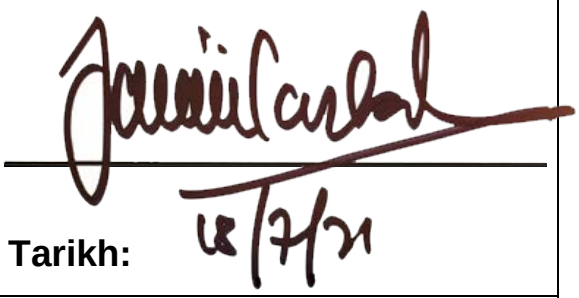
DASAR KESELAMATAN ICT

JABATAN PENGANGKUTAN JALAN MALAYSIA

VERSI 3.0

BAHAGIAN TEKNOLOGI DIGITAL

A. INFORMASI DOKUMEN

Jenis Dokumen:	Versi Dokumen:	Tarikh Berkuatkuasa:
Manual Keselamatan	3.0	1 Januari 2021
Disediakan Oleh:	**Disemak Oleh:**	**Diluluskan Oleh:**
Urus setia DKICT	i. CIO ii. Pengurus ICT iii. ICTSO	Dato' Zailani Haji Hashim Ketua Pengarah Jabatan Pengangkutan Jalan Malaysia  Tarikh: 12/7/21
Pengedaran Dokumen: JPJ		

B. SEJARAH DOKUMEN

KELUARAN/ PINDAAN	TARIKH	KELULUSAN OLEH	TARIKH KUATKUASA
1.0	9 September 2011	JPICT Bil. 2/2011	9 September 2011
2.0	28 Disember 2016	JPICT Bil. 3/2016	28 Disember 2016
3.0	17 Disember 2020	JPICT Bil. 3/2020	1 Januari 2021

C. JADUAL PINDAAN

TARIKH	PERKARA	BUTIRAN PINDAAN
9 September 2011	**Salinan Pertama**	**-**
28 Disember 2016	**Salinan Kedua**	**Pindaan keseluruhan Bidang Keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2013 *Information Security Management System* (ISMS)**
23 September 2020	**Salinan Ketiga**	**i. Pindaan keseluruhan Bidang Keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2013 *Information Security Management System* (ISMS)** **ii. Bidang keselamatan maklumat dan digital terkini:** • Tajuk Mekanisma Pelaporan Insiden Keselamatan ICT selari dengan Rangka Kerja Keselamatan Siber Sektor Awam • Tajuk Peralatan Mudah Alih menyokong konsep "*Bring Your Own Device"* • Tajuk Kerja Jarak Jauh dikemaskini dengan Aplikasi Mesyuarat Jarak Jauh dan Aplikasi Perhubungan Sosial • Tajuk Perkomputeran Awan (Cloud Computing) • Tajuk Capaian Jarah Jauh dipertingkatkan dengan teknologi *Virtual Private Network* (VPN)

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT JPJ (DKICT JPJ) sebuah dokumentasi yang mengandungi peraturan-peraturan yang perlu dibaca, difahami dan dipatuhi dalam urusan penggunaan dan pengendalian aset Teknologi Maklumat dan Komunikasi (ICT) JPJ.

Dasar ini juga menerangkan kepada semua pengguna di JPJ mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JPJ.

OBJEKTIF DKICT JPJ

Dasar Keselamatan ICT JPJ (DKICT JPJ) diwujudkan untuk menjamin kesinambungan penyampaian perkhidmatan JPJ dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Keselamatan ICT JPJ ialah seperti berikut:

a) Memastikan kelancaran perkhidmatan JPJ dan meminimumkan kerosakan atau kemusnahan;
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DKICT JPJ

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT JPJ berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. KeselamatanICT JPJ berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT JPJ merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a) **Kerahsiaan**
Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b) **Integriti**
Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

c) **Tidak Boleh Disangkal**

Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d) **Kesahihan**

Data dan maklumat hendaklah dijamin kesahihannya; dan

e) **Ketersediaan**

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT JPJ hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT JPJ, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul, dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP DKICT JPJ

Dasar ini meliputi semua sumber atau aset ICT JPJ yang digunakan seperti Maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan sistem perisian) dan fizikal (contoh: *mainframe*, *server*, komputer, peralatan komunikasi dan media storan).

Dasar ini adalah terpakai oleh semua pengguna di JPJ termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT JPJ.

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

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

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

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

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan JPJ contohnya komputer, *server*, peralatan komunikasi dan sebagainya;

b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT contohnya perisian aplikasi atau perisian sistem seperti system pengoperasian, sistem pengkalan data, perisian system rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada JPJ;

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain;

d) Data atau Maklumat

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

e) Manusia

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

f) Permis Komputer dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) di atas.

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

PRINSIP-PRINSIP DKICT JPJ

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT JPJ dan perlu dipatuhi adalah seperti berikut:

a) AKSES ATAS DASAR PERLU MENGETAHUI

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna JPJ tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan petikan perenggan 53, muka surat 15;

53. Dokumen terperingkat yang dikeluarkan sebagai panduan tetap mestilah bertulis dengan salah satu peringatan mengikut peringkatnya di kulit luar dan muka tajuk seperti berikut :

a) Rahsia Besar

"Dokumen ini ialah hak milik Kerajaan Malaysia/Negeri.....dan dimaksudkan bagi makluman..... sendiri dan lain-lain pegawai yang perlu mengetahui kandungannya dalam masa menjalankan tugas-tugas rasmi mereka, maklumat yang terkandung dalam dokumen ini tidak boleh diberitahu secara langsung atau tidak kepada akhbar atau sesiapa yang tidak dibenarkan",

b) Rahsia atau Sulit

"Dokumen ini ialah hak milik Kerajaan Malaysia/Negeri.....dan Dimaksudkan bagi makluman orang-orang yang perlu mengetahui kandungannya dalam masa menjalankan tugas-tugas rasmi mereka.Maklumat yang terkandung dalam dokumen ini tidak boleh diberitahu secara langsung atau tidak kepada akhbar atau sesiapa yang tidak dibenarkan",

c) *Terhad*

"Maklumat yang terkandung dalam dokumen ini tidak boleh diberitahu secara langsung atau tidak kepada akhbar atau sesiapa yang tidak dibenarkan",

d) Selain daripada peringatan-peringatan dalam perenggan 53(a),(b) dan (c), dokumen tersebut hendaklah juga mengandungi kenyataan tambahan berikut:

"Sesiapa yang menjumpai dokumen ini adalah dikehendaki oleh undang-undang menyerahkannya kepada Pejabat Daerah, Balai Polis atau Pejabat Angakatan Tentera untuk dihantar kepada Pejabat Pegawai Keselamatan Kerajaan berserta dengan keterangan-keterangan termasuk tarikh,masa,tempat dan bagaimana dijumpai.Menyimpan atau membinasakan dokumen ini denganb tiada kebenaran adalah suatu kesalahan di bawah Akta Rahsia Rasmi, 1972".

Petikan Arahan Keselamatan Perenggan 53

b) HAK AKSES MINIMUM

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja (read-only). Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari masa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c) AKAUNTABILITI

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT JPJ. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) PENGASINGAN

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e) PENGAUDITAN

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, *server*, *router*, *firewall* dan rangkaian hendaklah dipastikan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) PEMATUHAN

Dasar Keselamatan ICT JPJ hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT dan kesinambungan perkhidmatan Jabatan;

g) PEMULIHAN

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan keboleh capaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan Pelan Pemulihan Bencana dan Kesinambungan Perkhidmatan; dan

h) SALING BERGANTUNGAN

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisma keselamatan adalah perlu bagi menjamin keselamatan dan kesinambungan perkhidmatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

JPJ hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kelemahan yang semakin meningkat hari ini. Justeru itu, JPJ perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

JPJ hendaklah sentiasa melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Ianya diikuti dengan tindakan susulan dan/atau langkah-langkah yang bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan keatas sistem maklumat JPJ termasuklah aplikasi, perisian, *server*, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

JPJ bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat dan Sektor Awam.

JPJ perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 01
PEMBANGUNAN DAN PENYELENGGARAAN DASAR

P01/01 DASAR KESELAMATAN ICT

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JPJ dan perundangan berkaitan.

KENYATAAN	TINDAKAN
P01/01/01 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah Pengangkutan JalanMalaysia dan turut dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian/Negeri.	Ketua Pengarah
P01/01/02 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna ICT JPJ termasuk juga kakitangan di ibu pejabat/cawangan/negeri, rakan niaga, pembekal, pakar runding dan sebagainya.	ICTSO
P01/01/03 Penyelenggaraan Dasar	
Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan, kepentingan Jabatan serta pelanggan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT JPJ: a) Kenalpasti dan tentukan perubahan yang diperlukan;	ICTSO

b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) JPJ; c) Maklum kepada semua pengguna melalui medium penyebaran yang sesuai bagi perubahan yang telah dipersetujui oleh JPICT; dan d) Dasar ini hendaklah dikaji semula sekurang-kurangnya 3 tahun sekali atau mengikut keperluan semasa.	
P01/01/04 Pengecualian Dasar	
Dasar Keselamatan ICT JPJ adalah terpakai kepada semua pengguna ICT JPJ dan tiada pengecualian diberikan.	Semua

PERKARA 02
ORGANISASI KESELAMATAN

P02/01 STRUKTUR ORGANISASI KESELAMATAN

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT JPJ.

KENYATAAN	TINDAKAN
P02/01/01 Ketua Pengarah	
Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a) Memastikan semua pengguna JPJ memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT JPJ; b) Memastikan semua pengguna JPJ mematuhi Dasar Keselamatan ICT JPJ; c) Memastikan semua keperluan Jabatan (sumber kewangan, sumber kakitangan dan lain-lain sumber serta perlindungan keselamatan) adalah mencukupi; d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JPJ; dan e) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), JPJ.	Ketua Pengarah
P02/01/02 Ketua Pegawai Maklumat (CIO)	
Timbalan Ketua Pengarah Operasi (O) Jabatan Pengangkutan Jalan Malaysia adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab CIO adalah seperti berikut: a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT;	*Chief Information Officer* (CIO)

c) Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JPJ.	
P02/01/03 Pengurus ICT	
Pengarah Bahagian Teknologi Digital JPJ adalah merupakan Pengurus ICT JPJ. Peranan dan tanggungjawab PengurusICT adalah seperti berikut: a) Memahami dan mematuhi Dasar Keselamatan ICT JPJ; b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JPJ; c) Memberikan keputusan akhir kawalan akses semua pengguna JPJ terhadap aset ICT JPJ; d) Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JPJ.	Pengarah Bahagian Teknologi Digital
P02/01/04 Pegawai Keselamatan ICT (ICTSO)	
Jawatan ICTSO bagi Jabatan disandang oleh Pegawai yang bertanggungjawab ke atas ICT. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Mengurus keseluruhan program-program keselamatan ICT JPJ; b) Menguatkuasakan Dasar Keselamatan ICT JPJ; c) Memastikan semua pengguna JPJ memahami dan mematuhi Dasar Keselamatan ICT; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICTJPJ; e) Menjalankan pengurusan risiko;	*Information and Communication Technology Security Officer* (ICTSO)

f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN) dan memaklumkannya kepada CIO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j) Memperakui proses pengambilan tindakan Tatatertib ke atas pengguna JPJ yang melanggar Dasar Keselamatan ICT JPJ; dan k) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
P02/01/05 Pentadbir Sistem ICT	
Pegawai Teknologi Maklumat, Bahagian Teknologi Digital JPJ adalah Pentadbir Sistem ICT JPJ. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JPJ; c) Memantau aktiviti capaian harian pengguna JPJ; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan seterusnya mengambil langkah-langkah untuk membatal atau memberhentikan aktiviti berkenaan dengan serta merta; e) Menyimpan dan menganalisa rekod *audit trail*;	PTMK/PTM Aplikasi, PTMK/PTM Teknikal dan PPTMK/PPTM Negeri/ Cawangan

f) Menyediakan laporan mengenai aktiviti capaian maklumat yang tidak normal kepada pemilik sumber maklumat; dan g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
P02/01/06 Pengguna JPJ	
Peranan dan tanggungjawab pengguna JPJ adalah seperti berikut: a) Memahami dan mematuhi Dasar Keselamatan ICT JPJ; b) Mengetahui dan memahami implikasi keselamatan ICT akibat tidak mematuhi Dasar Keselamatan ICT JPJ; c) Lulus tapisan keselamatan; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT JPJ dan menjaga kerahsiaan maklumat JPJ; e) Melaksanakan langkah-langkah perlindungan keselamatan seperti berikut: i. Menghalang pendedahan maklumat terperingkat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosidur langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan serta merta; g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT JPJ.	Pengguna dan Pihak Ketiga

