan;

5.5 Penyelenggaraan Peralatan

Perkakasan hendaklah disenggarakan berdasarkan peraturan-peraturan semasa bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut :

a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;

b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

c) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; dan

d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

5.6 Peminjaman Peralatan

Peralatan yang dipinjam hendaklah mendapat kelulusan mengikut peraturan yang telah ditetapkan oleh JPSM.

Langkah-langkah perlu diambil termasuklah seperti berikut :

a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh JPSM bagi membawa keluar peralatan bagi tujuan yang dibenarkan;

b) Melindungi dan mengawal peralatan sepanjang masa;

c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan

d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.

5.7 Pengendalian Peralatan Luar Yang Dibawa Masuk / Keluar

Langkah keselamatan yang perlu diambil dalam mengendalikan peralatan luar yang dibawa masuk / keluar adalah seperti berikut :

a) Memastikan peralatan yang dibawa masuk / keluar tidak mengancam keselamatan ICT JPSM; dan

b) Mendapatkan kelulusan agensi mengikut peraturan yang telah ditetapkan.

5.8 Pelupusan Peralatan

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Kerajaan.

Langkah-langkah hendaklah diambil termasuklah menghapuskan semua kandungan peralatan khususnya maklumat rahsia rasmi sebelum dilupuskan.

5.9 *Clear Desk* dan *Clear Screen*

Clear Desk bermaksud tidak mendedahkan sebarang maklumat yang sensitif di tempat kerja. Manakala *Clear Screen* bermaksud tidak memaparkan sebarang maklumat sensitif di atas skrin atau yang seumpama dengannya tanpa pengawasan.

Dasar *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat yang tersimpan di dalam media storan tidak mengalami kerosakan, kecurian dan kehilangan:

a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer. *Password screen saver* akan diaktifkan secara automatik di dalam tempoh tidak melebihi lima (5) minit;

b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

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

5.10 Melaporkan Kehilangan atau Kecurian Kad Kakitangan

Kehilangan atau kecurian kad kakitangan mestilah dilaporkan serta-merta oleh pemilik kad kepada Bahagian Khidmat Pengurusan.

PENGURUSAN OPERASI & KOMUNIKASI

6. PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif :

Memastikan kemudahan pemprosesan maklumat dan komunikasi adalah berfungsi dengan baik dan selamat.

6.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Semua prosedur operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;

b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

6.2 Pengurusan Penyampaian Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

a) Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak- pihak lain;

b) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain;

c) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan

d) Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

6.3 Perancangan dan Penerimaan Sistem

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

a) Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum;

b) Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan

c) Semua urusan penerimaan dan ujian hendaklah direkodkan dengan jelas dan teratur bagi mengurangkan risiko kegagalan sistem.

6.4 Pengurusan dan Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Perubahan atau pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Bahagian Pengurusan Maklumat terlebih dahulu;

b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Bahagian Pengurusan Maklumat;

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;

d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

6.5 Perlindungan dari *Malicious* dan *Mobile Code*

Bagi tujuan perlindungan dari *malicious* dan *mobile code*, perkara yang mesti dipatuhi adalah seperti berikut :

a) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi integriti maklumat dan perisian dari ancaman *malicious code* seperti *viruses*, *worms*, *trojan horses*, dan *logic bombs*;

b) Dalam keadaan di mana *mobile code* dibenarkan, konfigurasinya hendaklah memastikan bahawa ianya beroperasi berdasarkan kepada dasar keselamatan yang jelas dan penggunaan *mobile code* yang tidak dibenarkan adalah dilarang sama sekali;

c) Semua penggunaan perisian hendaklah mematuhi lesen perisian dan disahkan oleh Bahagian Pengurusan Maklumat. Bahagian Pengurusan Maklumat haruslah dimaklumkan jika terdapat keperluan penggunaan perisian percuma (*freeware*) untuk tugas-tugas yang berkaitan;

d) Kakitangan dilarang memuat turun sebarang fail atau perisian daripada sumber yang tidak diketahui (sama ada dari rangkaian luar atau sebarang media) melainkan telah diimbas bagi memastikan ianya bebas dari kod yang mencurigakan sebelum digunakan;

