ARAHAN TEKNOLOGI MAKLUMAT

Disember 2007

MAMPU

Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia
Jabatan Perdana Menteri

Perpustakaan Negara Malaysia Data Pengkatalogan-dalam-Penerbitan

Arahan Teknologi Maklumat = Information Technology Instructions.
ISBN 978-983-9827-21-7

1. Information technology—Malaysia. 2. Management Information systems.
I. Information technology Instructions.
658.4038

Diterbitkan oleh:

Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri
Aras 6, Blok B2,
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

Telefon : 03-8888 1199

Faks : 03-8888 3721

Laman Web : www.mampu.gov.my

19 Disember 2007

KANDUNGAN

BAB I: PENGENALAN

1. Objektif

Arahan Teknologi Maklumat (*Information Technology* [IT]) dalam konteks ini adalah sebagai garis panduan bertujuan memenuhi keperluan minimum bagi menyokong Akta Aktiviti Kerajaan Elektronik (*Electronic Government Activities Act* [EGAA]) 2007 dalam memudah cara transaksi elektronik.

2. Latar Belakang

Latar belakang dan tujuan EGAA 2007

2.1. EGAA 2007 menyediakan rangka kerja undang-undang untuk pelaksanaan perkhidmatan Kerajaan elektronik yang efisien dan selamat. Tujuan Akta ini adalah untuk membolehkan dan memudah cara keseragaman urusan secara elektronik antara Kerajaan Persekutuan dengan orang awam.

Akta tidak menambah atau mengubah mana-mana undang-undang yang berkaitan

2.2. Akta ini terpakai apabila Agensi bersedia untuk menguruskan urusan elektronik dan tidak memberi sebarang tambahan hak undang-undang atau menukar sesuatu undang-undang secara substantif.

Menteri bertanggungjawab boleh mengeluarkan Arahan IT

2.3. Di bawah Seksyen 9 Akta ini, Menteri bertanggungjawab boleh mengeluarkan Arahan IT yang merupakan keperluan minimum untuk membolehkan Agensi melaksanakan transaksi elektronik. Dalam hal ini, apabila Agensi memulakan sebarang inisiatif berkaitan elektronik, Agensi boleh memilih untuk menggunakan Arahan IT sebagai garis panduan dalam bidang-bidang yang berkaitan. Justeru itu, Agensi hendaklah menetapkan akta-akta yang berkaitan dengan EGAA dan kemudiannya mematuhi garis panduan yang ditetapkan di bawah Arahan IT bagi bidang-bidang tertentu.

3. Skop

Skop Arahan IT

3.1. Dokumen ini mengandungi Arahan IT yang merangkumi bidang-bidang berikut:

3.1.1. standard teknologi maklumat;

3.1.2. kriteria tandatangan digital dan cap mohor elektronik yang bersesuaian dengan tujuan kegunaannya;

3.1.3. merekodkan masa, akuan penerimaan dokumen-dokumen elektronik atau mesej-mesej;

3.1.4. langkah-langkah keselamatan terhadap akses tanpa izin, pengubahsuaian tanpa izin, penghalang perkhidmatan dan penyangkalan;

3.1.5. prosedur pemulihan bencana;

3.1.6. peraturan aksesibiliti bagi perkhidmatan Kerajaan elektronik dan borang elektronik;

3.1.7. pengurusan dan penyelenggaraan dokumen elektronik;

3.1.8. prosedur berkaitan kemasukan data, semakan dan pengesahan mesej; dan

3.1.9. garis panduan untuk pembayaran dan penerimaan wang.

3.2. Bidang-bidang di atas dirangkumkan di dalam bab-bab berikut:

3.2.1. Bab II: Sistem Aplikasi;

3.2.2. Bab III: Keperluan-keperluan Keselamatan Teknologi Maklumat dan Komunikasi (*Information and Communication Technology* [ICT]); dan

3.2.3. Bab IV: Pengurusan Rekod Elektronik.

4. Pemakaian

Pemakaian Arahan IT

4.1. Arahan IT adalah terpakai untuk semua agensi Kerajaan Persekutuan (kemudian ini disebut sebagai "Agensi").

4.2. Dokumen ini mesti disemak semula tertakluk kepada perubahan berikut:

4.2.1. teknologi;

4.2.2. *statutory* dan *regulatory*; dan

4.2.3. arah tuju *stakeholder*.

5. Tanggungjawab Agensi

Tanggungjawab agensi – bagi memenuhi keperluan minimum Arahan IT

Agensi yang telah bersedia atau dalam proses persediaan melaksanakan transaksi elektronik perlu memenuhi keperluan minimum Arahan IT di mana relevan.

BAB II: SISTEM APLIKASI

6. Pendahuluan

Aplikasi yang dipasang dan digunakan di dalam sesebuah Agensi meliputi kombinasi aplikasi yang dibangunkan secara komersial dan dalaman.

7. Objektif

Bab ini menyediakan garis panduan bagi keperluan minimum bagi sistem aplikasi untuk digunakan oleh Agensi yang bertanggungjawab membangun, melaksana atau menyelenggarakan aplikasi tersebut.

8. Skop

Skop sistem aplikasi

8.1. Skop bab ini merangkumi perkara-perkara berikut:

8.1.1. Aksesibiliti;

(a) Pelbagai Saluran;

(b) Standard Terbuka;

(c) Interoperabiliti; dan

(d) Komuniti Istimewa.

8.1.2. Perisian Sumber Terbuka;

8.1.3. Kemasukan Data, Semakan dan Pengesahan;

8.1.4. Merekodkan Masa dan Akuan Penerimaan;

8.1.5. Jejak Audit; dan

8.1.6. Pembayaran dan Penerimaan Wang

(a) Arahan Am;

(b) Pembayaran; dan

(c) Penerimaan.

8.2. Bidang-bidang di atas perlu mengambil kira perubahan teknologi dan *trend* akan datang, khusus bagi meminimumkan impak dan memastikan kestabilan serta mengelakkan sebarang perubahan besar atau pengubahsuaian kepada keperluan sistem aplikasi yang digunakan.

9. Aksesibiliti

Aksesibiliti sistem aplikasi

9.1. Aspek aksesibiliti sistem aplikasi akan diterangkan dari segi pelbagai saluran, standard terbuka, interoperabiliti dan komuniti istimewa.

9.1.1. <u>Pelbagai Saluran</u>

Pemilihan saluran mesti berdasarkan kepada kehendak dan keperluan pengguna

Agensi digalakkan untuk menyediakan perkhidmatan kepada orang awam melalui pelbagai saluran elektronik. Saluran yang dipilih perlu memenuhi keperluan orang awam/ pelanggan. Sebarang pengubahsuaian kepada saluran tersebut mestilah merujuk kepada perkara ini. Keperluan berikut perlu diteliti oleh Agensi yang berkaitan dengan penyampaian pelbagai saluran:

Saluran elektronik

(a) Penyampaian pelbagai saluran hendaklah dikaitkan dengan penyediaan perkhidmatan Kerajaan melalui *Multimedia Messaging System* (MMS) atau saluran-saluran elektronik lain (contoh: *Personal Digital*

Assistant [PDA], Telefon, Faksimile dan Kios), perkhidmatan (contoh: Sistem Pesanan Ringkas (*Short Messaging System* [SMS]), Internet dan *Interactive Voice Recognition* [IVR]) serta saluran konvensional (seperti mesyuarat dan kaunter);

Kepelbagaian saluran untuk keselesaan pengguna

(b) Agensi hendaklah menentukan kepelbagaian saluran elektronik, di mana sesuai, bagi memastikan aksesibiliti pelanggan. Kepelbagaian saluran hendaklah berkos efektif daripada perspektif Agensi dan pelanggan;

Mengenal pasti keperluan pelanggan

(c) Agensi hendaklah mengenal pasti pelanggannya, keperluan perkhidmatan dan saluran pilihan mereka;

Pengasingan pelanggan mengikut segmen dan pemilihan kriteria

(d) Agensi hendaklah menggunakan kriteria yang berbeza untuk pengasingan pelanggan mengikut segmen berdasarkan keperluan dan pilihan. Ini membolehkan pelanggan yang mempunyai ciri-ciri berlainan dibahagikan kepada segmen yang mudah diurus. Pengenalpastian ciri-ciri tersebut membolehkan keperluan kumpulan pelanggan ditentukan dan perkhidmatan disediakan khusus untuk memenuhi keperluan yang dimaksudkan. Pelbagai kriteria boleh digunakan bagi mengasingkan pasaran pelanggan seperti secara *geographic* (contoh: kawasan, saiz bandar raya), *demographic* (contoh: umur, jantina, pendapatan, pekerjaan), *psychographic* (contoh: cara hidup, personaliti) dan lain-lain; dan

Halangan aksesibiliti

(e) Agensi hendaklah mengenal pasti halangan-halangan yang mungkin akan memberi kesan kepada kumpulan tertentu mengakses saluran elektronik. Jika segmen pelanggan tertentu (contoh: warga emas) tidak dapat mengakses atau tidak mahir menggunakan komputer atau teknologi *online* yang berkaitan, saluran-saluran lain perlu dikenal pasti untuk segmen pelanggan tersebut bagi memudahkan akses kepada perkhidmatan yang disediakan.

9.1.2. Standard Terbuka

Perkhidmatan penyampaian elektronik berasaskan Sistem Terbuka

Perkhidmatan penyampaian elektronik perlu berasaskan Standard Terbuka yang merupakan standard sejagat, dibangunkan secara terbuka dan telus dengan penglibatan industri. Standard ini tidak *proprietary* dan dimiliki secara bersama, mempunyai spesifikasi akses terbuka merangkumi akses kepada spesifikasi antara muka secara percuma. Spesifikasi Standard Terbuka adalah *technology neutral*.

9.1.3. Interoperabiliti

Keperluan interoperabiliti

Agensi hendaklah membangunkan aplikasi berdasarkan Standard Terbuka untuk memastikan interoperabiliti dan aksesibiliti.

9.1.4. Komuniti Istimewa

Perkhidmatan yang disediakan memenuhi keperluan komuniti istimewa dan warga emas

Perkhidmatan yang disediakan hendaklah memenuhi keperluan komuniti istimewa seperti golongan Orang Kurang Upaya (contoh: ketinggian dan kawasan di sekeliling

kios hendaklah sesuai untuk pengguna berkerusi roda) dan warga emas (contoh: saiz huruf di paparan kios hendaklah sesuai).