P02/01/07 Jawatankuasa Keselamatan ICT (JKICT) JPJ	
Jawatankuasa di Peringkat Jabatan **Pengerusi**: CIO **Ahli**: • Pengurus ICT • ICTSO • Pentadbir Sistem ICT • Pegawai Teknologi Maklumat **Urus setia**: Bahagian/Seksyen/Unit Bidang Kuasa: a) Memantau tahap pematuhan keselamatan ICT; b) Menilai aspek teknikal keselamatan projek-projek ICT; c) Memperakukan dan meluluskan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT JPJ; d) Memastikan sistem ICT sentiasa mematuhi keperluan keselamatan dari masa ke semasa; e) Menilai kesesuaian teknologi untuk keperluan keselamatan ICT; f) Memastikan DKICT JPJ selaras dengan dasar-dasar ICT kerajaan semasa; g) Membincangkan laporan keselamatan ICT dan menyelesaikan isu-isu berbangkit; h) Menimbang dan meluluskan Pelan Kesinambungan Perkhidmatan (PKP) JPJ; i) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan j) Membincangkan pelanggaran DKICT JPJ dan tindakan yang perlu diambil.	CIO dan Jawatankuasa Keselamatan ICT

P02/01/08 Pasukan Tindak Balas Keselamatan ICT JPJ (CERT JPJ)	
Jawatankuasa di Peringkat Jabatan **Pengarah:** Pengurus ICT **Pengerusi**: ICTSO **Ahli**: • Pegawai Teknologi Maklumat • Penolong Pegawai Teknologi Maklumat **Urus setia**: Ahli CERT JPJ Peranan dan tanggungjawab CERT adalah seperti berikut: a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b) Merekodkan dan menjalankan siasatan awal insiden yang diterima; c) Memberi tindak balas keatas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Menghubungi dan melaporkan insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya; e) Mengesyorkan tindakan pemulihan dan pengukuhan; f) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada pengguna JPJ; dan g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERTJPJ

P02/02 PIHAK KETIGA	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan danmemastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan oleh/dengan pihak ketiga.	
KENYATAAN	**TINDAKAN**

P02/02/01 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga	
Pernyataan ini bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPJ; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT JPJ perlu berlandaskan kepada perjanjian kontrak; e) Menandatangani “Surat Akuan Pematuhan” (Lampiran 1) bagi mematuhi DKICT JPJ; dan f) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. i. Dasar Keselamatan ICT JPJ; ii. Tapisan Keselamatan (jika perlu); iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek; <u>Nota:</u> Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk “Tatacara Penyediaan, Penilaian dan Penerimaan Tender” dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan” yang berkaitan juga boleh dirujuk.	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

P02/03 DALAMAN ORGANISASI	
Objektif: Mewujudkan satu rangka kerja pengurusan untuk memulakan dan mengawal pelaksanaan dan operasi keselamatan maklumat dalam organisasi.	
KENYATAAN	**TINDAKAN**
P02/03/01 Hubungan Dengan Pihak Berkuasa	
Mengekalkan hubungan dengan pihak berkuasa yang berkaitan (Jabatan Bomba dan Penyelamat, Pihak Polis, Pihak Hospital, Pihak Berkuasa Tempatan, JKR dan lain-lain) Jabatan perlu mempunyai prosedur pelaporan insiden yang efektif dalam menentukan pihak berkuasa yang perlu dihubungi ketika berlaku insiden keselamatan maklumat. *(A.6.1.3 Contact With Authorities)*	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT
P02/03/02 Hubungan Dengan Kumpulan Yang Mempunyai Kepentingan Khas	
Mengekalkan hubungan dengan pihak berkuasa yang berkaitan (CGSO, NACSA, MAMPU, SKMM dan lain-lain) Jabatan perlu menyertai *special interest group* bagi: a) Meningkatkan pengetahuan mengenai amalan terbaik dan terkini mengenai maklumat keselamatan yang sesuai; b) Memastikan pemahaman tentang keadaan keselamatan maklumat semasa dan lengkap; c) Menerima amaran awal, peringatan, nasihat dan *patches* yang berkaitan dengan serangan dan kelemahan; d) Mendapat khidmat nasihat daripada pakar perunding keselamatan maklumat;	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

e) Berkongsi dan bertukar-tukar maklumat mengenai teknologi-teknologi terbaru, produk, ancaman atau kelemahan; dan f) Menyediakan medium perhubungan yang sesuai ketika berhadapan dengan insiden keselamatan maklumat; Perjanjian perkongsian maklumat boleh dibangunkan untuk meningkatkan kerjasama dan penyelarasan isu-isu keselamatan. Perjanjian seharusnya mengenal pasti keperluan untuk perlindungan maklumat sulit. *(A.6.1.4 Contact With Special Interest Group)*	
P02/03/03 Keselamatan Maklumat Dalam Pengurusan Projek	
Setiap kumpulan/pasukan pengurusan projek hendaklah mengambil kira isu-isu Keselamatan Maklumat. Keselamatan Maklumat perlu diintegrasikan ke dalam kaedah pengurusan projek Jabatan. Ini secara umumnya terpakai kepada semua jenis projek. Kaedah pengurusan projek yang digunakan adalah: a) Objektif projek perlu merangkumi objektif keselamatan maklumat; b) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenalpasti kawalan - kawalan yang diperlukan; c) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam dokumen DKICT ini; dan d) Carta perbatuan projek dan Pengurusan kawalan perubahan hendaklah jelas dan dipatuhi. Implikasi keselamatan maklumat perlu ditangani dan dikaji dalam semua projek. Tanggungjawab keselamatan maklumat hendaklah dijelaskan dan diperuntukkan kepada peranan-peranan yang tertentu seperti mana yang dinyatakan dalam pengurusan projek. *(A.6.1.5 Information Security In Project Management)*	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

PERKARA 03
KAWALAN DAN PENGELASAN ASET

P03/01 AKAUNTABILITI ASET

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JPJ.

KENYATAAN	TINDAKAN
P03/01/01 Inventori Aset ICT	
Pernyataan ini bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan bahawa semua aset ICT JPJ hendaklah dikenal pasti dan maklumat aset yang diperoleh oleh jabatan wajib mengisi borang penerimaan aset dan pendaftaran aset hendaklah dilaksanakan melalui Sistem Pengurusan Aset dan mesti sentiasa dikemaskini. Ini termasuklah mengenalpasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya; Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; b) Memastikan semua pengguna mengesahkan penempatan aset ICT JPJ; c) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, di dokumen dan dilaksanakan; d) Setiap pengguna JPJ adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan e) Memastikan aset ICT didaftarkan dilabelkan dengan pelekat kod bar.	Pegawai Aset dan Semua

P03/02 PENGELASAN DAN PENGENDALIAN MAKLUMAT	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yangbersesuaian.	
KENYATAAN	**TINDAKAN**
P03/02/01 Pengelasan Maklumat	
Maklumat Terperingkat yang terdiri daripada maklumat fizikal dan digital hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad.	Semua
P03/02/02 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa	Semua

pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan berdasarkan kepada Arahan Keselamatan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	
P03/02/03 Penggunaan Aset	
Penggunaan aset ICT perlulah mengikut prosedur atau peraturan yang telahditetapkan dengan tidak mendedahkan maklumat aset dan juga maklumat yang diwujudkan melalui aset berkenaan. Maklumat aset ICT tersebut perlulah terlebih dahulu dikenalpasti dandirekodkan dalam bentuk dokumen sebelum ianya boleh digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Kakitangan dan pengguna termasuk pengguna luar perlu mengetahui terlebih dahulu peraturan-peraturan keselamatan semasa menggunakan aset ICT Jabatan; dan b) Kakitangan dan pengguna termasuk pengguna luar perlu bertanggungjawab melindungi maklumat samada maklumat aset tersebut atau maklumat yang diproses melalui aset ICT tersebut. *(A.8.1.3 Acceptable Use Of Assets)*	Semua
P03/02/04 Pemulangan Aset	
Semua pengguna dan pengguna pihak ketiga hendaklah memulangkan semua aset jabatan yang berada dalam pemilikannya apabila pekerjaan , kontrak atau perjanjian mereka ditamatkan.Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah mematuhi semua peraturan pengendalian aset terkini merujuk kepada: a) Semua pengguna dan pihak ketiga hendaklah memulangkan semua aset kepada jabatan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak; dan	Semua

b) Semasa notis penamatan JPJ perlu mengawal penyalinan tanpa kebenaran.	

PERKARA 04
KESELAMATAN SUMBER MANUSIA

P04/01 KESELAMATAN SUMBER MANUSIA DALAM TUGAS HARIAN

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

KENYATAAN	TINDAKAN
P04/01/01 Sebelum Perkhidmatan	
Perkara-perkara yang mesti dipatuhiseperti mana yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna dan pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan kepada warga JPJ melalui perakuan Aku Janji dan pihak ketiga melalui *Non-Disclosure Agreement* (NDA), Kontrak Perkhidmatan atau tapisan keselamatan CGSO. Ini adalah berdasarkan keperluan perundangan, peraturan dan tatacara terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua
P04/01/02 Dalam Perkhidmatan	
Perkara-perkara yang mesti dipatuhi seperti yang berikut:	Semua

a) Memastikan semua pengguna serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan garis panduan dan peraturan serta perundangan berkaitan yang ditetapkan; b) Memberi kesedaran mengenai pengurusan keselamatan aset ICT yang berkaitan diberi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya perlu ke atas semua pengguna, pembekal, pakar runding dan pihak ketiga yang berkepentingan apabila berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
P04/01/03 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang mesti dipatuhi seperti yang berikut: a) Memastikan semua aset ICT dikembalikan kepada Pegawai Aset mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/atau terma perkhidmatan.	Semua

P04/02 KESELAMATAN ICT DALAM TUGAS HARIAN	
Objektif: Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JPJ.	
KENYATAAN	**TINDAKAN**
P04/02/01 Tanggungjawab Keselamatan	

Peranan dan tanggungjawab pengguna JPJ terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam myPortFolio atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna JPJ dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Semua
P04/02/02 Terma Dan Syarat Perkhidmatan	
Semua warga JPJ yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa sementara pengguna JPJ yang lain perlu mematuhi syarat-syarat kontrak yang ditandatangani.	Semua
P04/02/03 Perakuan Akta Rahsia Rasmi	
Pengguna JPJ yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua

PERKARA 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

P05/01 KESELAMATAN KAWASAN

Objektif:

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

KENYATAAN	TINDAKAN
P05/01/01 Perimeter Keselamatan Fizikal	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut: a) Kawasan keselamatan hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter, memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c) Memperkukuhkan dinding dan siling; d) Memastikan alat penggera atau kamera sentiasa berfingsi dengan baik mengikut keperluan; e) Memastikan kaunter kawalan dan perkhidmatan keselamatan diwujudkan serta menghadkan jalan keluar masuk bagi memastikan pengguna yang dibenarkan sahaja memasuki kawasan tersebut; f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g) Mereka bentuk dan melaksanakan susun atur keselamatan fizikal di dalam ruang pejabat yang mempunyai kemudahan ICT; h) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana (force majeure); i) Menyediakan garis panduan (SOP) untuk pengguna yang bekerja di dalam kawasan terhad;	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO

j) Memastikan pihak yang dibenarkan sahaja memasuki kawasan terhad; dan k) Sentiasa memastikan pihak ketiga yang membuat penyelenggaraan aset ICT diiringi.	
P05/01/02 Kawalan Masuk/Keluar	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Setiap pengguna JPJ hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) Setiap pelawat mesti mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah memakainya sepanjang tempoh lawatan dan dikembalikan semula selepas tamat lawatan; c) Semua pas keselamatan mestilah diserahkan balik kepada jabatan apabila pengguna JPJ berhenti atau bersara; d) Setiap pelawat hendaklah mendaftar di kaunter Pelawat yang ditetapkan; e) Pemegang pas keselamatan yang kehilangan pas keselamatannya mestilah melaporkan kepada Unit Pentadbiran, Bahagian Teknologi Digital JPJ dengan segera; dan f) Hanya pengguna JPJ yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT JPJ.	Semua
P05/01/03 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Contoh kawasan larangan adalah: a) Bilik Ketua Pengarah; b) Bilik Timb Ketua Pengarah; c) Bilik Pengarah; d) Pusat Data; dan e) Bilik Dokumen dan sebagainya.	Semua

Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut melalui perkara-perkara berikut: a) Secara umumnya aset ICT hendaklah dijaga dan dikawal dengan baik; b) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan c) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	

P05/02 KESELAMATAN PERKAKASAN ICT	
Objektif: Melindungi perkakasan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.	
KENYATAAN	**TINDAKAN**
P05/02/01 Keselamatan Perkakasan	
Secara umumnya perkakasan hendaklah dijaga dan dikawal dengan baik: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; c) Pengguna bertangungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigirasi yang telah ditetapkan; d) Pengguna dilarang sama sekali menambah, menanggalkan atau menukar ganti sebarang perkakasan ICT yang telah ditetapkan tanpa kebenaran; e) Pengguna dilarang membuat sebarang pemasangan (*installation*) perisian tanpa kebenaran Pentadbir Sistem atau pegawai yang dipertanggungjawabkan;	Pegawai Aset, Pengurus ICT dan Semua

f) Pengguna mestilah memastikan perisian *antivirus* di komputer mereka kemaskini dan sentiasa melakukan imbasan ke atas media storan yang digunakan;

g) Semua peralatan sokongan ICT hendaklah dilindungi daripada dicuri, dirosakkan, disalah guna dan diubahsuai tanpa kebenaran;

h) Setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;

i) Peralatan-peralatan kritikal perlu dibekalkan dengan *Uninterruptable Power Supply* (UPS);

j) Semua pekakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch, hub, router* dan lain-lain perlu diletakkan di dalam rak;

k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai sistem pengudaraan (*air ventilation*) yang sesuai;

l) Peralatan ICT yang hendak dibawa keluar dari premis agensi, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

o) Pengguna tidak dibenarkan memindahkan peralatan ICT dari tempat asal tanpa kebenaran pegawai yang dipertanggungjawabkan;

p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih;

q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT;

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

u) Pengguna hendaklah mematikan suis semua perkakasan ICT apabila meninggalkan pejabat; v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; w) Memastikan plug dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. x) Semua perkakasan yang terlibat dalam penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal; dan y) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.	
P05/02/02 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti pita magnetik, *optical disk*, CDROM, *thumb drive* dan media storan lain. Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah keselamatan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat: a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna JPJ yang dibenarkan sahaja; c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan didalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Bagi media storan yang hendak dilupuskan, semua maklumat dalam media tersebut perlu hapuskan terlebih dahulu;	Semua

f) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; g) Media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; h) Media backup hendaklah diletakkan di tempat yang terkawal; i) Membuat salinan atau penduaan (data backup) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; j) Penghapusan maklumat mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan k) Akses dan pergerakan media storan yang mengandungi maklumat terperingkat hendaklah direkodkan dan mendapat kelulusan.	
P05/02/03 Media Tandatangan Digital	
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut: a) Pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada Pegawai Aset dan Pengurus ICT untuk tindakan seterusnya.	Semua, Pegawai Aset dan Pengurus ICT
P05/02/04 Media Perisian Dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut; a) Hanya perisian yang sah sahaja dibenarkan bagi kegunaan Jabatan;	Semua dan Pengurus ICT

b) Sebarang instalasi perisian selain daripada perisian *pre-installed* oleh BTD atau Bahagian/Seksyen/Unit IT hendaklah mendapatkan kebenaran bertulis daripada *Pengurus ICT* atau pegawai yang bertanggungjawab; c) Sistem aplikasi dalaman tidak dibenarkan diagih/didemonstrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; d) Lesen perisian (registration code, serials, CD-keys) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan e) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	
P05/02/05 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan dan kebolehpercayaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan; b) Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e) Memaklumkan kepada pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua Bahagian berkenaan.	Pegawai Aset dan Pentadbir Sistem ICT

P05/02/06 Perkakasan Di Luar Premis	
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut mesti diambil untuk menjamin keselamatan perkakasan: a) Perkakasan perlu dilindungi dan dikawal sepanjang masa; b) Perkakasan atau perisian yang dibawa keluar pejabat mestilahmendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; c) Penyimpanan atau penempatan perkakasan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan d) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
P05/02/07 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak ekonomik untuk dibaiki sama ada harta modal atau inventori yang dibekalkan. Perkakasan ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JPJ. Memastikan data-data dalam storan telah dihapuskan dengan cara yang selamat sebelum peralatan ICT dilupuskan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b) Memastikan data-data dalam storan telah dihapuskan dengan cara yang selamat sebelum peralatan ICT dilupuskan; c) Sekiranya maklumat perlu disimpan, salinan perlu dibuat pada perkakasan yang hendak dilupuskan. Peralatan ICT yang akan dilupuskan sebelum	Pegawai Aset dan Semua

dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

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

f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori yang diguna pakai iaitu Sistem Pengurusan Aset (SPA);

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

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

   i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

   ii. Menyimpan dan memindahkan perkakasan luaran computer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di JPJ;

   iii. Memindah keluar dari premis JPJ mana-mana peralatan ICT yang hendak dilupuskan; dan

   iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab JPJ; dan

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

Nota:

Maklumat lanjut pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan Bilangan 5 Tahun 2007.

P05/03 KESELAMATAN PERSEKITARAN	
Objektif: Melindungi aset ICT JPJ dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
KENYATAAN	**TINDAKAN**
P05/03/01 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperolehi, menyewa, ubahsuai atau membeli hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna JPJ adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Pegawai Yang Dilantik dan Pegawai Yang Berkenaan

P05/03/02 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS (Uninterruptable Power Supply) dan penjana (generator) hendaklah digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pentadbir Sistem ICT
P05/03/03 Kabel	
Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a) Menggunakan kabel mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir Sistem ICT
P05/03/04 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna JPJ hendaklah memahami dan mematuhi prosedur kecemasan dengan merujuk:	Semua

i. SOP dan prosidur Kecemasan JPJ; dan ii. Garis panduan keselamatan kerajaan yang sedang berkuatkuasa; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.	

P05/04 KESELAMATAN DOKUMEN	
Objektif: Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan dan kecuaian.	
KENYATAAN	**TINDAKAN**
P05/04/01 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap dokumen hendaklah difaildan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e) Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua
P05/04/02 Keselamatan Dokumen	
Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:	Semua

a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit dan Terhad kepada dokumen terperingkat; c) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; d) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; e) Menggunakan penyulitan (encryption) ke atas maklumat rahsia rasmi yang dihantar secara elektronik; f) Memastikan dokumen yang mengandungi maklumat terperingkat diambil segera dari pencetak; dan g) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara.	

PERKARA 06
PENGURUSAN OPERASI DAN KOMUNIKASI

P06/01 PENGURUSAN PROSEDUR OPERASI

Objektif:

Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan cepat, betul dan selamat daripada sebarang ancaman dan gangguan.

KENYATAAN	TINDAKAN
P06/01/01 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan paparan ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
P06/01/02 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengubahsuaian yang melibatkan perkakasan sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan	Semua

oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
P06/01/03 Pengasingan Tugas Dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan perluang berlakunya penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian jika perlu.	Pengurus ICT dan ICTSO
P06/01/04 Prosedur Pengurusan Insiden	
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan. Prosidur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;	Pengurus ICT, ICTSO dan CERT JPJ

b) Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c) Menyimpan *audit trail* dan memelihara bahan bukti; dan d) Menyediakan tindakan pemulihan segera.	

P06/02 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA	
Objektif: Memastikan perlaksanaan dan penyelenggaraan terhadap keselamatam maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
KENYATAAN	**TINDAKAN**
P06/02/01 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
P06/02/02 Polisi Keselamatan Maklumat Untuk Hubungan Dengan Pembekal	
Keselamatan maklumat berkenaan akses pembekal kepada aset Jabatan perlu diwujudkan dan didokumentasikan. Jabatan perlu mengenalpasti dan melaksanakan kawalan keselamatan maklumat Jabatan dalam sesuatu polisi yang melibatkan pembekal.	Pegawai Yang Berkenaan dan Pembekal

Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut:

a) Mengenalpasti dan mendokumenkan jenis pembekal (perkhidmatan IT, perkhidmatan logistik, perkhidmatan kewangan atau komponen infrastuktur IT), yang dibenarkan oleh Jabatan untuk mengakses maklumat Jabatan;
b) Mewujudkan proses yang seragam dalam mengurus hubungan dengan pembekal contohnya perjanjian dengan pembekal, borang akses dan sebagainya;
c) Menetapkan jenis akses maklumat yang boleh dibenarkan kepada pembekal mengikut keperluan, memantau dan mengawal capaian tersebut;
d) Keperluan minima keselamatan maklumat bagi setiap jenis maklumat dan akses dinyatakan dalam perjanjian pembekal berdasarkan kepada keperluan Jabatan;
e) Melaksanakan proses dan prosedur untuk memantau kepatuhan terhadap keperluan keselamatan maklumat bagi setiap pembekal dan jenis capaian;
f) Kawalan yang tepat dan lengkap dalam memastikan integriti maklumat atau pemprosesan maklumat yang dibekalkan oleh mana-mana pihak perlu dilaksanakan.(pengesahan dari ICTSO mengenai kawalan ada atau tidak di dalam Jabatan);
g) Jenis pematuhan yang diperlukan terhadap pembekal bagi melindungi maklumat Jabatan;
h) Pengendalianinsiden dan perkara diluarjangkaan berkaitan akses oleh pembekal adalah termasuk tanggungjawab Jabatan dan pembekal;
i) Pelan kontingensi bagi memastikan ketersediaan maklumat atau pemprosesan maklumat disediakan;
j) Kesedaran untuk pegawai Jabatan yang terlibat dalam pengambilalihan tugas berkenaan dengan polisi, proses dan prosedur(pengesahan dari ictso untuk kekalkan atau sebaliknya);
k) Kesedaran keselamatan maklumat untuk pegawai Jabatan yang berurusan dengan pembekal;
l) Syarat-syarat bagi keperluan dan kawalan keselamatan maklumat akan didokumenkan dalam perjanjian yang ditandatangai oleh kedua-dua pihak; dan
m) Mengurus peralihan maklumat, kemudahan pemprosesan maklumat dan