e) Penggunaan media mudah alih seperti katrij, *hard disk, thumbdrive*, CD dan DVD mestilah dikawal di dalam Pusat Data. Penggunaan media tersebut hanya dibenarkan untuk melaksanakan kerja yang berkaitan sahaja;

f) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

g) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;

h) Mengemas kini anti virus dengan *pattern* anti virus yang terkini;

i) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

j) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

k) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk

tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan

l) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

6.6 *Backup* dan *Restore*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Membuat *backup* dan *restore* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru bagi mengekalkan integriti, kesediaan dan kemudahan pemprosesan maklumat;

b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi menyimpan sekurang-kurangnya tiga (3) generasi *backup*. Kekerapan *backup* bergantung pada tahap kritikal maklumat;

c) Membuat dan menguji secara berkala sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan

d) Merekod dan menyimpan salinan *backup* di premis yang berbeza dan selamat.

6.7 Pengurusan Keselamatan Rangkaian

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

a) Memastikan perlindungan keselamatan maklumat dalam rangkaian serta infrastruktur sokongan;

b) Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan sistem dan aplikasi yang menggunakan rangkaian, termasuk maklumat yang dipindahkan melaluinya; dan

c) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenalpasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar.

6.8 Pengendalian Peralatan Penyimpanan Maklumat

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

a) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan;

b) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;

c) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;

d) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan

e) Dokumentasi sistem perlu dilindungi dari capaian yang tidak dibenarkan.

6.9 Pertukaran Maklumat

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

a) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin;

b) Kebenaran perlu diperolehi daripada pengurusan pihak atasan untuk pertukaran maklumat di antara agensi dengan pihak luar;

c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi;

d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan

e) Polisi dan prosedur penggunaan e-mel Pekeliling Ketua Pengarah Perhutanan Semenanjung Malaysia Bil 7 Tahun 2013 perlu dipatuh bagi memenuhi keperluan pengunan, langkah-langkah perlindungan dan penguatkuasan, agar pengunan e-mel terkawal dan perlindungan keselamatan yang lebih mantap dapat diwujudkan.

6.10 Pemantauan

Perkara yang mesti dipatuhi termasuk yang berikut :

a) Mengesan aktiviti pemprosesan maklumat yang tidak dibenarkan dan memastikan rekod log aktiviti tidak boleh diubahsuai dan dicapai oleh pihak yang tidak dibenarkan;

b) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

c) Prosedur untuk memantau penggunaan infrastruktur pemprosesan maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;

d) Aktiviti pentadbiran sistem perlu direkodkan;

e) Kesalahan, kesilapan dan / atau penyalahgunaan perlu direkod, dianalisis dan diambil tindakan sewajarnya; dan

f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam agensi atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.

6.11 Pengasingan Bidang Tugas

Pengarah Bahagian / Ketua Unit hendaklah memastikan pengasingan bidang tugas terutama bagi bidang tugasan yang kritikal dan sensitif seperti pemantauan aktiviti, audit trail dan pemantauan pengurusan bagi mengelakkan konflik dan pertindihan arahan.

Kawalan capaian secara logik mestilah digunakan bagi membolehkan pemisahan bidang tugas dilaksanakan dan mengikut prinsip seperti berikut :

a) Kakitangan tidak boleh mempunyai capaian untuk melakukan pengemaskinian ke atas mana-mana sistem aplikasi yang sedang beroperasi kecuali setelah mendapat kelulusan; dan

b) Pembangun Sistem tidak dibenarkan mempunyai akses rutin ke atas data, sistem atau perisian aplikasi yang beroperasi.

6.12 Pelarasan Masa Untuk Semua Sistem Bagi Pusat Data

Semua masa bagi sistem kritikal yang ditempatkan di dalam rangkaian dalaman JPSM mesti diselaraskan menggunakan titik rujukan masa dari sumber yang di tetapkan seperti menggunakan masa Domain Controller.