10. Perisian Sumber Terbuka

Objektif "Malaysian Public Sector OSS Framework" dalam konteks pembangunan perisian aplikasi

10.1. Kerajaan Malaysia menggalakkan penggunaan Perisian Sumber Terbuka (*Open Source Software* [OSS]) untuk pembangunan sistem aplikasi. "The Malaysian Public Sector OSS Framework" telah direka bentuk dan dibangunkan bagi menyediakan garis panduan untuk merancang dan melaksanakan OSS dalam Sektor Awam.

Pertimbangan utama pelaksanaan Sistem Terbuka

10.2. Pelaksanaan OSS hendaklah berdasarkan kepada beberapa pertimbangan utama iaitu:

10.2.1. mesti bersesuaian dengan tujuan dari segi fungsi dan juga *platform* teknologi;

10.2.2. kurang menimbulkan gangguan kepada operasi urusan sedia ada; dan

10.2.3. mesti ada keupayaan untuk wujud bersama-sama sistem legasi lain.

11. Kemasukan Data, Semakan dan Pengesahan

Prosedur perlu memastikan borang elektronik membenarkan pembetulan kesilapan sebelum borang dihantar

11.1. Prosedur berkaitan kemasukan, semakan dan pengesahan data hendaklah memastikan borang elektronik direka bentuk untuk membenarkan pembetulan kesilapan dilakukan oleh pengguna yang mengisi borang sebelum dihantar (contoh: sistem perlu memaparkan kotak dialog memohon pengesahan sebelum pengguna menghantar borang).

Pengesahan dan semakan input bagi mengesan kesalahan

11.2. Data yang dimasukkan ke dalam sistem aplikasi mesti disemak bagi memastikan betul dan sesuai. Semakan

input mesti dilaksanakan bagi mengesan kesilapan berikut di mana bersesuaian, sebagai contoh:

11.2.1. nilai di luar julat;

11.2.2. data hilang atau tidak lengkap;

11.2.3. aksara yang tidak sah dalam medan data;

11.2.4. melebihi had;

11.2.5. data tanpa izin (contoh: medan bagi kelulusan permohonan hanya boleh dikemas kini oleh personel yang diberi kuasa); dan

11.2.6. data tidak konsisten.

12. Merekodkan Masa dan Akuan Penerimaan

Kepentingan merekodkan tarikh dan masa serta akaun penerimaan

12.1. Sistem untuk merekodkan tarikh dan masa dan akuan penerimaan perlu disediakan untuk mengelakkan pertikaian bila dokumen diterima dan masa diterima. Ini penting terutama sekali apabila dokumen atau maklumat mesti diserahkan pada tarikh dan masa tertentu.

Pewujudan prosedur untuk menyemak ketepatan masa

12.2. Prosedur bagi menyemak ketepatan jam dan pembetulan mesti diwujudkan seperti menggunakan *Network Time Protocol* (NTP) yang direka bentuk untuk menyelaraskan jam sistem komputer (URL: http://www.ntp.org). *Real-time clock* bagi peranti komunikasi mesti ditetapkan mengikut “Malaysian Standard Time Act 1981”.

12.3. Merekodkan masa dan akuan penerimaan mesti mengambil kira komponen *front-end* dan *back-end*, iaitu yang berkaitan dengan penghantaran borang dan pemprosesan transaksi:

12.3.1. *Front-End*: Penghantaran Borang

Front-End: Penghantaran borang

Akuan penghantaran menggunakan waktu pelayan diperlukan tanpa mengambil kira jenis transaksi atau pemprosesan yang perlu dilaksanakan. Proses yang terlibat hendaklah meliputi tetapi tidak terhad kepada perkara-perkara berikut:

(a) data/dokumen memasuki pelayan;

(b) akuan penerimaan; dan

(c) rujukan kepada penghantaran borang.

12.3.2. *Back-End:* Pemprosesan Transaksi

Back-End: Pemprosesan Transaksi

Merekodkan penerimaan secara terperinci diperlukan dengan menggunakan waktu pelayan. Proses yang terlibat hendaklah meliputi tetapi tidak terhad kepada perkara-perkara berikut:

(a) data/dokumen memasuki pelayan;

(b) pengemaskinian pangkalan data;

(c) akuan penerimaan setelah pangkalan data berjaya dikemas kini; dan

(d) rujukan kepada penerimaan.

12.4. Terdapat keperluan penting untuk mewujudkan suatu bentuk mekanisme pemberitahuan kegagalan (contoh: kegagalan rangkaian).

13. Jejak Audit

Definisi dan kepentingan jejak audit

13.1. Jejak audit merupakan rekod aktiviti yang digunakan sebagai cara merekodkan peristiwa dan mewujudkan akauntabiliti. Adalah penting untuk memastikan ketepatan log audit yang diperlukan untuk siasatan atau sebagai bukti dalam undang-undang atau kes disiplin.

Jenis log yang mesti diperoleh dan disimpan

13.2. Beberapa jenis log mesti diperoleh dan disimpan, seperti log sistem, log rangkaian, log pelayan dan log transaksi. Jenis log dan jangka masa mengarkibkan mesti dirujuk kepada Akta yang berkaitan (contoh: “Akta Arkib Negara 2003”, “Akta Lembaga Hasil Dalam Negeri Malaysia 1995”), jika tidak, jangka masa minimum mengarkibkan mesti satu (1) tahun relatif kepada tahun sebelumnya.

Pengauditan sistem

13.3. Perkara-perkara berikut mesti diteliti berhubung dengan jejak audit:

13.3.1. Semua sistem mesti boleh diaudit.

13.3.2. Perubahan kepada data mesti direkodkan mengikut susunan kronologi dan secara terperinci. Sejarah lengkap transaksi mesti direkodkan dan dikekalkan bagi setiap sesi yang melibatkan akses kepada maklumat terperingkat dan maklumat-maklumat sensitif lain menurut “Arahan Keselamatan” bagi membenarkan pengauditan sistem. Dalam hal ini, jejak audit bagi yang berikut mesti diwujudkan dan dikekalkan:

(a) sesi memulakan dan menutup operasi sistem; dan

(b) sejarah transaksi dengan log minimum bagi maklumat berikut:

(i) semua jenis transaksi;

(ii) tarikh dan masa aktiviti;

(iii) pengenalan identiti pengguna;

(iv) aktiviti *sign-on* and *sign-off*; dan

(v) paparan transaksi sensitif (contoh: akses kepada laporan terperingkat, penggunaan pengenalan identiti sensitif).

13.3.3. Pembelian sebarang perkakasan atau sistem yang ada kaitan dengan memproses dan merekodkan maklumat terperingkat, sulit atau sensitif mesti merujuk dan mematuhi para 28 dan 29, "Arahan Keselamatan" oleh Pejabat Ketua Pegawai Keselamatan Kerajaan.

Analisis sejarah transaksi bagi mengesan perbezaan

13.3.4. Analisis sejarah transaksi bertujuan mengesan perbezaan mesti dikendalikan sebulan sekali bagi:

(a) mengesan kegagalan akses;

(b) mengesan penggunaan luar biasa seperti *login* di luar waktu biasa, frekuensi dan jangka masa akses;

(c) memantau hak keistimewaan akses;

(d) mengesan transaksi terpilih; dan

(e) memerhatikan penggunaan sumber-sumber yang sensitif seperti cek kosong, pasport, sijil peperiksaan, sijil lahir dan lain-lain.

Ciri-ciri kalis rosak

13.4. Log audit mesti kalis rosak dan integritinya tidak diragui (rujuk Bab III: Keperluan-keperluan Keselamatan ICT).

14. Pembayaran dan Penerimaan Wang

Keperluan bagi aplikasi yang digunakan untuk pembayaran dan penerimaan wang

14.1. Aplikasi yang digunakan untuk pembayaran dan penerimaan wang mesti dilengkapkan dengan prosedur kelulusan, keperluan pematuhan, proses kerja, ciri-ciri keselamatan, penyimpanan dan keupayaan jejak audit yang bersesuaian. Arahan bagi ciri-ciri ini diterangkan secara umum, diikuti dengan garis panduan yang lebih spesifik bagi pembayaran dan penerimaan.

14.1.1. Arahan Am

Kelulusan

(a) Pembangunan dan pengubahsuaian sistem kewangan seperti sistem yang berkaitan dengan pembayaran dan penerimaan wang, mesti terlebih dahulu mendapat kelulusan bertulis daripada Jabatan Akauntan Negara.

Pematuhan

(b) Pembangunan dan operasi sistem kewangan mesti mematuhi keperluan dan peruntukan "Arahan Perbendaharaan".

Prosedur/proses kerja

(c) Prosedur kerja bertulis yang jelas bagi proses kerja mesti disediakan untuk diikuti oleh pengguna sistem. Pengguna mesti menyimpan semua dokumen sokongan yang digunakan sebagai asas kepada kemasukan data.

Keselamatan

(d) Semua data yang diinput dan dijana oleh sistem mesti disimpan dengan sempurna dan selamat supaya boleh diperoleh semula dalam apa jua bentuk yang ditentukan bila diperlukan.

Jangka masa penyimpanan

(e) Data mesti disimpan di dalam sistem untuk jangka masa minimum menurut tempoh yang ditetapkan oleh “Arahan Perbendaharaan”.

Jejak audit

(f) Sistem mesti menyimpan perincian jejak audit bagi semua transaksi.

14.1.2. Pembayaran

Makluman kepada pembayar dan status semakan

(a) Untuk semua pembayaran yang telah dibuat secara elektronik, sistem mesti memastikan pembayar dimaklumkan. Butiran terperinci berkaitan tujuan pembayaran mesti dinyatakan dengan jelas dalam notis pemberitahuan. Sistem juga mesti menyediakan kemudahan untuk membolehkan pembayar membuat pertanyaan berkenaan status pembayaran mereka.