apa-apa yang diperlukan untuk peralihan dan memastikan keselamatan maklumat adalah dipelihara sepanjang tempoh peralihan tersebut. *(A.15.1.1 Information Security Policy for Supplier Relationships)*	
P06/02/03 Rantaian Pembekalan Informasi Dan Teknologi Komunikasi	
Perjanjian dengan pembekal perlu diwujudkan dengan mengambil kira keperluan keselamatan maklumat berkaitan dengan perkhidmatan dan rantaian bekalan teknologi maklumat dan komunikasi. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Mengenalpasti keperluan keselamatan maklumat khusus berkaitan dengan perolehan produk dan perkhidmaan sebagai tambahan kepada keperluan umum keselamatan maklumat; b) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat (polisi, prosedur, proses) kepada subkontraktor atau pembekal-pembekal lain yang memberi perkhidmatan atau pembekalan produk kepada jabatan; c) Melaksanakan pemantauan untuk mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat Jabatan; d) Menjalankan proses mengenalpasti komponen-komponen produk atau perkhidmatan kritikal untuk mengekalkan fungsinya. Oleh yang demikian, ianya memerlukan pemerhatian yang mendalam terutama apabila dilakukan/dibuat di luar Jabatan oleh pembekal utama bersama dengan pembekal-pembekal lain; e) Mengenalpasti dan mendapatkan jaminan bahawa semua komponen produk dan perkhidmatan kritikal boleh dikesan sumbernya; f) Mendapatkan jaminan bahawa produk ICT yang dibekalkan berfungsi seperti yang diharapkan tanpa ciri-ciri luar jangka atau tidak diingini; g) Mewujudkan proses khusus untuk mengurus perkhidmatan dan produk ICT bagi memastikan keselamatan maklumat terjamin. Proses yang diwujudkan mampu untuk mengurus risiko sekiranya komponen produk tidak lagi boleh	Pegawai Yang Berkenaan dan Pembekal

dibekalkan; dan h) Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (supply chain) dan sebarang isu antara Jabatan dan semua pembekal. *(A.15.1.3 Information and Communication Technology Supply Chain).*	

P06/03 PERANCANGAN DAN PENERIMAAN SISTEM	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
KENYATAAN	**TINDAKAN**
P06/03/01 Perancangan Kapasiti	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b) Keperluan kapasiti ini juga perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus ICT dan Pentadbir Sistem ICT
P06/03/02 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT

P06/04 PERISIAN BERBAHAYA

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *Trojan* dan sebagainya.

KENYATAAN	TINDAKAN
P06/04/01 Perlindungan Dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus *Instrusion Prevention System* (IPS) dan *Intrusion Detection System* (IDS) dan mengikut prosidur penggunaan yang betul dan selamat; b) Memasang dan menggunakan perisian yang sah dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c) Mengimbas semua perisian atau fail dengan anti virus sebelum menggunakannya; d) Mengemas kini *pattern* anti virus setiap hari; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Pentadbir sistem perlu menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosidur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	JPJ CERT dan Pentadbir Sistem ICT

P06/04/02 Perlindungan Dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

P06/05 *HOUSEKEEPING*	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
KENYATAAN	**TINDAKAN**
P06/05/01 Penduaan	
Bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat salinan keselamatan ke atas semua perisian sistem dan aplikasi sekurang kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; c) Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) JPJ hendaklah menyimpan penduaan mengikut keperluan atau sekurang-kurangnya satu generasi penduaan; dan e) Merekodkan dan menyimpan salinan penduaan di lokasi yang berlainan dan selamat.	Semua

P06/06 PENGURUSAN RANGKAIAN	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
KENYATAAN	**TINDAKAN**
P06/06/01 Kawalan Infrastruktur Rangkaian	
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan: a) Tanggungjawab atau kerja-kerja operasi rangkaian dan *server* hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna JPJ yang dibenarkan sahaja; d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JPJ; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna JPJ kecuali mendapat kebenaran Pengurus ICT; h) Memasang perisian *Instrusion Prevention System* (IPS) dan *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPJ; i) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan	Bahagian/Seksyen/Unit/ Pegawai Yang Bertanggungjawab

Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan JPJ hendaklah mendapat kebenaran Pengurus ICT; k) Semua pengguna hanya dibenarkan menggunakan rangkaian Jabatan sahaja. Penggunaan *modem, hub, unmanage switches* adalah dilarang sama sekali kecuali dengan kelulusan Pengurus ICT; l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan; dan m) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
P06/06/02 Pengasingan Dalam Rangkaian	
Satu kaedah pengurusan keselamatan rangkaian adalah untuk membahagikan pengguna ke dalam domain rangkaian yang berasingan. Domain boleh dipilih berdasarkan tahap jenis pengguna (contoh: domain akses awam, domain desktop, domain server), unit organisasi (contoh: sumber manusia, kewangan, pemasaran) atau gabungan (contoh: domain server menyambung kepada beberapa unit organisasi). Pengasingan ini boleh dilakukan sama ada menggunakan rangkaian fizikal yang berbeza atau dengan menggunakan rangkaian logik yang berbeza (rangkaian persendirian). Perimeter setiap domain perlu didefinisikan dengan jelas. Akses antara domain rangkaian yang dibenarkan perlu dikawal pada perimeter menggunakan gateway (contoh: firewall, router, proxy). Pengesahan, penyulitan dan tahap kawalan akses rangkaian mengikut had capaian pengguna, berasaskan standard rangkaian *wireless* perlu dilaksanakan untuk sambungan terus ke rangkaian dalaman organisasi. Rangkaian *wireless* perlu diikawal dengan teliti terutama untuk persekitaran yang sensitif, pertimbangan perlu dibuat untuk mengawal semua akses *wireless* sambungan luaran danmengasingkan akses ini daripada rangkaian dalaman	Bahagian/Seksyen/Unit/ Pegawai Yang Bertanggungjawab

seperti dinyatakan di dasar kawalan rangkaian sebelum memberikan akses kepada sistem dalaman. Pengesahan, penyulitan dan level kawalan akses rangkaian mengikut tahap pengguna, berasaskan standard rangkaian *wireless* perlu dilaksanakan untuk sambungan terus ke rangkaian dalaman organisasi. *(A.13.1.3 Segregation in Networks)*	

P06/07 PENGURUSAN MEDIA	
Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.	
KENYATAAN	**TINDAKAN**
P06/07/01 Penghantaran Dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
P06/07/02 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna JPJ yang sah sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat Terperingkat hendaklah dihapus atau dimusnahkan mengikut prosidur yang betul dan selamat.	Semua

P06/07/03 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Pentadbir Sistem ICT

P06/08 PENGURUSAN PERTUKARAN MAKLUMAT	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian dengan agensi luar terjamin.	
KENYATAAN	**TINDAKAN**
P06/08/01 Perjanjian Mengenai Penukaran/Pemindahan Maklumat	
Perjanjian antara organisasi dan pihak luar perlu ditandatangani bagi keselamatan penukaran/pemindahan maklumat perniagaan. Perjanjian penukaran/pemindahan maklumat perlu meliputi perkara-perkara berikut: a) Tanggungjawab pengurusan untuk mengawal dan makluman penghantaran, penghantaran dan penerimaan maklumat; b) Prosedur untuk memastikan kebolehkesanan dan bukan penolakan; c) Standard teknikal minimum untuk pembungkusan dan penghantaran; d) Standard pengenalan kurier; e) Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat, seperti kehilangan data; f) Penggunaan sistem pelabelan yang dipersetujui untuk maklumat sensitif atau kritikal, memastikan bahawa makna label mudah difahami;	Semua

g) Piawaian teknikal untuk rakaman dan maklumat bacaan dan perisian; h) Apa-apa kawalan khas yang diperlukan untuk melindungi barang-barang sensitif, seperti penggunaan kaedah kriptografi; i) Mengekalkan rantaian jagaan untuk keselamatan maklumat semasa dalam transit; j) Tahap yang boleh diterima daripada kawalan akses; k) Polisi, perosedur dan kawalam pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; l) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara JPJ dan pihak luar; m) Media yang mengandungi maklumat perlu dilindungi daripada capaianyang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JPJ; dan n) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya. Dasar, prosedur dan standard perlu diwujudkan dan dikekalkan untuk melindungi maklumat dan media fizikal dalam transit dan harus dirujuk dalam perjanjian penukaran/pemindahan itu. Kandungan keselamatan maklumat perjanjian harus mencerminkan sensitiviti maklumat perniagaan yang terlibat. *(A.13.2.2 Agreements on Information Transfer)*	
P06/08/02 Pengurusan Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber internet hendaklah dinyatakan;	Semua

c) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke internet;

d) Pengguna JPJ hanya dibenarkan memuat turun bahan yang sah seperti perisian yang sah dan di bawah hak cipta terpelihara;

e) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Ketua Jabatan;

f) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup*, *blog* dan *bulletin board*. Walaubagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

g) ICTSO, Pasukan JPJ CERT dan pegawai Jabatan di Negeri/Cawangan berhak untuk memantau dan mengawal penggunaan perkhidmatan Internet dan/atau sebarang jenis trafik yang dihantar menerusi Internet agar tidak mengganggu prestasi rangkaian rasmi myGov*NET Jabatan;

h) ICTSO dan Pasukan JPJ CERT berhak pada bila-bila masa menggantung atau menghadkan capaian kepada kemudahan Internet tanpa sebarang notis sekiranya berlaku penggunaan yang melampau atau luar biasa secara berterusan;

i) ICTSO, Pasukan JPJ CERT dan pegawai Jabatan di Negeri/Cawangan berhak pada bila-bila masa menghadkan atau menutup penggunaan sebarang aplikasi atas talian yang menggunakan sumber Internet yang tinggi sekiranya penggunaan aplikasi berkenaan melemah, mengganggu kebolehcapaian *(*accessibility*)* dan keboleharapan *(*reliability*)* prasarana ICT Jabatan;

j) ICTSO, Pasukan JPJ CERT dan pegawai Jabatan di Negeri/Cawangan tanpa prejudis berhak memberhentikan, mencabut dan merampas peralatan broadband modem, hub bersambung ke port rangkaian yang menjadi penyebab kepada gangguan rangkaian rasmi myGov*NET Jabatan;

k) ICTSO, Pasukan JPJ CERT dan pegawai Jabatan di Negeri/Cawangan berhak untuk mendapatkan nasihat tindakan yang wajar bagi memastikan perlanggaran polisi penggunaan Internet tidak berulang;

l) Pengguna ditegah, dilarang sekeras-kerasnya menyambung kabel rangkaian pejabat kepada *modem broadband* internet. Ini akan

mengakibatkan semua perkakasan elektronik ICT iaitu *network printer*, komputer di kaunter, komputer di back office dan komputer di dalam bilik pegawai, komputer cetakan lesen memandu akan mendapat alamat *IP broadband* internet Unifi/Streamyx dan sebagainya. Impaknya, prestasi rangkaian rasmi myGov*NET pejabat Jabatan menjadi perlahan dan menganggu capaian ke sistem mySIKAP. Ini secara tidak langsung akan menjejaskan imej Perkhidmatan Jabatan;

m) ICTSO, Pasukan JPJ CERT dan pegawai Jabatan di Negeri/Cawangan berhak mengeluarkan surat/notis amaran kepada pengguna terbabit dan keingkaran, salahlaku pengguna akan dikenakan tindakan tatatertib oleh Bahagian Integriti Ibu Pejabat Jabatan;

n) Pengguna dilarang menggunakan kemudahan Internet untuk sebarang aktiviti yang melanggar hak cipta, harta intelek dan hak privasi pengguna lain;

o) Pengguna dilarang menggunakan kemudahan Internet untuk sebarang aktiviti penggodaman, pengimbasan rangkaian, menghidu paket data (sniffing), memancing data (phising), perlombongan mata wang kripto dan penyulitan data (data encryption) secara tidak sah;

p) Pengguna dilarang menggunakan kemudahan Internet untuk tujuan penyebaran, penyimpanan, muat turun, muat naik bahan-bahan berunsur perdagangan saham, perdagangan insurans, berita palsu, hasutan, perjudian, fitnah, ugutan atau buli dan lain – lain berkaitan;

q) Pengguna Internet hendaklah pada bila-bila masa memastikan aktiviti yang dilaksana ketika menggunakan kemudahan Internet tidak melemah, mengganggu kebolehcapaian (accessibility) dan keboleharapan (reliability) prasarana ICT Jabatan seperti aktiviti memuat naik / turun data bersaiz besar yang memonopoli kapasiti rangkaian (bandwidth) dalam bentuk Point to Point dan seumpamanya. ICTSO, Pasukan JPJ CERT dan Jabatan di Negeri/Cawangan berhak menetapkan kuota penggunaan Internet yang bersesuaian dari masa ke semasa;

r) Pengguna yang menggunakan kemudahan Internet untuk melaksanakan sebarang transaksi peribadi melalui capaian kepada sistem atau aplikasi pihak luar hendaklah bertanggungjawab ke atas setiap transaksi yang dilakukan. ICTSO, Pasukan JPJ CERT dan pegawai Jabatan di