KAWALAN CAPAIAN

7. KAWALAN CAPAIAN

Objektif :

Mengawal capaian ke atas data, maklumat, sistem aplikasi, aset ICT dan rangkaian komunikasi ICT JPSM.

7.1 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;

b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih;

d) Kawalan ke atas kemudahan had capaian maklumat; dan

e) Pengguna perlu mematuhi amalan *clear desk* dan *clear screen*.

7.2 Kawalan Capaian Pengguna

Seksyen ini bertujuan memastikan bahawa sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.

Perkara-perkara yang perlu dipatuhi adalah termasuk :

a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;

b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;

c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan

direkodkan;

d) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan JPSM dan tindakan pengemaskinian dan / atau pembatalan hendaklah diambil atas sebab seperti berikut :

i. Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditentukan;

ii. Pengguna bertukar jawatan, tanggungjawab dan / atau bidang tugas. Pembatalan akan dilakukan di hari terakhir pertukaran tersebut berlaku (seperti yang dimaklumkan oleh pihak yang mengendalikan pengurusan sumber manusia);

iii. Pengguna yang sedang dalam prosiding dan / atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib. Pembatalan akan dilakukan serta merta apabila dimaklumkan oleh pihak yang mengendalikan pengurusan sumber manusia; dan

iv. Pengguna bertukar, berpindah, bersara dan / atau tamat perkhidmatan.

Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

7.3 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 JPSM seperti berikut :

a) Pengguna tidak seharusnya menulis atau menyimpan kata laluan tanpa encryption di atas talian. Di dalam hal ini, kata laluan haruslah dilindungi dengan menggunakan mekanisme kawalan lain seperti menyimpan kata laluan di dalam laci berkunci dan menggunakan kata laluan yang berbeza bagi capaian berbeza;

b) Pengguna adalah tidak digalakkan mengguna kata laluan yang sama bagi kegunaan sistem di JPSM mahupun sistem yang tidak terdapat di

JPSM;

c) Pengguna hendaklah tidak mendedahkan kata laluan yang diguna pakai di JPSM kepada sesiapa. Ini termasuklah ahli keluarga dan bukan ahli keluarga apabila melakukan kerja pejabat di rumah. Walau bagaimana pun, bagi ID kata laluan utama yang disimpan di dalam laci berkunci, harus diadakan satu proses mengenai tatacara memperoleh kata laluan berkenaan sekiranya berlaku ketidakhadiran pemegang kata laluan utama sewaktu ia diperlukan;

d) Pengguna haruslah menyimpan kata laluan mereka dengan selamat dan tidak dibenarkan berkongsi akaun dengan pengguna lain. Pengguna yang disahkan adalah bertanggungjawab ke atas kerahsiaan dan keselamatan kata laluan dan akaun mereka;

e) Penggunaan aplikasi seperti Remember Password adalah tidak digalakkan. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada Bahagian Pengurusan Maklumat dan tindakan menukar kesemua kata laluan perlu dilakukan;

f) Sistem pengurusan kata laluan hendaklah menekankan pilihan kata laluan yang berkualiti. Kata laluan yang berkualiti antara lainnya mempunyai ciri-ciri seperti berikut :

   i. Kata laluan haruslah mengandungi sekurang-kurangnya 8 aksara yang terdiri daripada kedua-dua abjad huruf dan bukan huruf (seperti: 0-9, a-z, ! @ # $ % ^ & * ( ) - +). Pengguna juga digalakkan untuk menggunakan kombinasi antara huruf besar dan huruf kecil (contoh: p@sSWorD);

   ii. Kata laluan admin / root bagi sistem utama haruslah mengandungi kombinasi huruf besar dan huruf kecil (contoh: a-z, A-Z);

   iii. Kata laluan yang ditentukan oleh pengguna seharusnya tidak digunakan semula. Pengguna haruslah tidak membina kata laluan yang sama atau seakan-akan serupa seperti mana yang pernah digunakan sebelum ini di tempat lain; dan

   iv. Kesukaran untuk meneka kata laluan perlulah dipraktikkan. Kata laluan adalah bukan perkataan di dalam mana-mana bahasa, dialek, loghat dan sebagainya. Kata laluan tidak seharusnya berdasarkan maklumat peribadi, nama ahli keluarga dan seumpamanya.