Kawalan dan perlindungan

(b) Mesti ada kawalan yang mencukupi bagi membenarkan hanya orang yang diberi kuasa mengemas kini maklumat dalam pangkalan data. Kawalan yang mencukupi mesti disediakan dalam sistem untuk memastikan pembayaran secara elektronik diterima oleh penerima yang sah.

Penghantaran data

(c) Penghantaran data ke institusi perbankan untuk tujuan pembayaran mesti dilindungi secukupnya dari sebarang bentuk perubahan (rujuk Bab III: Keperluan-keperluan Keselamatan ICT).

Pengesahan dan pengenalpastian personel

(d) Peranan dan had mengakses bagi setiap personel yang diizinkan dalam proses pembayaran mesti dinyatakan dengan jelas dan dikawal di dalam sistem. Sistem hendaklah berupaya mengenal pasti personel yang bertanggungjawab bagi sebarang transaksi kewangan.

14.1.3. Penerimaan

Kelulusan Kementerian Kewangan

(a) Penerimaan wang boleh dibuat dalam sebarang bentuk yang diluluskan oleh Kementerian Kewangan.

Bentuk kutipan dinyatakan di dalam sistem dan resit

(b) Bentuk kutipan mesti dinyatakan di dalam sistem dan semua resit yang dikeluarkan.

Mata wang asing

(c) Jika Agensi dibenarkan mengutip bayaran dalam mata wang selain dari mata wang tempatan, sistem perlu merekodkan:

(i) kadar tukaran;

(ii) tarikh kadar tukaran; dan

(iii) jumlah yang sama dalam mata wang tempatan.

Pengenalpastian penerimaan

(d) Sistem hendaklah boleh mengenal pasti atau mengaitkan sebarang penerimaan dengan rekod pungutan yang betul.

Saluran elektronik untuk pembayaran

(e) Apabila sebarang undang-undang memerlukan sebarang pembayaran dibuat, keperluan tersebut dipenuhi jika pembayaran tersebut dilakukan melalui

saluran elektronik (contoh: kios atau resit secara maya seperti SMS) dan mematuhi sebarang syarat yang dikenakan oleh Kerajaan.

Akses kepada maklumat pembayaran

(f) Sistem mesti memastikan maklumat pembayaran boleh dicapai dan sentiasa tersedia apabila diperlukan oleh orang awam.

Pengeluaran resit

(g) Apabila sebarang undang-undang memerlukan sebarang pengeluaran resit bayaran, keperluan tersebut dipenuhi dengan mengeluarkan resit elektronik jika resit tersebut boleh diakses, dapat dibaca dan boleh digunakan untuk rujukan selanjutnya.

BAB III: KEPERLUAN-KEPERLUAN KESELAMATAN ICT

15. Pendahuluan

Sistem pemprosesan ICT agensi terdedah kepada ancaman-ancaman keselamatan dari pelbagai sumber

15.1. Sistem pemprosesan ICT Agensi adalah tidak terkecuali daripada ancaman keselamatan ICT. Ancaman utama adalah akses tanpa izin, pengubahsuaian, pendedahan dan kemusnahan maklumat sama ada secara sengaja atau tidak sengaja. Ancaman-ancaman ini mungkin berpunca daripada pelbagai sumber seperti kod perosak, penipuan, kecurian, espionaj, sabotaj dan pencerobohan. Kesan ancaman boleh dikurangkan melalui pewujudan dan pemantauan langkah-langkah keselamatan termasuk dasar, proses, prosedur, struktur organisasi, fungsi perisian dan perkakasan seiring dengan proses pengurusan *business*. Kebergantungan terhadap sistem-sistem maklumat bagi penyampaian perkhidmatan awam dan hubung kait antara rangkaian sektor awam/swasta bagi perkhidmatan perkongsian maklumat memerlukan Agensi sentiasa berwaspada terhadap ancaman, risiko, kelemahan dan pendedahan.

Pastikan kesinambungan penyampaian perkhidmatan

15.2. Agensi hendaklah melindungi sistem ICT yang dimiliki atau di bawah kawalannya daripada risiko, ancaman, kelemahan atau keterdedahan dengan mengurangkan kesan gangguan secara kos efektif untuk memastikan kesinambungan penyampaian perkhidmatan dan gangguan terhadap perkhidmatan diminimumkan.

Tanggungjawab Ketua Jabatan

15.3. Ketua Jabatan hendaklah bertanggungjawab untuk memastikan keselamatan aset ICT memadai dan bersesuaian di bawah jagaan dan/atau kawalannya berdasarkan “Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”.

16. Objektif

Bab ini menyediakan garis panduan bagi keperluan minimum keselamatan ICT untuk melindungi aset ICT Kerajaan dari segi kerahsiaan, integriti, ketersediaan, kesahihan dan tidak boleh disangkal.

17. Skop

Skop keperluan-keperluan keselamatan ICT

17.1. Skop bab ini merangkumi perancangan dan pelaksanaan keselamatan ICT Agensi yang berkaitan dengan perkara-perkara berikut:

17.1.1. Ciri-ciri Keselamatan Maklumat;

17.1.2. Penilaian Risiko dan *Treatment Plan*; dan

17.1.3. Bidang-Bidang Keselamatan ICT.

18. Ciri-Ciri Keselamatan Maklumat

Ciri-ciri utama keselamatan maklumat

18.1. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

18.1.1. Kerahsiaan;

18.1.2. Integriti;

18.1.3. Ketersediaan;

18.1.4. Kesahihan; dan

18.1.5. Tidak Boleh Disangkal.

18.2. Perincian setiap ciri keselamatan maklumat adalah seperti berikut:

18.2.1. Kerahsiaan

Definisi kerahsiaan

(a) Kerahsiaan bermaksud mengekalkan sekatan terhadap akses dan pendedahan maklumat yang diizinkan. Hilang kerahsiaan bererti pendedahan maklumat tanpa izin.

Enkrip maklumat terperingkat semasa dalam storan dan penghantaran

(b) Semua maklumat terperingkat hendaklah dienkrip semasa dalam storan dan penghantaran dengan menggunakan algoritma standard industri yang mematuhi "Akta Tandatangan Digital 1997" (Akta 562).

Melindungi dan merahsiakan *private key*

(c) Semua *private keys* perlu dilindungi dan dirahsiakan. Laporan hendaklah dibuat dengan segera apabila *private keys* hilang atau musnah.

Kunci kriptografi

(d) Semua kunci kriptografi hendaklah disimpan dalam *Hardware Security Module* (HSM) yang selamat dan kalis rosak.

Penghantaran yang selamat di setiap peringkat

(e) Agensi hendaklah memastikan penghantaran yang selamat di setiap peringkat dan melindungi trafik dari dicuri dengar, *connection hijacking* dan serangan rangkaian lain dengan menggunakan protokol *Secure Socket Layer* (SSL), *Secure Shell* (SSH) dan HSM versi semasa.

HSM hendaklah mematuhi standard minimum

(f) Semua HSM hendaklah mematuhi standard minimum FIPS 140-2 tahap tiga (3) atau setaraf dengannya.

18.2.2. Integriti

Definisi integriti

(a) Integriti bermaksud kawalan terhadap pengubahsuaian dan penghapusan maklumat yang tidak teratur, kesilapan dan maklumat tertinggal. Pendedahan dan/atau pengubahsuaian maklumat yang tidak diizinkan bererti tiada integriti.

Semakan integriti

(b) Agensi hendaklah melaksanakan semakan integriti seperti *hash total* untuk mencegah kesilapan dan maklumat tertinggal bagi mengekalkan integriti.

Semakan komprehensif

(c) Semakan komprehensif hendaklah diwujudkan di dalam subsistem keselamatan untuk memastikan integriti dan kesempurnaan semua data yang dihantar/diterima dari sistem/aplikasi luar.

Perlindungan dari serangan dalaman dan luaran rangkaian

(d) Sistem aplikasi dan infrastruktur keselamatan yang dilaksanakan hendaklah dilindungi dari serangan dalaman dan luaran rangkaian.

18.2.3. Ketersediaan

Definisi ketersediaan

(a) Ketersediaan bermaksud memastikan akses *on demand* terhadap data dan sumber kepada individu yang diizinkan.

Mekanisme perlindungan

(b) Mekanisme perlindungan hendaklah diwujudkan untuk melindungi daripada ancaman yang boleh memberi kesan terhadap ketersediaan sistem rangkaian dan maklumat.

Elakkan *single point of failure*

(c) *Single point of failure* hendaklah dielakkan.

Langkah-langkah *backup* dan mekanisme *redundancy*

(d) Langkah-langkah *backup* hendaklah dilaksanakan dan mekanisme *redundancy* diwujudkan jika perlu. Peranti *backup* hendaklah disediakan untuk menggantikan sistem kritikal dengan segera apabila berlaku kegagalan.

Kakitangan mahir hendaklah tersedia

(e) Kakitangan mahir hendaklah tersedia bagi tindakan pemulihan supaya sistem segera kembali beroperasi.

Perkhidmatan dan *port* diperlukan sahaja disediakan

(f) Hanya perkhidmatan dan *port* yang diperlukan sahaja disediakan.

Sistem Pengesanan Pencerobohan

(g) Sistem Pengesanan Pencerobohan (*Intrusion Detection System* [IDS]) hendaklah dipasang bagi memantau trafik rangkaian dan aktiviti hos.

18.2.4. Kesahihan

Definisi kesahihan

(a) Kesahihan bermaksud jaminan bahawa sesuatu subjek (pengguna, program atau proses) telah dikenal pasti dan disahkan dengan suatu set pengenalan, berbanding dengan maklumat yang telah disimpan bagi memastikan bahawa subjek berkenaan adalah entiti seperti yang didakwa.

Kesahihan akses

(b) Bagi membolehkan subjek mengakses sesuatu sumber, subjek tersebut perlu membuktikan siapa subjek sebenarnya sebagaimana yang didakwa, mempunyai pengenalan yang diperlukan dan telah

diizinkan untuk melaksanakan tindakan seperti yang dipohon.

Semua aktiviti hendaklah direkodkan

(c) Semua aktiviti yang dilaksanakan ke atas sumber sistem ICT Agensi hendaklah direkodkan bagi tujuan pengesanan dan akauntabiliti.