Negeri/Cawangan tidak bertanggungjawab atas sebarang kerugian, kehilangan dan kerosakan yang berlaku akibat daripada transaksi berkenaan; s) Pengguna hendaklah memastikan Amalan Terbaik Penggunaan Media Jaringan Sosial Sektor Awam 2011 dipatuhi ketika membuat capaian kepada kemudahan Media Jaringan Sosial seperti facebook, twitter, instagram dan lain – lain. Pengguna dilarang menggunakan laman web jaringan sosial untuk mengaibkan individu tertentu; t) ICTSO, Pasukan JPJ CERT bertindak memastikan pengurusan *content filtering/web application filtering/internet access management* sentiasa berfungsi dalam menapis capaian ke laman web Internet dan laman jaringan sosial yang tiada kaitan dengan kegunaan rasmi jabatan; u) Pengguna bertanggungjawab memasang perisian dan aplikasi yang tulen dan sentiasa dikemaskini pada peranti yang digunakan. Pentadbir ICT, ICTSO, Pasukan JPJ CERT dan pegawai Teknologi Digital di Negeri/Cawangan tidak akan bertanggungjawab terhadap sebarang implikasi perundangan sekiranya pengguna memasang sistem pengoperasian dan aplikasi cetak rompak; dan v) Setiap pengguna hendaklah memaklumkan kepada ICTSO, Pasukan JPJ CERT dan pegawai Teknologi Digital di Negeri/Cawangan sekiranya mengetahui atau mengesyaki berlakunya insiden yang boleh menggugat keselamatan kemudahan Internet Jabatan. <u>Nota:</u> Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	
P06/08/03 Pengurusan Mel Elektronik	
Maklumat yang terlibat dalam mesej elektronik perlu sewajarnya dilindungi.	Semua

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

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

a) Akaun atau alamat mel elektronik (emel) yang diperuntukkan oleh JPJ sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
b) Setiap emel rasmi yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JPJ;
c) Memastikan subjek dan kandungan emel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
d) Penghantaran emel rasmi hendaklah menggunakan akaun emel rasmi dan pastikan alamat emel penerima adalah betul;
e) Pengguna JPJ dinasihatkan menggunakan fail kepilan sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
f) Pengguna JPJ hendaklah mengelak dari membuka emel daripada penghantar yang tidak diketahui atau diragui;
g) Pengguna JPJ hendaklah mengenal pasti dan mengesahkan identiti pengguna JPJ yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel;
h) Setiap emel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
i) Emel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi perlulah dihapuskan;
j) Pengguna JPJ hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

k) Mengambil tindakan dan memberi maklum balas terhadap emel dengan cepat dan mengambil tindakan segera;

l) Pengguna hendaklah memastikan alamat emel persendirian (seperti *yahoo.com, gmail.com, streamyx.com.my* dan sebagainya) tidak boleh digunakan untuk tujuan rasmi;

m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing;

n) Melindungi mesej daripada akses yang tidak dibenarkan, pengubahsuaian atau penafian perkhidmatan setimpal dengan skema klasifikasi yang diterima pakai oleh Jabatan;

o) Memastikan alamat dan penghantaran mesej yang betul;

p) Kebolehpercayaan dan penawaran perkhidmatan;

q) Pertimbangan undang-undang contohnya keperluan untuk tandatangan elektronik;

r) Mendapatkan kelulusan sebelum menggunakan perkhidmatan awam luaran seperti mesej segera, rangkaian sosial atau perkongsian fail; dan

s) Tahap pengesahan yang lebih kukuh mengawal akses daripada rangkaian diakses oleh orang awam.

Terdapat pelbagai jenis mesej elektronik seperti emel, pertukaran data elektronik dan rangkaian sosial yang memainkan peranan dalam komunikasi perniagaan.

Nota:

Maklumat lanjut mengenai keselamatan emel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

(A.13.2.3 Electronic Messaging)

P06/09 PERKHIDMATAN DALAM TALIAN	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
KENYATAAN	**TINDAKAN**
P06/09/01 E-Dagang	
Bagi menggalakkan pertumbuhan Perkhidmatan Dalam Talian serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Maklumat yang terlibat perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua
P06/09/02 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisma yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; c) Memastikan segala maklumat yang hendak dipaparkan telah disah	Semua

dan diluluskan sebelum dimuat naik ke laman *web*; d) Memastikan segala maklumat yang hendak dipaparkan perlu mendapat pengesahan dan kelulusan daripada pihak bertanggungjawab sebelum dimuat naik ke laman *web* Jabatan; dan e) Memastikan maklumat sensitif dilindungi dengan menggunakan kaedah penyulitan semasa transaksi dilaksanakan.	

P06/10 PEMANTAUAN	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
KENYATAAN	**TINDAKAN**
P06/10/01 Pengauditan Dan Forensik ICT	
CERT JPJ mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT JPJ; b) Serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (fogery, phishing), pencerobohan(*intrusion*), ancaman(*threats*) dan kehilangan fizikal (physical loss); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengerdar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; g) Aktiviti penyalahgunaan akaun emel; dan	CERT JPJ

h) Aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem.	
P06/10/02 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekodkan aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi ciri-ciri berikut: a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai cirri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Digital dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari masa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
P06/10/03 Log Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem

a) Mewujudkan log sistem bagi merekodkan semua aktiviti harian pengguna JPJ; b) Menyemak log sistem secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	
P06/10/04 Pemantauan Log	
Ianya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, antaranya adalah seperti berikut: a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu di pantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator/pengendali sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan f) Penyelarasan masa bagi domain keselamatan perlu menggunakan sumber masa yang sama (time synchronization). Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPJ atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Bahagian/Seksyen/Unit/ Pegawai Yang Bertanggungjawab dan Pentadbir Sistem

PERKARA 07
KAWALAN CAPAIAN

P07/01 DASAR KAWALAN CAPAIAN

Objektif:
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT JPJ.

KENYATAAN	TINDAKAN
P07/01/01 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna JPJ yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna JPJ sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah serperti berikut: a) Kawalan capaian ke atas asset 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; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	Bahagian/Seksyen/Unit/ Pegawai yang bertanggungjawab, Pentadbir Sistem dan Pengurus ICT

P07/02 PENGURUSAN CAPAIAN PENGGUNA

Objektif:
Mengawal capaian pengguna JPJ ke atas aset ICT JPJ.

KENYATAAN	TINDAKAN
P07/02/01 Akaun Pengguna	
Pengguna JPJ adalah bertanggungjawab ke atas system ICT yang digunakan. Bagi mengenal pasti pengguna JPJ dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b) Akaun pengguna JPJ mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna JPJ yang di wujud pertama kali akan diberi tahap capaian (access right) paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna JPJ bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f) Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna JPJ atas sebab-sebab berikut; i. Pengguna yang bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	Semua dan Pentadbir Sistem ICT
P07/02/02 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Semua

P07/02/03 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data didalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JPJ seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf, simbol dan nombor (Alphanumerik); d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada computer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j) Had tempoh penggunaan kata laluan adalah selama 365 hari dan mesti ditukar selepas tempoh tersebut; dan k) Mengelak dari menggunakan semula empat (4) kata laluan yang pernah digunakan.	Semua

P07/02/04 *Clear Desk* Dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif/terperingkat terdedah sama ada di atas meja pengguna atau dipaparan skrin apabila pengguna tidak berada di tempatnya: a) Menggunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat; d) Pastikan semua maklumat yang sensitif/sulit dalam bentuk hardcopy atau elektronik diletakkan di tempat yang selamat; e) Pastikan kawasan kerja dalam keadaan bersih dan tiada sebarang dokumen sensitif/sulit ditinggalkan di atas meja sebelum meninggalkan pejabat; f) Pastikan komputer dan semua suis perkakasan ICT ditutup sepenuhnya sebelum meninggalkan pejabat; g) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; h) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan computer; i) Komputer riba mestilah dikunci dengan kabel atau disimpan di dalam laci berkunci; j) Pastikan skrin komputer dikunci (Lock Screen) setiap kali meninggalkan kawasan kerja; k) Pastikan mana-mana maklumat sensitif/sulit disimpan di dalam laci berkunci; l) Kunci yang digunakan untuk akses kepada maklumat sensitif/sulit tidak boleh ditinggalkan di atas meja tanpa dijaga;	Semua

m) Pastikan kata laluan dijaga dengan selamat dan tidak didedahkan kepada orang lain; n) Kata laluan tidak boleh ditinggalkan pada nota dan diletakkan pada tempat yang boleh dicapai oleh orang lain seperti pada papan kenyataan, di bawah papan kekunci atau dilekatkan di tepi komputer; o) Bahan cetakan yang mengandungi maklumat sensitif/sulit harus segera diambil dari mesin pencetak; p) Bahan cetakan yang mengandungi maklumat sensitif/sulit tidak digunakan perlu dilupuskan dengan betul supaya tidak berlaku kebocoran maklumat; q) Semua mesin pencetak dan faks perludibersihkan dari kertas sebaik sahaja proses pencetakan, ini membantu memastikan dokumen mengandungi malumat sensitif/sulit tidak ditinggalkan dalam dulang pencetak; r) Papan putih yang mengandungi mengandungi maklumat sensitif/sulit perlu dipadam setelah digunakan; s) Bahan media seperti CD-ROM/DVD atau USB yang mengandungi maklumat sensitif/sulit perlu disimpan di tempat yang selamat iaitu disimpan di dalam laci yang berkunci, dan t) Semua perkakasan dan dokumen hendaklah disimpan atau diletakkan di tempat teratur, bersih dan mempunyai ciri-ciri keselamatan.	
P07/02/05 Pendaftaran dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian. Perkara –perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan profil pengguna; c) Akaun pengguna luar yang diwujudkan pertama kali akan diberi tahap capaian paling minima iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada Jabatan terlebih dahulu;	Semua

d) Pemilikan akaun pengguna adalah tertakluk kepada peraturan dan arahan Jabatan. Akaun pengguna boleh ditarik balik sekiranya berlaku perlanggaran peraturan; dan e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telahmendapat kelulusan Jabatan. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacarajabatan) perlulah dilakukan dengan segera dan berkala atas tujuan keselamatan. *(A.9.2.1 User Registration and De-Registration)*	
P07/02/06 Tadbir Urus Akses Pengguna	
Tadbirurus akses pengguna perlu dilaksanakan secara berkala untuk mengkaji semula akses pengguna ke atas semua aplikasi dan perkhidmatan (*A.9.2.5 Review of User Acces Rights*) Tadbirurus akses pengguna harus mempertimbangkan perkara-perkara berikut: a) Akses pengguna perlu dikaji semula secara berkala dan selepas sebarang perubahan skop tugas pengguna; b) Pewujudan akses khas hendaklah dikaji dan diperiksa secara berkala untuk memastikan akses khas ini tidak disalahguna; dan c) Perubahan kepada akaun khas harus di rekod untuk semakan berkala. *(A.9.2.5 Review of User Access Rights)*	Semua
P07/02/07 Pembatalan Atau Pelarasan Akses Pengguna	
Selepas penamatan, akses individu untuk maklumat dan aset yang berkaitan dengan kemudahan dan perkhidmatan pemprosesan maklumat hendaklah dibatalkan atau digantung. Hak akses yang perlu dikeluarkan atau diselaraskan adalah termasuk aspek akses fizikal dan logikal. Sebarang perubahan akses pengguna perlu dikemaskini dalam dokumen berkaitan. *(A.9.2.6 Removal or Adjustment of Access Rights)*	Semua