g) Kata laluan untuk pentadbir sistem harus ditukar sekurang-kurangnya setiap enam (6) bulan untuk ke semua sistem utama.

h) Kata laluan haruslah ditukar mengikut syarat seperti berikut:

i. Daftar masuk kali pertama bagi pengguna baru;

ii. Apabila terdapat kata laluan biasa (default) yang telah disediakan di dalam sistem atau dibekalkan oleh pihak pembekal;

iii. Setiap kali pengguna mengesyaki kata laluan telah diketahui oleh orang lain; dan

iv. Apabila hak capaian pengguna bertukar disebabkan perubahan tanggungjawab di dalam bidang tugas.

Nota : Keperluan seperti yang dinyatakan di atas adalah bergantung kepada keupayaan sistem yang digunakan.

7.4 Kawalan Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan :

a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JPSM, rangkaian agensi lain dan rangkaian awam;

b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;

c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;

d) Maklumat IP dalaman, konfigurasi dan reka bentuk dalaman setiap sistem di JPSM mesti mempunyai kawalan capaian yang terhad bagi menghalang capaian dari luar JPSM;

e) Semua rangkaian JPSM mestilah mempunyai domain logical yang dipisahkan dan dilindungi dengan menggunakan perimeter keselamatan dan mekanisme kawalan capaian tertentu;

f) Untuk membolehkan JPSM bertindak terhadap ancaman luar, semua aset ICT yang bersambung ke Internet mestilah dilindungi oleh Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS);

g) Semua rangkaian dalaman JPSM mesti melalui pusat kawalan capaian tertentu (contohnya firewall) sebelum pengguna mencapai sistem JPSM;

h) Semua firewall yang digunakan untuk melindungi rangkaian dalaman JPSM mesti beroperasi di dalam sistem yang tersendiri dan tidak boleh mempunyai operasi sistem selainnya;

i) Memastikan maklumat berkaitan reka bentuk dan konfigurasi sistem rangkaian JPSM hanya terhad kepada pihak yang dibenarkan sahaja; dan

j) Penggunaan Wireless Access Point adalah tidak dibenarkan kecuali mendapat kebenaran daripada Bahagian Pengurusan Maklumat.

7.5 Kawalan Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut :

a) Mengesahkan pengguna yang dibenarkan;

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

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

d) Menyediakan kaedah yang sesuai untuk pengesahan capaian (authentication); dan

e) Menghadkan tempoh penggunaan mengikut kesesuaian.

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) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi;

d) Menamatkan sesuatu sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan

e) Menghadkan tempoh sambungan ke sesuatu aplikasi berisiko tinggi.

7.6 Kawalan Capaian Aplikasi dan Maklumat

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara 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) Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat; dan

d) Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem maklumat terperingkat (sulit / rahsia).

7.7 Peralatan Mudah Alih dan Kerja Jarak Jauh

Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut :

a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih;

b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat;

c) Memastikan bahawa anti virus digunakan dan sentiasa dikemaskinikan untuk aset ICT;

d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan

e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

7.8 Penggunaan Capaian Tanpa Wayar

Penggunaan capaian tanpa wayar adalah tidak dibenarkan seperti penggunaan Modem Broadband yang disambung kepada komputer peribadi (PC) Jabatan adalah tidak dibenarkan sama sekali. Sekiranya ada keperluan, pengguna hendaklah mendapatkan kebenaran daripada Bahagian Pengurusan Maklumat.