Penilaian teknik bagi pengenalan identiti dan kesahihan

(d) Agensi hendaklah menilai teknik yang digunakan bagi pengenalan identiti dan kesahihan untuk menentukan mekanisme yang sesuai dengan persekitaran.

Laksanakan *two factor authentication*

(e) Agensi hendaklah melaksanakan *two factor authentication*.

18.2.5. Tidak Boleh Disangkal

Definisi tidak boleh disangkal

(a) Tidak boleh disangkal bermaksud keperluan bagi membuktikan integriti dan punca data boleh disahkan daripada penafian penglibatan tindakan sebelumnya. Tidak boleh disangkal dapat dilaksanakan secara kriptografi dengan penggunaan tandatangan digital.

Penggunaan tandatangan digital

(b) Tandatangan digital hendaklah digunakan bagi tujuan tidak boleh disangkal. Penggunaan tandatangan digital hendaklah mematuhi keperluan-keperluan "Akta Tandatangan Digital 1997 (Akta 562)".

19. Penilaian Risiko dan *Treatment Plan*

Mengenal pasti risiko, ancaman, kelemahan dan pendedahan

19.1. Penilaian risiko akan membantu Agensi mengenal pasti risiko, ancaman, kelemahan dan pendedahan. Apabila risiko, ancaman, kelemahan dan pendedahan

telah dikenal pasti dan keputusan mengenai tindakan pengukuhan diambil, kawalan yang bersesuaian hendaklah dipilih dan dilaksanakan untuk memastikan kelemahan dikurangkan ke tahap yang boleh diterima.

Metodologi penilaian risiko

19.2. Metodologi standard berdasarkan "Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam" hendaklah digunakan untuk penilaian risiko. Agensi hendaklah melaksanakan "The Malaysian Public Sector Information Security High Level Risk Assessment (HiLRA)" dan/atau "The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)" untuk penilaian risiko.

Kekerapan melaksanakan penilaian risiko

19.3. Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam keperluan keselamatan ICT atau perubahan dalam persekitaran ICT Agensi.

20. Bidang-Bidang Keselamatan ICT

20.1. Terdapat sebelas (11) bidang keselamatan ICT seperti berikut:

20.1.1. Dasar Keselamatan ICT

Dasar Keselamatan ICT Agensi

(a) Dasar Keselamatan ICT merupakan elemen paling kritikal dalam program keselamatan ICT Agensi. Dasar ini mengenal pasti keseluruhan hala tuju keselamatan ICT Agensi dan sebagai panduan bagi pembangunan peraturan yang lebih spesifik untuk menangani keadaan tertentu.

Mewujudkan Dasar Keselamatan ICT secara bertulis

(b) Agensi hendaklah bertanggungjawab ke atas semua aset ICT di bawah pemilikannya. Ini dilaksanakan dengan mewujudkan Dasar Keselamatan ICT secara bertulis untuk membantu mengenal pasti perkara yang perlu dilindungi dan untuk memaklumkan kepada personel Agensi, aktiviti-aktiviti yang dibenarkan atau tidak dibenarkan. Dasar tersebut hendaklah menetapkan peraturan umum yang perlu dipatuhi oleh semua personel Agensi. Dasar tersebut juga hendaklah mengambil kira keperluan menguatkuasakan kawalan dan langkah-langkah bagi melindungi aset ICT Agensi.

Dasar dibangunkan berasaskan persekitaran Agensi masing-masing

(c) Agensi hendaklah membangunkan Dasar Keselamatan ICT Agensi berasaskan kepada persekitaran masing-masing.

Dasar hendaklah diluluskan oleh pengurusan atasan Agensi

(d) Dasar Keselamatan ICT hendaklah mendapat kelulusan pengurusan atasan Agensi, diterbitkan dan dimaklumkan kepada semua personel Agensi dan kepada pihak luar yang berkaitan jika perlu dengan memastikan maklumat sensitif tidak didedahkan.

Dasar hendaklah relevan dan dikuatkuasakan

(e) Dasar Keselamatan ICT hendaklah relevan, disebarkan ke seluruh Agensi, dimaklumkan, dikuatkuasakan dan pematuhannya dipantau.

Pengurusan keselamatan ICT oleh pusat pentadbiran bersepadu

(f) Semua aktiviti berkaitan dengan pengurusan keselamatan ICT (contoh: pengesahan pengguna, hak keistimewaan aplikasi dan pengurusan dasar

keselamatan ICT) hendaklah ditadbirkan oleh satu pusat pentadbiran bersepadu.

Dasar Keselamatan ICT perlu ada pemilik

(g) Dasar Keselamatan ICT hendaklah ada pemilik yang bertanggungjawab membangun, menilai dan mengkaji semula dasar.

Kekerapan kajian semula Dasar Keselamatan ICT

(h) Dasar Keselamatan ICT hendaklah dikaji semula secara berjadual atau apabila terdapat perubahan ketara kepada organisasi bagi memastikan dasar sentiasa kekal, relevan dan efisien.

Kajian semula dasar

(i) Kajian semula dasar hendaklah direkodkan. Dokumen dasar yang telah dipinda hendaklah mendapat kelulusan pengurusan atasan dan dimaklumkan semula kepada semua personel Agensi.

20.1.2. Struktur Pengurusan Keselamatan ICT

Struktur organisasi untuk memula dan mengawal keselamatan ICT

(a) Agensi hendaklah menyedari bahawa struktur organisasi bagi keselamatan ICT adalah penting untuk memulakan dan mengawal pelaksanaan keselamatan ICT.

Penubuhan kumpulan pengurusan

(b) Satu kumpulan pengurusan hendaklah ditubuhkan bagi memastikan terdapat sokongan terhadap inisiatif-inisiatif keselamatan ICT.

Pelantikan Pegawai Keselamatan ICT

(c) Seorang pegawai kanan hendaklah dilantik sebagai Pegawai Keselamatan ICT untuk menguruskan keseluruhan program keselamatan ICT.

Aktiviti-aktiviti keselamatan selaras dengan Dasar Keselamatan ICT Agensi

(d) Pegawai Keselamatan ICT hendaklah memastikan aktiviti-aktiviti keselamatan dilaksanakan selaras dengan Dasar Keselamatan ICT Agensi.

20.1.3. Pengurusan Aset

Pelindungan dari akses dan pendedahan tanpa izin

(a) Aset ICT Sektor Awam hendaklah dilindungi pada setiap masa daripada akses dan pendedahan tanpa izin.

Aset ICT dikenal pasti dengan jelas dan diuruskan dengan baik

(b) Aset ICT hendaklah dikenal pasti dengan jelas dan diuruskan dengan baik bagi mengekalkan kerahsiaan, integriti, dan ketersediaan. Aset ICT termasuk aset nyata dan tidak nyata seperti lesen, paten, jenama, cap perniagaan, hak cipta terpelihara dan metodologi *business* seperti "Seksyen 3 Akta Tatacara Kewangan 1957 (pindaan 1972)".

Aset ICT hendaklah diakaunkan

(c) Semua aset ICT hendaklah diakaunkan, mempunyai rekod inventori dan pemilik.

Inventori aset ICT

(d) Inventori aset ICT hendaklah mengandungi semua maklumat yang diperlukan untuk pemulihan daripada bencana, merangkumi jenis aset, format, lokasi, maklumat *backup*, maklumat lesen dan nilai *business.*

Pengelasan maklumat

(e) Pengelasan maklumat hendaklah mengikut "Arahan Keselamatan" dan tahap perlindungan yang diperlukan bagi setiap aset hendaklah dipersetujui dan didokumenkan.

Had akses

(f) Personel Agensi, kontraktor dan pengguna pihak ketiga yang mengakses aset ICT Agensi hendaklah dimaklumkan mengenai had penggunaan mereka dan dipertanggungjawabkan terhadap aset yang digunakan.

20.1.4. Keselamatan Sumber Manusia

Personel adalah aset terpenting Agensi

(a) Personel adalah aset terpenting bagi sesebuah Agensi. Menerusi perancangan pembudayaan yang baik, personel boleh menyumbang dalam mencapai misi dan visi Agensi. Personel memainkan peranan penting dalam menyokong program keselamatan ICT Agensi. Berbekalkan latihan yang sempurna, kebanyakan personel boleh diharapkan untuk mengenal pasti anomali dan penyelewengan dari amalan terbaik keselamatan, yang kelak boleh menjadi asas untuk tindakan pemulihan.

Kerajaan berhak memantau penggunaan sumber-sumber ICT

(b) Agensi hendaklah menerapkan kepada pengguna bahawa sumber-sumber ICT adalah hak milik Kerajaan termasuk data, maklumat yang tercatat atau yang diperoleh daripadanya. Kerajaan sebagai pemilik, berhak memantau aktiviti pengguna yang mengakses sumber-sumber ICT untuk mengesan salah guna atau penggunaan sumber ICT selain dari tujuan yang telah ditetapkan.

Akauntabiliti pengguna

(c) Semua pengguna adalah bertanggungjawab keatas tindakan masing-masing apabila mengakses aset ICT Sektor Awam. Akauntabiliti ini hendaklah diperjelaskan kepada semua pengguna.

Keupayaan merekod dan mengesan tindakan pengguna

(d) Semua sistem maklumat ICT hendaklah mempunyai keupayaan merekodkan dan mengesan tindakan pengguna.

Tapisan keselamatan

(e) Personel Agensi, kontraktor dan pengguna pihak ketiga hendaklah melalui tapisan keselamatan selaras dengan undang-undang, peraturan dan etika yang relevan serta perlu seimbang dengan tahap klasifikasi maklumat yang perlu dicapai dan risiko yang terlibat.

Peranan dan tanggungjawab

(f) Personel Agensi, kontraktor dan pengguna pihak ketiga hendaklah dimaklumkan mengenai peranan dan tanggungjawab mereka terhadap keselamatan seperti yang ditetapkan dalam Dasar Keselamatan ICT Agensi.

Latihan dan program kesedaran

(g) Personel Agensi dan jika perlu, kontraktor dan pengguna pihak ketiga hendaklah diberikan latihan, program kesedaran serta dikemas kini mengenai dasar dan prosedur Agensi yang berkaitan dengan tugas mereka secara berkala.