P07/03 KAWALAN DAN CAPAIAN RANGKAIAN	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatanrangkaian.	
KENYATAAN	**TINDAKAN**
P07/03/01 Capaian Rangkaian	
Kawalan capaian perkhidmatan hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka (login page) yang bersesuaian di antara rangkaian Jabatan, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisma sebagai identiti pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT Jabatan.	Pentadbir Sistem ICT dan Pentadbir Rangkaian
P07/03/02 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna Internet di JPJ hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan dilarang yang tidak sepatutnya ke dalam rangkaian JPJ; b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO dan Pentadbir Rangkaian berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; c) Kaedah Content Filtering mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; d) Penggunaan teknologi *bandwidth/packet shaper* untuk mengawal aktiviti (video conferencing, video streaming, chat, downloading) adalah perlu bagi menguruskan penggunaan bandwidth yang maksimum dan lebih berkesan;	Pentadbir Rangkaian

e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pegawai yang diberi kuasa; f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke internet; h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JPJ; j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walaubagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan k) Penggunaan *modem, hub, unmanage switch* untuk tujuan sambungan ke Internet **TIDAK DIBENARKAN** sama sekali kecuali dengan kebenaran khas dari ICTSO.	
P07/03/03 Capaian Jarak Jauh VPN	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Capaian Jarak Jauh menggunakan VPN boleh dilaksanakan hanya untuk capaian ke sistem tertentu dalam tempoh masa yang ditetapkan; b) Ruang kerja dan persekitaran bagi akses ke sistem ICT JPJ hendaklah dipastikan selamat; c) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada ICTSO/Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; d) Penggunaan *VPN* oleh warga Jabatan; dan e) Sekiranya pegawai memerlukan akses bagi kemudahan tersebut, mohon untuk mendapatkan borang penggunaan dari Seksyen Teknikal dan	Semua

Keselamatan. Penggunaan kemudahan ini adalah tertakluk kepada syarat dan ketetapan seperti berikut: i. Mendapat kebenaran daripada Pengurus ICT dan ICTSO/; ii. Ruang kerja dan persekitaran bagi akses ke sistem ICT JPJ hendaklah dipastikan selamat; dan iii. Penggunaan VPN oleh pihak pembekal. Sekiranya syarikat pembekal memerlukan akses bagi kemudahan tersebut, mohon untuk mendapatkan borang penggunaan dari Seksyen Teknikal dan Keselamatan. Penggunaan kemudahan ini adalah tertakluk kepada syarat dan ketetapan seperti berikut: i. Ruang kerja dan persekitaran bagi akses ke sistem ICT JPJ hendaklah dipastikan selamat; ii. Radius lokasi tempat capaian adalah munasabah sekiranya diluar dari kawasan daerah dan negeri pejabat; iii. Tujuan penggunaan yang jelas seperti berkursus, kerja luar Kawasan; iv. Tempoh capaian yang telah ditetapkan bergantung kepada tujuan penggunaan; dan v. Laptop atau komputer digunakan hendaklah mempunyai perisian *antivirus* yang sentiasa dikemaskini. Penggunaan Teknologi Pengkomputeran Awan hendaklah dipastikan tahap intergriti dan keselamatan teknologi tersebut serta mendapat kebenaran pihak atasan.	
P07/03/04 Akses Kepada Rangkaian Dan Perkhidmatan Rangkaian	
Pengguna hanya perlu diberikan akses kepada rangkaian dan perkhidmatan rangkaian secara khusus mengikut polisi yang dibenarkan. Polisi ini hendaklah meliputi: a) Rangkaian dan perkhidmatan rangkaian yang dibenarkan untuk diakses; b) Prosedur untuk menentukan pengguna yang dibenarkan untuk akses rangkaian dan perkhidmatan rangkaian;	Bahagian/Seksyen/Unit/ Pegawai yang bertanggungjawab

c) Kawalan pengurusan dan prosedur untuk melindungi akses kepada sambungan rangkaian dan perkhidmatan rangkaian; d) Cara yang digunakan untuk akses kepada rangkaian dan perkhidmatan rangkaian (contoh: penggunaan VPN atau rangkaian wifi); e) Pengguna perlu mendapat pengesahan (contoh: borang) sebelum diberi kebenaran untuk mengakses pelbagai perkhidmatan rangkaian; dan f) Pemantauan penggunaan perkhidmatan rangkaian perlu dilaksanakan secara berkala. Dasar mengenai penggunaan perkhidmatan rangkaian perlu selaras dengan dasar kawalan capaian organisasi iaitu sambungan yang tidak dibenarkan dan tidak selamat kepada perkhidmatan rangkaian boleh memberi kesan kepada keseluruhan organisasi. *(A.9.1.2 Access to Networks And Network Services)*	
P07/03/05 Pengkomputeran Awan (Cloud Computing)	
Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna. Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak bertanggungjawab. Pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat berdasarkan penerangan berikut: a) Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna; b) Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak Kerajaan; c) Pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat; dan d) Penggunaan Teknologi Pengkomputeran Awan seperti *Google Cloud, Google Drive* dan lain-lain hendaklah dipastikan tahap intergriti dan keselamatan teknologi tersebut serta mendapat kebenaran pihak atasan.	Semua

P07/04 KAWALAN CAPAIAN SISTEM PENGOPERASIAN	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
KENYATAAN	**TINDAKAN**
P07/04/01 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Kementerian /Jabatan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan c) Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi termasuk berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Mengehadkan dan mengawal penggunaan program; dan d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem ICT

P07/04/02 Kad Pintar Dan Token Keselamatan GPKI	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan kad pintar kerajaan elektronik (Kad EG) dan token keselamatan GPKI hendaklah digunakan bagi capaian sistem kerajaan elektronik yang dikhususkan; b) Kad pintar dan token keselamatan GPKI hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) Perkongsian kad pintar dan token keselamatan GPKI untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar dan token keselamatan GPKI yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d) Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar dan token keselamatan GPKI perlu dimaklumkan kepada pegawai yang dipertanggungjawabkan.	Semua
P07/04/03 Sistem Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai sistem dan maklumat mestilah mematuhi piawaian amalan terbaik bagi memastikan kualiti kata laluan. Sistem pengurusan kata laluan hendaklah mematuhi perkara berikut: a) menguatkuasakan penggunaan ID pengguna dan kata laluan untuk mengekalkan akauntabiliti; b) Kata laluan hendaklah berlainan dan tidak mengambarkan identiti pengguna; c) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; d) kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Semua

e) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan, ditampal atau didedahkan dengan apa cara sekalipun; f) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan pada setiap komputer, g) Tentukan had masa melahu (idle) selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; h) Penguatkuasaan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; i) Menyenggara rekod kata laluan agar dapat mengelakkan penggunaan semula kata laluan sedia ada iaitu mengelakkan pernggunaan semula tiga (3) generasi kata laluan yang telah digunakan j) Had tempoh penggunaan kata laluan adalah selama 365 hari dan mesti ditukar selepas tempoh tersebut; k) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; l) Menyimpan fail kata laluan berasingan daripada data sistem aplikasi; dan m) Menyimpan dan menghantar kata laluan dalam bentuk dilindungi. *(A.9.4.3 Password Management System)*	

P07/05 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
KENYATAAN	**TINDAKAN**
P07/05/01 Capaian Aplikasi Dan Maklumat	
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di JPJ adalah terhad kepada pengguna dan tujuan yang dibenarkan.	Pentadbir Sistem ICT

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah langkah berikut hendaklah dipatuhi: a) Pengguna JPJ hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap hak capaian dan sensitiviti maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna JPJ hendaklah direkodkan (sistem log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c) Memaparkan notis amaran pada skrin komputer pengguna JPJ sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna JPJ akan disekat; e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah tidak digalakkan. Walau bagaimanapun, penggunaannya dibenarkan terhad kepada perkhidmatan yang dibenarkan sahaja; dan g) Sebarang maklumat yang perlu dimuat naik ke portal atau laman web hendaklah mendapat kebenaran daripada pegawai yang dipertanggungjawabkan.	

P07/06 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
KENYATAAN	**TINDAKAN**
P07/06/01 Peralatan Mudah Alih	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a) Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; b) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan c) Bagi konsep penggunaan" *Bring Your Own Device*" atau BYOD, peralatan tersebut wajib dipastikan tahap intergriti dan keselamatan aplikasi tersebut serta mendapat kebenaran pihak atasan.	
P07/06/02 Kerja Jarak Jauh	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kerja jarak jauh adalah tidak dibenarkan di luar dari kawasan JPJ; b) Sekiranya berada di luar dari kawasan tempat bekerja (masih di dalam premis JPJ) tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; c) Penggunaan Aplikasi Mesyuarat Jarak Jauh seperti *Zoom, Google Meet* dan lain-lain hendaklah dipastikan tahap integriti dan keselamatan aplikasi tersebut serta mendapat kebenaran pihak atasan; dan d) Penggunaan Aplikasi Perhubungan Sosial seperti *WhatsApp, Telegram* dan lain-lain hendaklah dipastikan tahap intergriti dan keselamatan aplikasi tersebut serta mendapat kebenaran pihak atasan.	Semua

PERKARA 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

P08/01 KESELAMATAN DALAM MEMBANGUNKAN SISTEM DAN APLIKASI

Objektif:

Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

KENYATAAN	TINDAKAN
P08/01/01 Keperluan Keselamatan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan serta 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 sempurna 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 sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

P08/01/02 Pengesahan Data Input	
Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pemilik Sistem dan Pentadbir Sistem ICT
P08/01/03 Pengesahan Data Output	
Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

P08/02 KRIPTOGRAFI	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.	
KENYATAAN	**TINDAKAN**
P08/02/01 Penyulitan (Enkripsi)	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
P08/02/02 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
P08/02/03 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

P08/03 KESELAMATAN FAIL SISTEM	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
KENYATAAN	**TINDAKAN**
P08/03/01 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 dan mengikut prosedur yang telah ditetapkan; b) Kod atau aturcara sistem yang telah dikemas kini 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) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e) Data ujian hendaklah dipilih dan penggunaannya dikawal serta dilindungi.	Pemilik Sistem dan Pentadbir Sistem ICT

P08/04 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
KENYATAAN	**TINDAKAN**
P08/04/01 Prosedur Kawalan Perubahan Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;	Pemilik Sistem dan Pentadbir Sistem ICT