7.9 Tanggungjawab Pengguna

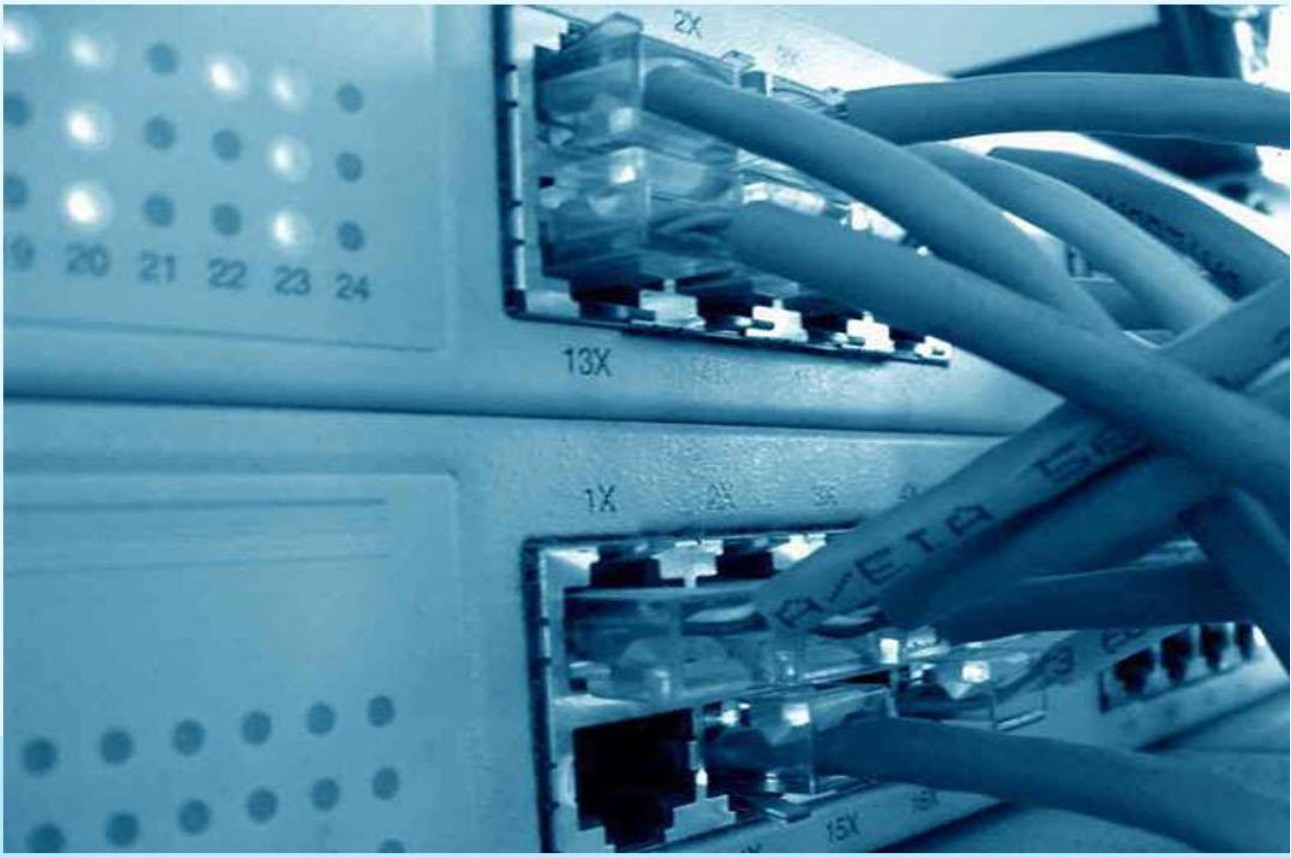
Seksyen ini bertujuan memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut :

a) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan;

b) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan

c) Mematuhi amalan clear desk policy dan clear screen policy.



PEROLEHAN, PEMBANGUNAN & PENYELENGGARAAN SISTEM

8. PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif :

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

8.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;

b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sistem output untuk memastikan data yang telah diproses adalah tepat;

c) Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan

d) Semua sistem yang dibangunkan secara dalaman / luaran hendaklah diuji sepenuhnya bagi memenuhi keperluan keselamatan yang telah ditetapkan.