Pengurusan kawalan akses

(h) Agensi hendaklah menguruskan urusan keluar, berhenti, pertukaran peranan dan tanggungjawab personel, kontraktor dan pengguna pihak ketiga bagi memastikan semua perkakasan, perisian dan dokumen agensi dipulangkan dan hak akses ditarik balik.

20.1.5. Keselamatan Fizikal dan Persekitaran

(a) Para ini hendaklah dibaca bersekali dengan "Arahan Keselamatan" yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan.

Prinsip *defense-in-depth*

(b) Bagi menghalang akses tanpa izin, kerosakan dan gangguan, perlindungan fizikal hendaklah sepadan dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth.*

Tempatkan kemudahan ICT yang kritikal/sensitif di kawasan selamat

(c) Kemudahan ICT yang kritikal atau sensitif hendaklah ditempatkan di kawasan yang selamat, jauh dari penglihatan awam, dilindungi oleh perimeter keselamatan yang ditetapkan, dengan halangan keselamatan dan kawalan pintu masuk yang sesuai. Kemudahan tersebut juga hendaklah dilindungi secara fizikal daripada akses tanpa izin, kerosakan dan gangguan.

Lindung kawasan selamat dengan kawalan kemasukan yang sesuai

(d) Kawasan selamat hendaklah dilindungi dengan kawalan kemasukan yang sesuai bagi memastikan hanya personel yang diizinkan dibenarkan masuk.

Had akses fizikal

(e) Akses fizikal hendaklah dihadkan kepada personel dan/atau krew penyelenggaraan yang perlu bagi operasi sistem ICT.

Kawalan kemasukan ke tempat akses

(f) Tempat akses seperti tempat penghantaran dan pemunggahan serta tempat-tempat lain yang mungkin membolehkan individu tanpa izin masuk ke premis hendaklah dikawal dan jika boleh, dijauhkan dari kemudahan

pemprosesan ICT bagi mengelakkan akses tanpa izin.

Perlindungan fizikal dari kerosakan

(g) Perlindungan fizikal hendaklah disediakan untuk melindungi dari kerosakan yang disebabkan oleh kebakaran, banjir, makhluk perosak, letupan, rusuhan awam dan bentuk bencana alam yang lain atau bencana buatan manusia.

Rujuk cadangan bangunan kepada CGSO

(h) Cadangan berkaitan bangunan, perolehan, sewaan, pengubahsuaian, pembelian bangunan Kerajaan dan swasta untuk menempatkan kemudahan pemprosesan ICT hendaklah dirujuk kepada Ketua Pegawai Keselamatan Kerajaan (*Chief Government Security Officer* [CGSO]).

Peralatan utiliti sokongan hendaklah dilindungi

(i) Peralatan utiliti sokongan Agensi hendaklah dilindungi dari gangguan bekalan elektrik dan gangguan-gangguan lain.

Pelbagai sumber bekalan elektrik

(j) Agensi hendaklah mengambil kira pelbagai sumber bekalan elektrik bagi mengelakkan *single point of failure.*

Kabel elektrik dan talian data hendaklah dilindungi

(k) Agensi hendaklah memastikan kabel elektrik dan telekomunikasi yang menyalurkan data atau perkhidmatan maklumat sokongan dilindungi daripada pintasan atau kerosakan.

Selenggara semua peralatan

(l) Agensi hendaklah menyelenggarakan semua peralatan dengan betul bagi memastikan ketersediaan dan integriti yang berterusan.

Keizinan membawa keluar

(m) Agensi hendaklah mendapat keizinan terlebih dahulu sebelum membawa keluar semua peralatan, maklumat atau perisian.

Pindah dan/atau hapus data sensitif atau perisian berlesen

(n) Semua peralatan yang mempunyai media storan hendaklah diperiksa terlebih dahulu bagi memastikan semua data sensitif atau perisian berlesen telah dipindahkan dan/atau dihapuskan dengan selamat terlebih dahulu sebelum peralatan tersebut dilupuskan.

20.1.6. Pengurusan Komunikasi dan Operasi

Bangunkan prosedur operasi

(a) Pengurusan komunikasi dan operasi adalah penting untuk memastikan operasi kemudahan ICT selamat dan betul. Agensi hendaklah mewujudkan pengurusan komunikasi dan operasi dengan membangunkan prosedur operasi yang bersesuaian untuk menghalang pendedahan tanpa izin, pengubahsuaian, pemindahan atau pemusnahan aset dan gangguan terhadap aktiviti *business*.

Dokumenkan prosedur operasi

(b) Agensi hendaklah memastikan prosedur operasi didokumenkan, diselenggarakan dan tersedia untuk semua pengguna.

Asingkan tugas dan beri hak akses minimum

(c) Agensi hendaklah melaksanakan pengasingan tugas dan pemberian hak akses minimum kepada pengguna bagi mengurangkan risiko terhadap kecuaian atau penyalahgunaan sistem yang disengajakan.

Kawalan perubahan

(d) Agensi hendaklah mengawal sebarang perubahan kepada kemudahan ICT dan sistem.

Pengasingan kemudahan pembangunan, ujian dan operasi

(e) Agensi hendaklah mengasingkan kemudahan pembangunan, ujian dan operasi untuk mengurangkan risiko akses tanpa izin atau perubahan kepada sistem yang sedang beroperasi.

Agensi bertanggungjawab ke atas maklumat yang diproses oleh pihak luar

(f) Agensi hendaklah sedar bahawa pada dasarnya mereka bertanggungjawab ke atas maklumat yang diproses oleh pihak luar. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak luar hendaklah dipantau, disemak semula dan diaudit secara berkala. Tindakan sewajarnya hendaklah diambil apabila terdapat kekurangan dalam penyampaian perkhidmatan.

Unjuran keperluan kapasiti masa depan

(g) Agensi hendaklah memantau, memperbaiki dan membuat unjuran keperluan kapasiti masa depan penggunaan sumber bagi memastikan prestasi sistem yang diperlukan tercapai.

Kriteria dan keperluan penerimaan sistem hendaklah ditentukan

(h) Agensi hendaklah memastikan dengan jelas kriteria dan keperluan bagi penerimaan sistem baru, dipersetujui, didokumenkan dan diuji sebelum sistem diterima. Sistem maklumat yang baru, peningkatan sistem serta versi baru hendaklah diuji dan mendapat persetujuan rasmi sebelum digunakan. Bagi pembangunan utama, pengguna dan personel operasi hendaklah dirujuk pada semua fasa pembangunan

untuk memastikan keberkesanan operasi sistem yang dicadangkan.

Melaksanakan pengesanan, pencegahan, kawalan pemulihan dan program kesedaran pengguna

(i) Agensi hendaklah melaksanakan pengesanan, pencegahan, kawalan pemulihan dan program kesedaran pengguna untuk melindungi kemudahan pemprosesan ICT dan sistem dari kod perosak. Penggunaan dua (2) atau lebih produk perisian yang melindungi dari kod perosak daripada vendor berlainan boleh meningkatkan keberkesanan perlindungan kawalan kod perosak.

(j) *Backup*

SOP bagi *backup* dan pemulihan diperlukan

(i) *Backup* diperlukan untuk mengekalkan integriti dan ketersediaan maklumat serta kemudahan pemprosesan ICT. Prosedur Operasi Standard (*Standard Operating Procedure* [SOP]) hendaklah diwujudkan untuk dijadikan panduan bagi melaksanakan kerja *backup* dan pemulihan. Ini melibatkan semua fail penting, data, program aplikasi dan dokumentasi.

Pelabelan fail *backup* dengan teratur dan jelas

(ii) Fail *backup* hendaklah dilabelkan dengan teratur dan jelas untuk mengelakkan kesilapan *overwrite* secara tidak sengaja.

Kawalan akses fail *backup*

(iii) Kawalan akses terhadap fail *backup* hendaklah dihadkan kepada personel yang diizinkan dengan rekod pengauditan yang teratur.

Kekerapan *backup*

(iv) *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung kepada tahap kritikal maklumat.

Simpan *backup* di premis luar yang selamat

(v) Agensi hendaklah mempunyai sekurang-kurangnya tiga (3) salinan *backup*. Media *backup* hendaklah disimpan dengan selamat dan di premis luar. Akses kepada lokasi storan yang dilindungi hendaklah dikawal dengan ketat daripada akses tanpa izin.

Kekerapan menguji prosedur *backup*/ pemulihan

(vi) Agensi hendaklah menguji prosedur *backup*/pemulihan dan media *backup* sekurang-kurangnya sekali setahun.

Tiga (3) generasi *backup*

(vii) Agensi hendaklah menyimpan sekurang-kurangnya tiga (3) generasi *backup*.

(k) Jejak Audit, *Alerts* dan Laporan

Keadaan di mana jejak audit diperlukan

(i) Jejak audit hendaklah disediakan apabila:

a. maklumat kritikal diakses seperti maklumat yang mempunyai hak keistimewaan, perubahan terhadap profil pengguna dan akses kepada fail-fail log;

b. perkhidmatan rangkaian diakses seperti pengesahan paket data,

aplikasi rangkaian, *Internet Protocol* (IP) tanpa wayar; dan

c. hak keistimewaan atau kuasa digunakan seperti arahan pentadbiran keselamatan, identiti pengguna dalam keadaan kecemasan, fungsi penyeliaan dan pelanggaran terhadap aliran proses normal.

Jejak audit hendaklah dilog secara berpusat

(ii) Jejak audit untuk semua peristiwa dan aktiviti kritikal hendaklah dilog secara berpusat dan integriti dilindungi dari perubahan yang disengajakan atau yang tidak disengajakan.

Log audit hendaklah mengandungi maklumat terperinci yang mencukupi

(iii) Log audit hendaklah mengandungi maklumat terperinci yang mencukupi (contoh: identiti pengguna, transaksi spesifik atau program yang dilaksanakan, fungsi, maklumat dan sumber-sumber yang digunakan atau diubah, tarikh/masa akses, maklumat terperinci mengenai perubahan, status permintaan).

Laporan audit yang komprehensif

(iv) Laporan audit yang komprehensif mengenai aktiviti pengguna dan pentadbiran keselamatan hendaklah disediakan.

Tempoh penyimpanan

(v) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh “Akta Arkib Negara”.