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) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh syarikat pembekal; d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan f) Menghalang sebarang peluang untuk membocorkan maklumat.	
P08/04/02 Pembangunan Secara *Outsource*	
Pembangunan perisian aplikasi secara outsource hendaklah mematuhi perkara-perkara berikut: a) Setiap projek perlu dipantau oleh Pengurus ICT; b) Kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik Jabatan; c) Kod sumber yang diserahkan kepada Jabatan mesti bebas daripada sebarang ralat dan kerentanan; d) Mengutamakan kepakaran teknologi tempatan; e) Pembangunan aplikasi hendaklah dijalankan dalam persekitaran pengkomputeran Jabatan; f) Penggunaan data masking semasa pengujian; g) Data ujian hendaklah dilupuskan secara kekal (secured delete) selepas projek disiapkan/tamat kontrak; dan h) Aktiviti sandaran hendaklah berjaya dilakukan sebelum projek tamat.	Pentadbir Sistem ICT
P08/04/03 Polisi Keselamatan Pembangunan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

a) Keselamatan persekitaran pembangunan; b) Keperluan keselamatan dalam fasa reka bentuk; c) Pemeriksaan keselamatan dalam setiap fasa projek; d) Repositori yang selamat; e) Keselamatan kawalan versi; f) Pasukan pembangun hendaklah berupaya untuk menghindar, mencari dan memperbaiki kelemahan sistem; dan g) Teknik pengaturcaraan yang selamat perlu digunakan.	
P08/04/04 Kajian Teknikal Aplikasi Selepas Perubahan	
Perkara-perkara yang perlu diambilkira adalah seperti berikut: a) Perubahan yang telah dilaksanakan perlu mematuhi Prosedur Kawalan Perubahan Sistem; b) Notifikasi perubahan perlu dimaklumkan kepada pengguna; dan c) Memastikan perubahan yang telah dilaksanakan diselaraskan kepada Pasukan Pelan Kesinambungan Perkhidmatan. (A.14.2.3 *Technical Review of Applications After Operating Platform Changes*)	Pemilik Sistem dan Pentadbir Sistem ICT
P08/04/05 Prinsip Kejuruteraan Keselamatan Sistem	
Prinsip-prinsip sistem kejuruteraan yang selamat perlu diwujudkan, didokumenkan, disemak dan digunakan untuk setiap pembangunan sistem maklumat. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Ujian keselamatan meliputi pengesahan data *input*, kawalan proses dan pengesahan data *output*; b) Kawalan sesi selamat; dan *c)* Bebas dari kod penyahpepijatan (debugging).	Bahagian/Seksyen/Unit/ Pegawai Yang Bertanggungjawab

P08/04/06 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi memastikan aktiviti pembangunan sistem, pengintegrasian dan pengujian sistem terjamin untuk melindungi keseluruhan kitaran hayat pembangunan sistem maklumat. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b) Peraturan dalaman dan luaran; c) Kawalan keselamatan sedia ada perlu dipatuhi; d) Kebolehpercayaan kakitangan yang bekerja dipersekitaran; e) Tahap penglibatan sumber luar dalam pembangunan sistem maklumat; f) Keperluan untuk pengasingan antara persekitaran pembangunan yang berbeza; g) Kawalan capaian ke persekitaran pembangunan sistem maklumat; h) Pemantauan perubahan kepada persekitaran pembangunan dan kod sumber; i) Sandaran kepada data-data projek pembangunan sistem maklumat disimpan di lokasi berasingan; dan j) Kawalan ke atas pergerakan data.	Pemilik Sistem dan Pentadbir Sistem ICT
P08/04/07 Pengujian Keselamatan Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan sistem; b) Semua pembangunan dan penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA); c) Menyemak dan mengesahkan input data; d) Mengenalpasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan pelindungan data;	Pemilik Sistem dan Pentadbir Sistem ICT

e) Membuat semakan pengesahan dalam aplikasi untuk mengenalpasti sebarang pengubahsuaian maklumat, sama ada kerana kesilapan atau disengajakan; dan f) Menyemak dan mengesahkan *output data.* *(A.14.2.8 System Security Testing)*	
P08/04/08 Pengujian Penerimaan Sistem	
Pengujian penerimaan pembangunan dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai. *(A.14.2.9 System Acceptance Testing)*	Pemilik Sistem dan Pentadbir Sistem ICT

P08/05 KAWALAN TEKNIKAL KETERDEDAHAN (VULNERABILITY)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
KENYATAAN	**TINDAKAN**
P08/05/01 Kawalan Dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

P08/06 DATA UJIAN	
Objektif: Memastikan data yang digunakan untuk ujian sistem dilindungi	
KENYATAAN	**TINDAKAN**
P08/06/01 Perlindungan Data Ujian	
Data ujian perlu dipilih dengan sewajarnya, dilindungi dan dikawal dari sebarang capaian tidak sah. Perkara-perkara yang perlu dipatuhi untuk melindungi data pengoperasian, yang digunakan semasa pengujian: a) Prosedur kawalan capaian/Akses yang digunakan dalam pengoperasian sistem aplikasi perlu digunakan semasa pengujian; b) Pengujian haruslah dilaksanakan terhadap semua aplikasi baharu dan pindaan terkini; c) Setiap penyalinan maklumat kepada persekitaran pengujian perlu mendapatkan pengesahan; d) Maklumat pengoperasian sistem dan aplikasi perlu dihapuskan setelah pengujian selesai; e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan f) Penyalinan dan penggunaan maklumat operasi harus direkodkan (log) bagi tujuan pengauditan. *(A.14.3.1 Protection of Test Data)*	Pemilik Sistem dan Pentadbir Sistem ICT

P08/07 KESELAMATAN PENGOPERASIAN	
Objektif: Memastikan operasi yang betul dan selamat daripada kemudahan pemprosesan maklumat	
KENYATAAN	**TINDAKAN**

P08/07/01 Pengasingan Persekitaran Pembangunan, Pengujian Dan Operasi	
Persekitaran pembangunan, pengujian, dan operasi perlu diasingkan bagi mengurangkan risiko akses tidak dibenarkan atau perubahan kepada persekitaran operasi. Tahap pemisahan antara persekitaran operasi, ujian, dan pembangunan yang perlu untuk mengelakkan masalah operasi perlu dikenal pasti dan dilaksanakan. Berikut adalah perkara-perkara yang perlu dipertimbangkan: a) Peraturan bagi pemindahan perisian daripada pembangunan kepada status operasi perlu ditakrifkan dan didokumenkan; b) Perisian Pembangunan dan operasi perlu dijalankan pada sistem atau pemproses komputer yang berbeza dan dalam domain atau direktori yang berbeza; c) Perubahan kepada sistem operasi dan aplikasi perlu diuji dalam persekitaran pengujian sebelum ianya dioperasikan; d) Selain daripada dalam keadaan tertentu, ujian tidak perlu dilakukan pada sistem operasi; e) Penyusun, editor dan alat pembangunan lain atau utiliti sistem tidak boleh diakses dari sistem operasi apabila tidak diperlukan; f) Pengguna perlu menggunakan ID pengguna yang berbeza untuk sistem operasi dan ujian, dan menu harus memaparkan mesej pengenalan yang sesuai untuk mengurangkan risiko kesilapan; dan g) Data sensitif tidak boleh disalin ke dalam persekitaran sistem ujian melainkan kawalan bersamaan disediakan untuk sistem ujian. *(A.12.1.4 Separation of Development, Testing and Operational Environments)*	Bahagian/ Seksyen/Unit/ Pegawai Yang Bertanggungjawab
P08/07/02 Pemasangan Perisian Pada Sistem Operasi	
Garis panduan berikut perlu dipertimbangkan untuk mengawal perubahan perisian pada sistem operasi dan prosedur perlu dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi seperti berikut:	Bahagian/ Seksyen/Unit/ Pegawai Yang Bertanggungjawab

a) Pengemaskinian perisian operasi, aplikasi dan program hanya boleh dilakukan oleh pentadbir dilatih atas kebenaran pengurusan yang sesuai;
b) Sistem operasi sepatutnya hanya melaksanakan kod yang diluluskan sahaja;
c) Perisian aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang menyeluruh dan berjaya; ujian hendaklah meliputi kebolehgunaan, keselamatan, kesan ke atas sistem dan *userfriendliness* lain dan hendaklah dijalankan ke atas sistem yang berasingan. Ia perlu memastikan bahawa semua sumber program yang sepadan telah dikemaskini;
d) Sistem kawalan konfigurasi boleh digunakan untuk mengekalkan kawalan semua perisian dilaksanakan sebagaimana dokumentasi sistem;
e) Strategi kembalikan (roll-back) perlu disediakan sebelum perubahan dilaksanakan;
f) Log audit disediakan untuk setiap perubahan yang dilaksanakan; Versi terdahulu perisian aplikasi perlu dikekalkan sebagai langkah kontingensi; dan
g) Perisian versi lama perlu diarkibkan, bersama-sama dengan maklumat semua diperlukan dan parameter, prosedur, butiran konfigurasi dan perisian sokongan selagi data dikekalkan dalam arkib.

Sokongan oleh pembekal yang membekalkan perisian yang digunakan dalam sistem operasi adalah diperlukan sepanjang tempoh pembekalan.

Jabatan perlu mengambil kira risiko ke atas perisian yang telah tamat tempoh sokongan oleh syarikat pembekal.

Apa-apa keputusan untuk menaik taraf kepada perisian baru perlu mengambil kira keperluan dan implikasi keselamatan kepada Jabatan.

Sebarang akses hanya diberikan kepada pembekal apabila perlu dengan kelulusan pihak pengurusan dan pemantauan.

Patch perisian boleh digunakan bagi membantu menghapuskan atau mengurangkan kelemahan keselamatan maklumat. Apa-apa perisian komputer yang digunakan perlu dipantau dan dikawal bagi mengelakkan perubahan yang tidak dibenarkan kepada aplikasi, atau yang boleh mendedahkan aplikasi kepada ancaman keselamatan. *(A.12.5.1 Installation of Software on Operational Systems)*	
P08/07/03 Sekatan Ke Atas Pemasangan Perisian	
Peraturan yang mengawal pemasangan perisian oleh pengguna-pengguna perlu diwujudkan dan dilaksanakan. Jabatan perlu menentukan dan menguatkuasakan dasar bagi perisian yang dibenarkan. Pemasangan perisian yang tidak terkawal pada peranti komputer boleh membawa kepada kelemahan dan kebocoran maklumat, hilang integriti atau lain-lain insiden keselamatan maklumat, atau melanggar hak-hak harta intelek. *(A.12.6.2 Restrictions on Software Installation)*	Bahagian/ Seksyen/Unit/ Pegawai Yang Bertanggungjawab
P08/07/04 Kawalan Audit Sistem maklumat	
Keperluan audit dan aktiviti yang melibatkan pengesahan sistem operasi perlu dirancang dengan teliti untuk meminimumkan gangguan kepada proses kerja Jabatan. Garis panduan berikut hendaklah dipatuhi: a) Akses audit kepada sistem dan data hendaklah diuruskan dengan baik; b) Skop audit teknikal perlu dipersetujui dan terkawal; c) Pengauditan harus terhad kepada akses baca sahaja bagi perisian dan data;	Bahagian/ Seksyen/Unit/ Pegawai Yang Bertanggungjawab

d) Akses selain baca sahaja hanya dibenarkan untuk salinan terpencil fail sistem, yang perlu dipadamkan apabila audit itu selesai, atau diberi perlindungan yang sewajarnya jika terdapat kewajipan untuk menyimpan fail-fail itu di bawah keperluan dokumentasi audit; e) Keperluan untuk pemprosesan khas atau tambahan perlu dikenal pasti dan dipersetujui; f) Audit yang boleh mengganggu operasi sistem perlu dijalankan di luar waktu urusniaga Jabatan; dan g) Semua akses perlu dipantau dan direkodkan (log) untuk tujuan audit. *(A.12.7.1 Information Systems Audit Controls)*	

PERKARA 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

P09/01 MEKANISMA PELAPORAN INSIDEN KESELAMATAN ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

KENYATAAN	TINDAKAN
P09/01/01 Mekanisma Pelaporan	
Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada JPJ CERT, ICTSO dan Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN)dengan kadar segera: a) Maklumat didapati hilang, didedahkan kepada pihak –pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan d) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam;	Semua

c) Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010; d) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA); e) Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019; dan f) Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019.	