8.2 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan mengikut prosedur yang ditetapkan;

b) Kod atau atur cara sistem yang telah dikemaskini hanya boleh

dilaksanakan atau digunakan selepas diuji;

c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;

d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan

e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

8.3 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut :

a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;

b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi;

c) Mengawal perubahan dan / atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;

d) Mewujudkan jejak audit dalam sistem aplikasi;

e) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan;

f) Menghalang sebarang peluang untuk membocorkan maklumat;

g) Pembangunan perisian secara khidmat luar (*outsource*) perlu diselia dan dipantau oleh pemilik sistem;

h) Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik JPSM; dan

i) Kawalan yang bersesuaian dan log audit perlu direka bentuk ke dalam sistem aplikasi. Ini termasuklah pengesahan data yang dimasukkan, data yang dihasilkan, pemprosesan dalaman, pengesahan dan integriti mesej, dan sebagainya. Ukuran keselamatan mesti dititik beratkan semasa membangunkan aplikasi baru atau mengemas kini / menambah baik aplikasi sedia ada.

8.4 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Keterdedahan adalah bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman. Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan adalah seperti berikut :

a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;

b) Menilai tahap keterdedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan

c) Mengambil langkah kawalan untuk mengatasi risiko berkaitan.

8.5 Kawalan Kriptografi (Cryptography)

Kriptografi bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

Tindakan melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi yang boleh dilakukan adalah seperti berikut:39 Dasar Keselamatan Teknologi Maklumat dan Komunikasi

a) Pengguna digalakkan membuat enkripsi dengan menukarkan teks biasa (plain text) kepada bentuk cipher text ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa;
b) Penggunaan tandatangan digital digalakkan kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; dan
c) Pengurusan ke atas Public Key Infrastructure (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

9. PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Objektif :

- Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.
- Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

9.1 Pengurusan Pengendalian Insiden Keselamatan

ICTSO dan Pasukan Pengendali Insiden JPSM bertanggungjawab mengurus dan mengendalikan insiden keselamatan ICT termasuk perkara-perkara berikut :

a) Menguruskan tindakan ke atas insiden yang berlaku sehingga keadaan pulih; dan

b) Menentukan sama ada sesuatu insiden perlu dilaporkan kepada agensi penguatkuasaan undang-undang / keselamatan.

9.2 Insiden Keselamatan

Insiden keselamatan bermaksud adverse event yang berlaku ke atas sistem maklumat dalam pelbagai keadaan seperti:

a) Percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (probing);

b) Serangan kod perosak (malicious code) seperti virus, trojan horse, worms dan seumpamanya;

c) Gangguan yang disengajakan (intended disruption) atau penafian penyampaian perkhidmatan (denial of service);

d) Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (unauthorised access); dan

e) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana

komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

9.3 Melaporkan Insiden

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Bahagian Pengurusan Maklumat. Sekiranya terdapat keperluan insiden keselamatan akan dilaporkan kepada CERT NRE. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO.

9.4 Menentukan Keutamaan Tindakan Ke Atas Insiden

Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden. Keutamaan akan ditentukan seperti berikut:

Keutamaan 1 :

Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.

Keutamaan 2 :

a) Pencerobohan atau percubaan menceroboh melalui infrastruktur Internet ke atas peralatan rangkaian;

b) Penyebaran penafian penyampaian perkhidmatan (distributed denial of service);

c) Serangan atau pendedahan keterdedahan terbaru (new vulnerabilities); atau

Lain-lain insiden seperti :

a) Pencerobohan melalui pemalsuan identiti;

b) Pengubahsuaian laman web, perisian, atau mana-mana komponen sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; dan

c) Gangguan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran.

9.5 Pengendalian Insiden

Sekiranya berlaku insiden keselamatan ICT, laporan hendaklah dimajukan kepada JPSM Computer Emergency Response Team (JPSMCERT) di alamat emel jpsm_cert@forestry.gov.my atau menghubungi Bahagian Pengurusan Maklumat.