20.1.7. Kawalan Akses

Kawalan akses berdasarkan peranan dan keperluan keselamatan

(a) Akses kepada maklumat, proses dan kemudahan pemprosesan ICT hendaklah dikawal berdasarkan peranan dan keperluan keselamatan. Peraturan kawalan akses hendaklah mengambil kira dasar mengenai keizinan dan penyebaran maklumat.

Tentukan dan dokumenkan semua akses kepada aset ICT

(b) Semua akses kepada aset ICT hendaklah ditentukan dan didokumenkan melalui prosedur pendaftaran pengguna dan dikawal berdasarkan kepada:

(i) prinsip perlu mengetahui;

(ii) peranan;

(iii) hak akses minimum; dan

(iv) pengasingan tugas.

Kaji semula semua akses dan hak keistimewaan secara berkala

(c) Semua hak keistimewaan dan akses hendaklah dikaji semula secara berkala. Akses yang mempunyai hak keistimewaan hendaklah dihadkan dan dipantau setiap hari oleh Pegawai Keselamatan ICT.

Pantau aktiviti akses setiap hari

(d) Aktiviti akses hendaklah dipantau setiap hari untuk mengesan aktiviti luar biasa seperti cubaan berulang akses yang tidak sah yang mungkin mengancam integriti, kerahsiaan atau ketersediaan sistem.

Pengesahan pengenalan identiti sebelum akses

(e) Setiap pengguna hendaklah dikenal pasti dengan pengenalan identiti pengguna

yang unik dan hendaklah disahkan sebelum mendapat akses kepada sumber maklumat.

Keselamatan bagi aplikasi hendaklah menyokong kaedah pengesahan

(f) Keselamatan bagi aplikasi hendaklah menyokong kaedah pengesahan berikut:

(i) pengenalan identiti normal dan kata laluan; dan/atau

(ii) berdasarkan sijil *Public Key Infrastructure* (PKI).

Maklumat akses dirahsiakan

(g) Maklumat pengenalan identiti, kata laluan dan pengesahan hendaklah dirahsiakan.

Ciri-ciri aplikasi keselamatan

(h) Keselamatan bagi aplikasi hendaklah mempunyai ciri-ciri berikut:

(i) *Logoff* secara automatik apabila tiada aktiviti dalam tempoh yang ditetapkan;

(ii) Pengesahan semula pengguna yang aktif secara automatik selepas tempoh yang ditetapkan;

(iii) *Logoff* pengguna secara paksa dan batalkan dengan segera semua hak keistimewaan pengguna yang telah bertukar tugas, berpindah atau berhenti;

(iv) Tidak membenarkan lebih dari satu sesi *login* untuk setiap pengenalan pengguna;

(v) Wujud pengenalan pengguna yang unik dalam sistem;

(vi) Hentikan akaun pengguna dan pentadbir sistem keselamatan selepas maksimum tiga (3) kali gagal cubaan *login*;

(vii) Gantung hak keistimewaan pengguna selepas 30 hari (boleh diubah) sekiranya tidak digunakan dan menghapuskannya selepas 30 hari (boleh diubah) digantung penggunaan;

(viii) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

(ix) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula;

(x) Kuatkuasakan pertukaran kata laluan selepas 90 hari atau selepas suatu tempoh masa bersesuaian bergantung kepada kajian semula dasar;

(xi) Kuatkuasakan penggunaan kata laluan minimum 12 aksara dengan kombinasi aksara, angka dan aksara khas;

(xii) Cegah penggunaan semula empat (4) kata laluan yang terakhir digunakan;

(xiii) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

(xiv) Tentukan had masa pengesahan selama dua (2) minit (boleh diubah) dan selepas had itu, sesi ditamatkan; dan

(xv) Papar tarikh dan masa terakhir *login* pengguna yang berjaya dan tidak berjaya.

Pemilihan kaedah pengesahan

(i) Pegawai Keselamatan ICT hendaklah boleh memilih kaedah pengesahan secara dinamik untuk setiap aplikasi tanpa perlu merujuk kepada kod sumber aplikasi.

Prinsip perlu mengetahui

(j) Kebenaran akses secara automatik tidak boleh diberikan kepada individu walau apa jua peringkat tapisan keselamatan individu berkenaan. Dalam semua keadaan pendedahan maklumat, prinsip perlu mengetahui mengatasi segalanya.

Dasar *clear desk* dan *clear screen*

(k) Dasar *clear desk* atau *clear screen* hendaklah digunakan bagi semua media storan maklumat dan kemudahan pemprosesan ICT.

Perkara-perkara keselamatan yang perlu dipertimbangkan

(l) Agensi hendaklah mempertimbangkan untuk:

(i) mengehadkan akses sistem pengoperasian Agensi kepada pengguna yang diizinkan sahaja;

(ii) menggunakan prosedur *login* yang selamat; dan

(iii) melaksanakan kawalan masa hubungan bagi aplikasi komputer yang sensitif terutama dari lokasi yang berisiko tinggi.

Persekitaran pengkomputeran yang khusus bagi sistem sensitif

(m) Agensi hendaklah mengehadkan akses logikal terhadap perisian aplikasi dan maklumat kepada pengguna yang diizinkan. Persekitaran pengkomputeran yang khusus hendaklah disediakan bagi sistem yang sensitif.

20.1.8. <u>Perolehan, Pembangunan dan Penyelenggaraan Sistem ICT</u>

Keperluan keselamatan hendaklah dipersetujui sebelum dibangunkan

(a) Sistem ICT terdiri daripada perkakasan, infrastruktur rangkaian, perisian termasuk sistem pengoperasian, aplikasi pengguna, produk *off-the-shelf* dan perkhidmatan. Keperluan keselamatan hendaklah dikenal pasti, dipersetujui dan didokumenkan terlebih dahulu semasa fasa mengkaji keperluan projek sebelum pembangunan dan pelaksanaan sistem ICT.

Sahkan input data

(b) Input data kepada aplikasi hendaklah disahkan untuk memastikan data betul dan sesuai.

Aplikasi hendaklah mengandungi semakan pengesahan

(c) Aplikasi hendaklah mengandungi semakan pengesahan untuk mengesan sebarang kerosakan maklumat akibat dari kesilapan pemprosesan atau perbuatan yang disengajakan.

Semak output

(d) Output yang dikeluarkan dari sistem aplikasi perlu disahkan untuk memastikan maklumat adalah betul.

Prosedur bagi mengawal pemasangan perisian

(e) Prosedur untuk mengawal pemasangan perisian ke dalam sistem yang beroperasi hendaklah diwujudkan.

Prosedur kawalan perubahan

(f) Pelaksanaan perubahan hendaklah dikawal dengan menggunakan prosedur rasmi kawalan perubahan.

Data ujian

(g) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.

Pengujian perisian baru dilaksanakan dalam persekitaran berasingan

(h) Agensi hendaklah mengamalkan pengujian perisian baru termasuk *patches*, *service packs* dan pengemaskinian-pengemaskinian lain, dalam persekitaran yang berasingan dari persekitaran pembangunan dan operasi. Pengemaskinian secara automatik terhadap sistem hendaklah dielakkan.

Kaji semula dan uji aplikasi kritikal apabila terdapat perubahan sistem pengoperasian

(i) Aplikasi kritikal hendaklah dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan buruk terhadap operasi atau keselamatan. Satu kumpulan spesifik atau individu tertentu hendaklah diberi tanggungjawab memantau pengeluaran produk *patches* dan *fixes*.

Had akses kepada kod sumber program

(j) Akses kepada kod sumber program hendaklah dihadkan kepada pengguna yang diizinkan untuk mencegah fungsi aplikasi ditambah tanpa izin dan bagi mengelakkan perubahan yang tidak disengajakan.

Selia dan pantau pembangunan perisian yang di*outsource*

(k) Agensi hendaklah menyelia dan memantau pembangunan perisian yang dio*utsource*.

20.1.9. Pengurusan Insiden Keselamatan ICT

Prosedur rasmi pelaporan insiden keselamatan ICT

(a) Agensi hendaklah memastikan insiden keselamatan ICT dan kelemahan sistem ICT dilaporkan dengan segera untuk tindakan pemulihan melalui prosedur rasmi pelaporan insiden keselamatan ICT berdasarkan:

(i) "Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi"; dan

(ii) "Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam".

Prosedur melaporkan insiden dan keselamatan

(b) Semua personel, kontraktor dan pengguna pihak ketiga hendaklah diberitahu mengenai prosedur bagi melaporkan insiden dan kelemahan.

Laporkan sebarang kelemahan keselamatan ICT yang diperhatikan atau disyaki

(c) Semua personel, kontraktor dan pengguna pihak ketiga dikehendaki untuk mengambil maklum dan melaporkan dengan segera sebarang kelemahan keselamatan ICT yang diperhatikan atau disyaki kepada Pegawai Keselamatan ICT.

Insiden hendaklah dilaporkan dengan segera kepada Pegawai Keselamatan ICT dan CERT Agensi/ GCERT MAMPU

(d) Insiden berikut hendaklah dilaporkan dengan segera kepada Pegawai Keselamatan ICT dan CERT Agensi/ GCERT MAMPU:

(i) Kehilangan atau pendedahan maklumat tanpa izin;

(ii) Kehilangan atau pendedahan maklumat tanpa izin yang disyaki*;*

(iii) Penggunaan sistem ICT tanpa izin atau penggunaan sistem ICT tanpa izin yang disyaki;

(iv) Kehilangan atau kehilangan yang disyaki, kecurian, pendedahan tanpa izin mekanisme kawalan akses atau kata laluan;

(v) Aktiviti sistem yang luar biasa seperti kehilangan fail, kerosakan sistem yang kerap dan *misrouted messages;* dan

(vi) Percubaan untuk menceroboh sistem ICT dan insiden keselamatan yang tidak dijangka.

Kepentingan bukti

(e) Bukti hendaklah dikumpulkan, disimpan dan diserahkan kepada pihak berkuasa yang berkaitan untuk tindakan susulan tatatertib dan/atau tindakan undang-undang.

20.1.10. Pengurusan Kesinambungan *Business*

Objektif BCM

(a) Objektif Pengurusan Kesinambungan *Business* (*Business Continuity Management* [BCM]) adalah untuk memastikan kesinambungan fungsi kritikal *business* dan kemudahan pemprosesan ICT dipulihkan dengan segera selepas berlaku gangguan.

Kenal pasti gangguan, impak dan akibat

(b) Peristiwa yang boleh mengakibatkan gangguan terhadap proses *business* hendaklah dikenal pasti bersama-sama dengan kebarangkalian dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT.

Penglibatan sepenuhnya pengurusan atasan agensi

(c) Pengurusan atasan Agensi hendaklah terlibat secara sepenuhnya dalam aktiviti penilaian risiko kesinambungan *business*.

Bangunkan strategi BCM

(d) Berdasarkan hasil penilaian risiko, strategi BCM hendaklah dibangunkan untuk menentukan pendekatan keseluruhan terhadap kesinambungan *business*.

Kelulusan strategi BCM

(e) Pengurusan atasan Agensi hendaklah meluluskan strategi BCM yang dibangunkan.

Isi kandungan pelan BCM

(f) Pelan BCM yang akan dibangunkan hendaklah mengandungi sekurang-kurangnya perkara-perkara berikut:

(i) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

(ii) Senarai personel dalaman dan dari vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk menangani insiden;

(iii) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya dengan arahan pemulihan maklumat dan kemudahan yang berkaitan;

(iv) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

(v) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Simpan pelan BCM di lokasi berasingan

(g) Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.

Kekerapan pengujian pelan BCM

(h) Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi *business* untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Jadualkan pengujian pelan BCM

(i) Agensi hendaklah menjadualkan ujian pelan BCM untuk memastikan semua ahli dalam pasukan pemulihan dan personel yang terlibat memahami pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

Pelan BCM dikemas kini

(j) Agensi hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

Pemilik pelan BCM

(k) Agensi hendaklah menentukan pemilik pelan BCM.

20.1.11. Pematuhan

Prosedur bersesuaian untuk memastikan pematuhan

(a) Reka bentuk, operasi, penggunaan dan pengurusan sistem ICT mungkin tertakluk kepada keperluan *statutory, regulatory* dan/atau kontrak. Prosedur yang bersesuaian hendaklah dilaksanakan untuk memastikan pematuhan kepada keperluan *statutory, regulatory* dan kontrak bagi penggunaan sistem.

Semakan pematuhan oleh pegawai yang kompeten dan yang diizinkan

(b) Agensi perlu memastikan semua prosedur keselamatan di bawah

tanggungjawab mereka dilaksanakan dengan betul dan hendaklah disemak secara berkala untuk mencapai pematuhan kepada dasar dan standard keselamatan ICT. Semakan pematuhan teknikal hendaklah dilaksanakan oleh individu yang kompeten dan yang diizinkan atau dilaksanakan di bawah penyeliaan mereka.

Rekod penting perlu dilindungi

(c) Rekod penting seperti maklumat kontrak, lesen, bayaran dan maklumat peribadi perlu dilindungi daripada pendedahan, kehilangan, kemusnahan dan pemalsuan selaras dengan keperluan *business*, *statutory* dan kontrak.

Dasar perlindungan data dan privasi

(d) Agensi hendaklah membangunkan dan melaksanakan dasar perlindungan data dan privasi serta memaklumkannya kepada semua individu yang terlibat dalam pemprosesan maklumat peribadi.

Data digunakan hanya untuk tujuan yang ditetapkan

(e) Agensi hendaklah memastikan bahawa data digunakan hanya untuk tujuan yang telah ditetapkan bagi melindungi privasi maklumat peribadi.

Pengekalan dan pemusnahan rekod mematuhi "Akta Arkib Negara 2003"

(f) Agensi perlu memastikan bahawa sistem untuk penyimpanan dan pengendalian maklumat mempunyai rekod pengenalan identiti yang jelas dan tempoh pengekalan serta membenarkan pemusnahan rekod yang bersesuaian selepas tempoh tersebut, sekiranya rekod tidak lagi diperlukan oleh Agensi sebagaimana yang ditetapkan oleh "Akta Arkib Negara 2003".

BAB IV: PENGURUSAN REKOD ELEKTRONIK

21. Pendahuluan

Kepentingan pengurusan rekod elektronik

21.1. Agensi perlu menyimpan rekod-rekod yang berkaitan dengan keputusan dan transaksi Agensi bagi memenuhi keperluan akauntabiliti. Rekod-rekod yang diwujudkan dalam urusan kerja harian Kerajaan perlu ditawan, diurus dan dipelihara dalam satu sistem yang terancang yang mengekalkan integriti dan kesahihannya, di samping mengekalkan nilai-nilai asal sebagai rekod organisasi yang boleh dicapai semula dan boleh digunakan sebagai bahan bukti utama. Rekod-rekod elektronik boleh wujud dalam pelbagai bentuk dan format seperti e-mel, bunyi digital dan video, laman web, model realiti maya dan sebagainya.

Aktiviti pengurusan rekod tertakluk kepada "Akta Arkib Negara 2003" dan dokumen-dokumen lain

21.2. Aktiviti pengurusan rekod di Agensi adalah tertakluk kepada "Akta Arkib Negara 2003", surat-surat pekeliling dan garis panduan yang berkaitan serta keperluan *business* dan operasi organisasi berkenaan.

22. Objektif

Bab ini menyediakan garis panduan bagi keperluan minimum berkaitan pewujudan, pengelasan, storan, akses, pemeliharaan dan pelupusan rekod elektronik.

23. Skop

Skop pengurusan rekod elektronik

23.1. Skop bab ini merangkumi bidang-bidang berikut:

23.1.1. Perolehan Sistem Pengurusan Rekod Elektronik (ERMS);

23.1.2. Prasyarat untuk pelaksanaan ERMS;

(a) Sistem Pengelasan Fail; dan

(b) Jadual Pelupusan Rekod.

23.1.3. Pewujudan Rekod Elektronik – Keperluan Metadata;

23.1.4. Penyelenggaraan; dan

23.1.5. Pelupusan

(a) Pemindahan Rekod; dan

(b) Pemusnahan Rekod.

24. Perolehan Sistem Pengurusan Rekod Elektronik (ERMS)

Sistem Pengurusan Rekod Elektronik

Agensi adalah digalakkan memperoleh ERMS untuk mewujudkan dan menguruskan semua rekod elektronik. Semua ERMS mesti mematuhi keperluan mandatori yang dinyatakan di dalam "Functional Specifications for ERMS" yang dikeluarkan oleh Arkib Negara Malaysia.

25. Prasyarat untuk Pelaksanaan ERMS

25.1. Agensi hendaklah membangunkan Sistem Pengelasan Fail dan Jadual Pelupusan Rekod sebagai prasyarat untuk pelaksanaan ERMS. Agensi digalakkan mendapatkan nasihat daripada Arkib Negara Malaysia.

25.1.1. Sistem Pengelasan Fail

Hierarki pengelasan fail

Hierarki pengelasan fail apabila digunakan di dalam sistem maklumat Agensi, boleh memudahkan penawanan, pemberian tajuk, dapatan semula, penyelenggaraan dan pelupusan rekod.

25.1.2. Jadual Pelupusan Rekod

Jadual rekod mesti dikekalkan dan boleh diakses

Jadual yang menunjukkan tempoh masa sesuatu rekod mesti dikekalkan dan boleh diakses. Di akhir tempoh pengekalan, rekod hendaklah sama ada dipindahkan ke Arkib Negara Malaysia atau dimusnahkan.

26. Pewujudan Rekod Elektronik

Metadata ditetapkan dan ditawan bersama-sama semasa pewujudan

26.1. Rekod hendaklah ditawan secara elektronik ke dalam sistem yang mempunyai keupayaan pengurusan rekod untuk menyokong proses kerja. Metadata hendaklah ditetapkan dan ditawan bersama-sama rekod bermula dari masa pewujudannya (rujuk “Standard Metadata Sistem Pengurusan Rekod Elektronik Sektor Awam” yang disediakan oleh Arkib Negara Malaysia).

Keperluan pewujudan dan penawanan rekod

26.2. Dalam mewujud dan menawan rekod, Agensi hendaklah menyediakan perkara-perkara berikut:

26.2.1. Proses untuk mengenal pasti maklumat bersesuaian yang perlu ditawan dalam persekitaran kerja;

26.2.2. Mekanisme yang boleh berfungsi dengan semua aplikasi pewujudan rekod bagi membolehkan penawanan semua elemen rekod mengikut format dan standard yang diluluskan; dan

26.2.3. Hubung kait dengan rekod-rekod lain termasuk rekod elektronik dan kertas dalam klasifikasi-klasifikasi yang lain hendaklah diwujudkan dan dikekalkan.

26.3. Keperluan Metadata

Keterangan metadata

26.3.1. Metadata adalah data yang menerangkan konteks, kandungan dan struktur rekod serta pengurusannya. Metadata membolehkan pengguna mengawal, mengurus, mencari, memahami dan memelihara rekod.

Contoh-contoh metadata

26.3.2. Contoh-contoh metadata adalah:

(a) tajuk rekod;

(b) subjek yang diliputi;

(c) format rekod;

(d) tarikh rekod diwujudkan;

(e) sejarah penggunaan rekod; dan

(f) perincian mengenai pelupusan.

Kategori utama metadata

26.3.3. Dua (2) kategori utama metadata yang digunakan untuk menguruskan rekod elektronik adalah metadata pengurusan rekod dan metadata arkib. Dalam mengenal pasti dan menawan metadata yang berkaitan, Agensi hendaklah merujuk kepada “Standard Metadata Pengurusan Rekod Elektronik Sektor Awam” yang disediakan oleh Arkib Negara Malaysia.

27. Penyelenggaraan

Pertimbangan dalam penyimpanan rekod elektronik

27.1. Bagi menyimpan rekod elektronik untuk jangka masa yang lama, Agensi hendaklah mempertimbangkan perkara-perkara berikut:

27.1.1. peranti storan yang sesuai;

27.1.2. kemudahan tempat penyimpanannya; dan

27.1.3. sistem-sistem komputer yang menjana rekod.

Persekitaran dan keadaan storan

27.2. Keadaan storan hendaklah menyokong perlindungan rekod, mudah diakses dan kos efektif. Keadaan persekitaran yang stabil adalah perlu bagi melindungi peranti storan digital yang mudah terdedah kepada perubahan kelembapan, suhu dan *radiation*.