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif :

Menjamin operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

10.1 Kesinambungan Perkhidmatan

Ketua Jabatan atau Pengarah Bahagian / Ketua Unit bertanggungjawab memastikan perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

10.2 Pelan Kesinambungan Perkhidmatan

Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk mengekalkan kesinambungan perkhidmatan bagi memastikan tiada gangguan di dalam penyediaan perkhidmatan agensi. Pelan ini mestilah diperakui oleh pengurusan JPSM dan perkara-perkara berikut perlu diberi perhatian:

a) Mengenal pasti dan mendokumenkan semua tanggungjawab dan prosedur kecemasan atau pemulihan;

b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;

c) Mengadakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan;

d) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali;

e) Menguji Pelan Pemulihan Bencana (Disaster Recovery Plan - DRP) sekali setahun (atau selepas perubahan besar, atau mana yang lebih dahulu); dan

f) Membuat backup.

10.3 Perubahan atau Pengecualian Business Continuity Plan (BCP)

a) Jika pengecualian / pertukaran / kemas kini BCP diperlukan, permintaan secara bertulis termasuk keterangan dan kebenaran untuk pengecualian / perubahan hendaklah dikemukakan kepada Ketua Jabatan atau Pengarah Bahagian / Ketua Unit;

b) Salinan pelan kesinambungan perkhidmatan mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan;

c) Ujian pelan kesinambungan perkhidmatan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan

d) JPSM hendaklah memastikan salinan pelan kesinambungan perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

10.4 Program Latihan dan Kesedaran Terhadap BCP

Semua kakitangan JPSM perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap BCP. Ketua Jabatan atau Pengarah Bahagian / Ketua Unit bertanggung jawab dalam memastikan latihan dan program kesedaran terhadap BCP dilaksanakan setiap tahun.

10.5 Pengujian BCP

DRP perlu diuji sekali (1) kali setahun (atau selepas perubahan utama, atau yang mana terdahulu) bagi memastikan kakitangan JPSM mengetahui bagaimana ianya laksanakan. Komponen BCP yang lain perlu diuji sekali (1) setahun atau selepas perubahan utama, atau yang mana terdahulu.

PEMATUHAN

11. PEMATUHAN

Objektif :

Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

11.1 Pematuhan Dasar

Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang perlanggaran dielakkan.

Langkah-langkah perlu bagi mengelakkan sebarang perlanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

11.2 Keperluan Perundangan

Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan termasuklah seperti berikut :

a) Keselamatan dokumen

   i. Akta Rahsia Rasmi 1972; dan

   ii. Akta Arkib Negara 2003.

b) Keselamatan individu

   Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

c) Keselamatan aset ICT

i. Akta Tandatangan Digital 1997;

ii. Akta Jenayah Komputer 1997;

iii. Akta Hak Cipta (Pindaan) 1997;

iv. Pekeliling Am Bil. 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi;

v. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);

vi. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi-Agensi Kerajaan;

vii. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;

viii. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005;

ix. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

x. Arahan Keselamatan; dan

xi. ISO/IEC 27001:2013.

11.3 Perlindungan dan Privasi Data Peribadi

Warga JPSM perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik JPSM. Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT.

Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian. Pihak pengurusan JPSM berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi dasar ini.

JPSM menggalakkan dasar privasi yang adil. Pihak pengurusan perlu bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat.

Pendedahan maklumat peribadi tentang warga JPSM kepada pihak ketiga tidak sepatutnya berlaku kecuali :

a) Dikehendaki oleh undang-undang atau peraturan;

b) Dengan persetujuan yang jelas dan nyata daripada warga tersebut; atau

c) Setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh Bahagian Perundangan dan Pendakwaan serta perjanjian jelas diperoleh daripada pengurusan sumber manusia.

11.4 Semakan Keselamatan Maklumat

Semakan keselamatan maklumat mestilah diambil kira seperti berikut :

a) Pematuhan pemeriksaan ke atas dasar keselamatan maklumat piawaian dan prosedur perlu dilakukan secara tahunan. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi;

b) Penetration Test bagi sistem yang kritikal mestilah dilaksanakan sekurang-kurangnya setahun sekali atau bila ada keperluan. Tujuan Penetration Test ini adalah untuk memastikan pematuhan terhadap piawaian keselamatan ICT; dan

c) Perkara (a) dan (b) di atas mestilah dilaksanakan oleh pihak yang tidak terlibat dalam pelaksanaan aktiviti keselamatan ICT tersebut.

11.5 Pelanggaran Perundangan

Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan termasuk dasar keselamatan ICT yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972. Antara tindakan yang boleh diambil terhadap pihak ketiga adalah penamatan kontrak.

11.6 Surat Akuan Pematuhan Dasar Keselamatan ICT

Adalah menjadi tanggungjawab Ketua Jabatan dan Pengarah Bahagian / Ketua Unit untuk memastikan setiap pegawai di JPSM menandatangani Surat Akuan Pematuhan Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) seperti di **LAMPIRAN A**.

12. PENGHARGAAN

Sekalung jutaan terima kasih kepada :

1. YBhg. Dato' Prof Dr. Haji Abd. Rahman Bin Haji Abd. Rahim
   Ketua Pengarah Perhutanan Semenanjung Malaysia
2. YBhg. Dato' Haji Nor Akhirrudin Bin Mahmud
   Timbatan Ketua Pengarah Perhutanan (Dasar dan Perancangan)
3. En. Borhanudin Bin Hj. Arshad
   Timbalan Ketua Pengarah (Operasi dan Teknikal)
4. Pengarah-Pengarah Bahagian
5. Ketua Unit
6. Semua individu yang terlibat secara langsung ataupun tidak langsung dalam penyediaan Dokumen Dasar Keselamatan ICT (DKICT) JPSM

13. JAWATANKUASA KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI JABATAN PERHUTANAN SEMENANJUNG MALAYSIA

Pengerusi	:	Tn. Haji Khairudin Bin Mohamad Mor
Setiausaha	:	Pn. Noriswani Binti Za'aldin
Ahli	:	En. Mohd Farid Bin Mahfar
		Cik Mutia Anggerek Binti Jusoh
		En. Muhammad Hanafi Bin Mohd Bakri
		En. Khairul Amir Bin Mohammad
		En. Mohammad Eqmal Fareed Bin Md Yusof

LAMPIRAN A

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (DKICT)
JABATAN PERHUTANAN SEMENANJUNG MALAYSIA (JPSM)

Nama :

No. Kad Pengenalan :

Jawatan :

Bahagian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT JPSM ; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : _____

Tarikh : _____

Pengesahan Pegawai Keselamatan ICT

_____

(**ICTSO JPSM**)

b.p. Ketua Jabatan
Jabatan Perhutanan Semenanjung Malaysia

Tarikh : _____

14. GLOSARI

No.	Akronim	Keterangan
1.	ICT	Teknologi Maklumat dan Komunikasi (*Information Communication Technology*)
2.	JPSM	Jabatan Perhutanan Semenanjung Malaysia
3.	ICTSO	*Information Communication Technology Security Officer*
4.	JPICT	Jawatankuasa Pemandu ICT
5.	CERT ICT	*Community Emergency Response Team, Information Communication Technology*
6.	CD	*Compact Disc*
7.	DVD	*Digital Video Disc*
8.	ID	Data Maklumat (*Information Data)*
9.	PC	Komputer Peribadi (*Personal Computer*)
10.	ISO/IEC 27001:2013	International Organization for Standardization / International Electrotechnical Commission (27001:2013)
11.	DKICT	Dasar Keselamatan Teknologi Maklumat dan Komunikasi (*Information Communication Technology*)
12.	NRE	Kementerian Sumber Asli & Alam Sekitar (*Ministry of Natural Resources & Environment*)
13.	JKR	Jabatan Kerja Raya

Diterbitkan oleh :

Ibu Pejabat Jabatan Perhutanan Semenanjung Malaysia,
Jalan Sultan Salahuddin,
50660 Kuala Lumpur
Malaysia
Telefon : 03 - 2616 4488
Faks : 03 - 2692 5657
Laman Web : http://www.forestry.gov.my

JABATAN PERHUTANAN SEMENANJUNG MALAYSIA