Pemeriksaan secara berkala

27.3. Agensi hendaklah menjalankan pemeriksaan secara berkala dan berterusan serta semakan integriti ke atas semua peranti storan digital dan kandungannya bagi memastikan tiada *deterioriation* atau kerosakan data berlaku.

Keadaan storan yang bersesuaian

27.4. Agensi hendaklah mendapatkan nasihat berkaitan keadaan storan yang sesuai bagi sistem komputer dan maklumat serta peranti storan digital serta aspek-aspek lain pengurusan rekod elektronik daripada Arkib Negara Malaysia.

Ciri-ciri pengurusan rekod

27.5. Agensi hendaklah sentiasa memastikan supaya:

27.5.1. rekod wujud – maklumat berkaitan semua aktiviti dan transaksi direkodkan;

27.5.2. rekod boleh diakses – boleh dikesan, diakses dan mempersembahkan maklumat sebagaimana bentuk asal;

27.5.3. rekod boleh diinterpretasikan – boleh membuktikan bila, di mana, dan siapa yang mewujudkannya, bagaimana rekod digunakan dan kaitannya dengan maklumat yang lain;

27.5.4. rekod boleh dipercayai – maklumat dan pernyataannya benar-benar menepati seperti yang telah diwujudkan dan digunakan, dan integriti serta kesahihannya tidak boleh disangkal;

27.5.5. rekod boleh diselenggarakan – rekod boleh dipersembahkan, diakses, ditafsirkan dan dipercayai selagi diperlukan, walaupun telah dipindahkan ke lokasi, sistem dan teknologi lain yang diluluskan;

27.5.6. migrasi data dilakukan apabila terdapat perubahan teknologi untuk memastikan rekod boleh diakses; dan

27.5.7. pangkalan data yang usang diuruskan dengan cara khusus. Agensi digalakkan untuk mendapatkan nasihat daripada Arkib Negara Malaysia mengenai cara terbaik pemeliharaan pangkalan data yang usang.

27.6. Penjagaan Media Elektronik

Langkah-langkah pencegahan

Agensi hendaklah mempertimbangkan langkah-langkah pencegahan bagi memelihara media elektronik untuk jangka masa panjang dalam memastikan pengaksesan yang berterusan. Langkah-langkah pencegahan tersebut adalah seperti berikut:

27.6.1. Kawalan Persekitaran

(a) Simpan cakera dan pita dalam kedudukan menegak dalam persekitaran bebas habuk.

(b) Simpan cakera dan pita pada kadar suhu yang tetap antara 18˚C–20˚C dan kelembapan bandingan yang tetap antara 35%–45%. Perubahan kadar suhu dan kelembapan yang kerap atau ekstrem akan mempercepatkan kerosakan pita.

27.6.2. Kawalan Media

(a) Elakkan penggunaan cakera liut untuk penyimpanan rekod jangka panjang atau kekal.

(b) Selenggara salinan pendua dalam persekitaran storan yang terkawal, berasingan dari lokasi asal.

(c) Laksanakan ujian tahunan sampel statistik pita dan cakera magnetik bagi mengenal pasti sebarang kehilangan data, mengesan dan memperbetulkan punca kehilangan data.

(d) Pastikan pemacu cakera dan pita dalam keadaan bersih.

(e) Pastikan cakera dan pita disimpan jauh dari medan elektrik dan magnet yang kuat, termasuk telefon.

(f) Pastikan individu tanpa izin tidak dibenarkan mengakses komputer, pita, cakera dan dokumen.

28. Pelupusan

28.1. Pemindahan Rekod Elektronik

Pemindahan rekod elektronik ke Arkib Negara Malaysia

Agensi hendaklah mengikut garis panduan dan prosedur pemindahan rekod elektronik yang telah ditetapkan oleh Arkib Negara Malaysia.

28.2. Pemusnahan Rekod Elektronik

Kelulusan bertulis bagi pemusnahan rekod elektronik

28.2.1. Agensi tidak boleh memusnahkan atau memberi kelulusan pemusnahan rekod awam di bawah jagaan atau kawalannya tanpa memperoleh kelulusan bertulis terlebih dahulu daripada Ketua Pengarah, Arkib Negara Malaysia.

Pemformatan semula media dengan selamat

28.2.2. Agensi hendaklah menyedari bahawa penghapusan rekod daripada storan cakera adalah tidak sama dengan pemusnahan rekod. Dokumen masih boleh dicapai semula kecuali proses memformatkan semula media dilakukan dengan lengkap dan selamat. Jika lebih daripada satu (1) salinan rekod wujud, semua salinan termasuk salinan asal dan salinan kerja hendaklah dimusnahkan pada masa yang sama.

28.3. Kaedah-kaedah Pemusnahan

Cadangan kaedah pemusnahan

28.3.1. Terdapat beberapa kaedah pemusnahan yang sesuai bagi media storan yang berbeza. Agensi hendaklah melaksanakan langkah-langkah berikut:

(a) Media Magnetik

(i) Memadam secara keseluruhan media magnetik dengan mendedahkannya kepada medan magnetik yang kuat; dan

(ii) Memformatkan semula media magnetik untuk pemusnahan yang selamat dan penggunaan semula.

(b) Media Optik

(i) Memotong, menghancur atau kaedah-kaedah pemusnahan fizikal media optik yang lain; dan

(ii) Memformatkan semula *rewritable optical disk* bagi pelupusan atau penggunaan semula.

(c) Cakera Keras

Memformatkan semula cakera keras komputer peribadi dan pelayan sebelum melupuskannya.

Pertimbangan-pertimbangan bagi pemusnahan rekod

28.3.2. Agensi hendaklah memastikan pemusnahan rekod adalah:

(a) Bersesuaian

(i) Tidak boleh diubah lagi - pemusnahan rekod hendaklah tidak boleh diubah atau diterbalikkan bagi memastikan maklumat tidak boleh diperoleh semula; dan

(ii) Mesra alam – rekod hendaklah dimusnahkan dalam keadaan mesra alam.

(b) Tepat Pada Masanya

Rekod hendaklah dimusnahkan dalam tempoh 14 hari dari tarikh memperoleh kelulusan daripada Arkib Negara Malaysia.

(c) Didokumenkan

Pemusnahan bagi semua rekod hendaklah didokumenkan.

RUJUKAN

1. Arkib Negara Malaysia, 2003. “Akta Arkib Negara 2003. (Akta 629)”. Kuala Lumpur: Percetakan Nasional Berhad

2. Pejabat Ketua Pegawai Keselamatan Kerajaan, 2007. “Arahan Keselamatan 2007”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

3. Kementerian Kewangan. “Arahan Perbendaharaan 2007”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

4. Arkib Negara Malaysia, 2004. “Standard Metadata Sistem Pengurusan Rekod Elektronik Sektor Awam”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

5. Arkib Negara Malaysia, 2004. “Garis Panduan Am Pengurusan Rekod Elektronik Sektor Awam”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

6. Arkib Negara Malaysia, 2004. “Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

7. Suruhanjaya Komunikasi dan Multimedia Malaysia. “Akta Tandatangan Digital 1997. (Akta 562)”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

8. National Institute of Standards and Technology, 2001. “Security Requirements For Cryptographic Modules”. Washington: United States of America Government Printing Office

9. Hansche, S., Berti, J., Hare, C., 2004. “Official (ISC)2 Guide To CISSP Exam”. Amerika Syarikat: Auerbach Publications

10. International Organization for Standardization, 2001. “ISO 15489: Information and Documentation – Records Management – Part 1: General”, [Online]. Didapati di: http://www.iso.org/iso/iso_catalogue/catalogue_tc/cataloguedetail.htm?csnumber=31908

11. Kew, Richmond, Surrey, Second Edition 1999. Public Record Office: “Guidelines For Management, Appraisal and Preservation of Electronic Records Volume 2: Procedures (EROS)”, [Online]. Didapati di: http://www.nationalarchives.gov.uk/documents/procedures.pdf

12. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 1 Julai 1997. “Electronic Government Information Technology Policy & Standards (EGIT). Version 1.0”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

13. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 1 Jun 2007. “Pekeliling MAMPU – Langkah-Langkah mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

14. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 15 Januari 2002. “The Malaysian Public Sector Management of ICT Security Handbook (MyMIS). Version 2”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

15. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 20 Oktober 2006. “Arahan KSN – Langkah-Langkah Untuk Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

16. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 1 Oktober 2000. “Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

17. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 4 April 2001. “Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

18. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 7 November 2005. “Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

19. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 9 November 2006. “Surat Pekeliling Am Bilangan 4 Tahun 2006 Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

20. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 28 November 2003. “Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

21. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 31 Januari 2007. “Surat Arahan KSN – Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Alat-Alat Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensi-agensi Kerajaan”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

22. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 6 November 2006. “Pekeliling Am Bilangan 1 Tahun 2006 – Pengurusan Laman Web/Portal Sektor Awam”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

23. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, April 2006. “OSS Implementation Guideline”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

24. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, Ogos 2003. “Channel Framework. Version 1.0”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

25. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, Ogos 2003. “Malaysian Government Interoperability Framework (MyGIF). Version 1.0”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

26. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, Februari 2006. “Malaysian Government Interoperability Framework for Open Source Software (MyGIFOSS)”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

27. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, Januari 2005. “Malaysian Public Sector Open Source Software (OSS) Master Plan”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

28. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU, 2006. “Open Source Software (OSS) Policy Handbook”. Kuala Lumpur: Percetakan Nasional Malaysia Berhad

29. Arkib Negara Australia, Mei 2004. “Digital Recordkeeping – Guidelines for Creating, Managing and Preserving Digital Records”, [Online]. Didapati di: http://www.naa.gov.au/records-management/publications/Digital-recordkeeping-guidelines.aspx

30. Tipton, H.F., Krause, M., 2003. “Information Security Management Handbook Volume 4, 4th ed”. Amerika Syarikat: Auerbach Publications

31. Kerajaan United Kingdom, Julai 2001. “E-Government Policy Framework for Electronic Records Management. Version 2.0”. United Kingdom: United Kingdom Government Printed Office