P09/02 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
KENYATAAN	**TINDAKAN**
P09/02/01 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Jabatan. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut; a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan	ICTSO dan JPJ CERT

e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu. Carta lengkap mengenai perjalanan laporan insiden seperti di **Lampiran 2**.	
P09/02/02 Tugasan Dan Keputusan Untuk Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat. JPJ CERT, Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN) bertanggungjawab terhadap insiden keselamatan ICT dan keputusan perlu dibuat jika insiden tersebut boleh diklasifikasikan sebagai insiden keselamatan maklumat mengikut prosidur yang ditetapkan. Pasukan yang terlibat wajar menentukan keutamaan insiden keselamatan dan memberi pengelasan bagi membantu jabatan dalam mengenal pasti kesan kejadian secara lebih lanjut. Setiap keputusan dan hasil daripada penilaian yang dibuat boleh dipanjangkan kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN) supaya pengesahan atau penilaian semula dapat dilakukan. Hasil dari setiap penilaian dan keputusan perlu direkodkan secara terperinci sebagai rujukan jabatan pada masa depan. *(A.16.1.4 Assessment of And Decision on Information Security Events)*	ICTSO, JPJ CERT dan Agensi Keselamatan Siber Negara (NACSA)
P09/02/03 Tindak Balas Kepada Insiden Yang Melibatkan Keselamatan Maklumat ICT	
Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosedur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan ICT adalah untuk mengembalikan	ICTSO, JPJ CERT dan Agensi Keselamatan Siber Negara (NACSA)

tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah perlu pemulihan. Pasukan tindakbalas wajar melaksanakan perkara berikut: a) Mengumpul bahan bukti secepat yang mungkin selepas kejadian; b) Melaksanakan forensik keselamatan maklumat; c) Melaksanakan aktiviti penambahbaikan; d) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk analisis selanjutnya; e) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu; f) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku; dan g) Selepas sesuatu insiden ditangani dengan sempurna, penutupan kes secara rasmi perlu dilakukan dan direkod. Analisis selepas kejadian perlu dilakukan, untuk mengenal pasti punca kejadian berlaku, sekiranya perlu. *(A.16.1.5 Response to Information Security Incidents)*	

P09/03 MENANGANI INSIDEN KESELAMATAN ICT	
Objektif: Meminimumkan kesan insiden keselamatan ICT	
KENYATAAN	**TINDAKAN**
P09/03/01 Pelaporan Insiden	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar serta merta:	ICTSO dan CERT JPJ

a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
c) Kata laluan atau mekanisma kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan maklumat tersalah hantar; dan
e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

Nota:

Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisma Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah dirujuk.

PERKARA 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

P10/01 DASAR KESINAMBUNGAN PERKHIDMATAN

Objektif:

Menjamin operasi *perkhidmatan* agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

KENYATAAN	TINDAKAN
P10/01/01 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Business Continuity Management* - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT JPJ dan perkara-perkaraberikut perlu diberi perhatian: a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap sistem penyampaian perkhidmatan, bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT. c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; e) Mengadakan program latihan kepada pengguna Jabatan mengenai prosedur kecemasan; f) Membuat penduaan (backup); dan g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau mengikut keperluan.	Pengurus ICT

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b) Senarai *personnel* Jabatan dan syarikat pembekal berserta nombor yang boleh dihubungi (faksimili, telefon dan emel). Senarai kedua juga hendaklah disediakan sebagai menggantikan *personnel* tidak dapat hadir untuk menangani insiden;
c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

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

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

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

JPJ hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

P10/01/02 Kebolehsediaan Fasiliti Pemprosesan Maklumat	
Memastikan kebolehsediaan fasiliti pemprosesan maklumat ditahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi/platform pemprosesan) perlu diwujudkan. Bagi tujuan itu, perkara berikut wajar diberi tumpuan: a) Jabatan perlu mengenalpasti keperluan kebolehsediaan sistem maklumat (memahami sejauh mana kritikalnya kebolehsediaan sesuatu sistem maklumat); b) Jika kebolehsediaan sistem maklumat tidak dapat dipastikan dengan satu lokasi pemprosesan, maka fasiliti pemprosesan bertindan perlu dipertimbangkan; c) Fasiliti pemprosesan bertindan perlu diuji bagi memastikan ianya bersedia untuk beroperasi jika pemprosesan utama gagal berfungsi; dan d) Pemprosesan bertindan boleh membawa risiko kepada keutuhan dan kerahsiaan maklumat dan sistem maklumat. Perkara ini perlu diambil kira semasa merekabentuk sistem maklumat. *(A.17.2.1 Availability of Information Processing Facilities)*	Pengurus ICT

PERKARA 11
PEMATUHAN

P11/01 PEMATUHAN DAN KEPERLUAN PERUNDANGAN

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT JPJ.

KENYATAAN	TINDAKAN
P11/01/01 Pematuhan Dasar	
Setiap pengguna di JPJ hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JPJ dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di JPJ termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah/Ketua Jabatan atau pegawai yang diturunkan kuasa berhak untuk memantau aktiviti pengguna JPJ untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT JPJ selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber JPJ.	Semua
P11/01/02 Pematuhan Dengan Dasar, Piawaian Dan Keperluan Teknikal	
ICTSO/Pengurus ICT hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem ICT/maklumat perlu diperiksa secara berkala bagi memastikan standard pelaksanaan keselamatan ICT sentiasa dipatuhi.	Pengurus ICT dan ICTSO

P11/01/03 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem ICT. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
P11/01/04 Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JPJ: a) Arahan Keselamatan; b) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) yang dikeluarkan pada 1 April 2016; c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002; d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”; f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g) Surat Pekeliling Am Bilangan 4 Tahun 2006 – “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam”; h) Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar	Pengurus ICT dan ICTSO

(Wireless Local Area Network) di Agensi-Sgensi Kerajaan yang bertarikh pada 20 Oktober 2006;

i) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh pada 1 Jun 2007;

j) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Perlaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

k) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) – "tatacara Penyediaan, Penilaian dan Penerimaan Tender";

m) Surat Pekeliling Perbendaharaan Bil. 3/1995 – "Peraturan Perolehan Perkhidmatan Perundingan";

n) Akta Tandatangan Digital 1997;

o) Akta Rahsia Rasmi 1972;

p) Akta Jenayah Komputer 1997;

q) Akta Hak cipta (Pindaan) Tahun 1997;

r) Akta Komunikasi dan Multimedia 1998;

s) Perintah-Perintah Am;

t) Arahan Perbendaharaan;

u) Arahan Teknologi Maklumat 2007;

v) Garis Panduan Keselamatan MAMPU 2004;

w) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

x) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;

y) Tatacara Penggunaan E-mail dan Internet;

z) Standard Operating Precedure (SOP) ICT JPJ; dan

aa) Polisi, standard, SOP JPJ yang berkaitan.

P11/01/05 Perlanggaran Dasar	
Perlanggaran Dasar Keselamatan ICT JPJ boleh dikenakan tindakan tatatertib.	Semua
P11/01/06 Hak Harta Intelek	
Prosedur ini memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan dengan hak harta intelektual. Prosedur ini bagi pelaksanaan kawalan terhadap keperluan perlesenan yang mematuhi had pengguna yang telah ditetapkan dan penggunaan material yang berlesen serta berdaftar yang dilindungi di bawah Hak Cipta dan Harta Intelek. Bagi melindungi dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat, garis panduan berikut perlu dilaksanakan; a) Akta Hakcipta 1997 hendaklah sentiasa dipatuhi bagi menghalang aktiviti meniru hak cipta orang lain; b) Pembelian dari sumber yang sahih; c) Memastikan pematuhan berterusan oleh kakitangan JPJ bagi melindungi hak harta intelek. Tindakan boleh diambil terhadap kakitangan yang tidak mematuhi Akta Hakcipta; d) Rekodkan daftar aset dan mengenalpasti semua keperluan perlindungan terhadap aset; e) Rekodkan bukti-bukti pemilikan lesen, cakera master, manual dan lain-lain; f) Memastikan bilangan had lesen tidak melebihi had ditetapkan; g) Penggunaan perisian yang sah; h) Menjalankan pemeriksaan perisian yang sah dan produk berlesen yang digunakan; i) Pengguna adalah dilarang menyalahgunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan; j) Menyediakan dasar untuk mengekalkan syarat-syarat lesen yang sesuai; k) Menyediakan dasar untuk melupuskan atau memindahkan perisian; l) Mematuhi terma-terma dan syarat-syarat bagi perisian dan maklumat yang diambil dari rangkaian awam;	Semua

m) Penggunaan internet bagi tujuan yang disebut di atas mestilah menghormati hak cipta, harta intelek dan hak persendirian pengguna lain; n) Tidak membuat pendua, menukar ke format lain atau mendapatkannya dari rakaman komersial (filem, audio) selain daripada yang dibenarkan oleh undang-undang hak cipta; dan o) Tidak membuat salinan terhadap buku, artikel, laporan atau dokumen lain selain daripada yang dibenarkan oleh Akta Hakcipta. Hak harta intelektual adalah termasuk perisian atau dokumen hak cipta, hak cipta reka bentuk, cap dagangan, paten dan lesen *source code*. Produk perisian proprietari biasanya dibekalkan di bawah perjanjian berlesen yang menentukan terma-terma dan syarat-syarat lesen, sebagai contoh mengehadkan penggunaan sesuatu produk/perisian untuk mesin tertentu sahaja atau menghadkan salinan pendua untuk kerja-kerja backup sahaja. Kepentingan dan kesedaran hak harta intelektual harus disampaikan kepada kakitangan bagi perisian yang telah/akan dibangunkan oleh JPJ. Wujudnya kaedah-kaedah perundangan, peraturan dan kontrak boleh menghadkan penyalinan bahan proprietari. Selain dari itu, hanya sistem atau perkara yang dibangunkan oleh organisasi itu atau dilesenkan atau diberikan oleh developer kepada JPJ sahaja yang boleh digunakan di organisasi ini. Pelanggaran hak cipta boleh membawa kepada tindakan undang-undang, yang mungkin melibatkan denda dan prosiding jenayah. *(A.18.1.2 Intellectual Property Rights)*	
P11/01/07 Privasi Dan Perlindungan Maklumat Peribadi	
JPJ perlu mengenalpasti privasi dan perindungan maklumat peribadi penguna seperti yang termaktub didalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkaitan dengannya. *(A.18.1.4 Privacy and Protection of Personally Identifiable Information)*	Semua

P11/01/08 Kawalan Kriptografi	
Objektif Kawalan Kriptografi adalah untuk melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi. Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang, dan peraturan-peraturan yang berkaitan dengannya. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi; b) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah direka untuk mempunyai fungsi kriptografi; c) Sekatan ke atas penggunaan enkripsi; dan d) Kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian. *(A.18.1.5 Regulation of Cryptographic Controls)*	Semua

P11/02 KAJIAN KESELAMATAN MAKLUMAT	
Objektif: mengelakkan pelanggaran kewajipan undang-undang, undang-undang, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat dan apa-apa keperluan keselamatan	
KENYATAAN	**TINDAKAN**
P11/02/01 Kajian Bebas Terhadap Keselamatan Maklumat	
Perlaksanan keselamatan maklumat JPJ hendaklah dikaji secara bebas atau oleh pihak ketiga pada jangka masa yang dirancang atau apabila perubahan ketara berlaku dalam perlaksanaannya. *(A.18.2.1 Independent Review of Information Security)*	Pengurus ICT

P11/02/02 Pematuhan Dasar Dan Standard / Piawaian	
JPJ hendaklah membuat kajian semula pematuhan dan prosedur pemprosesan maklumat di dalam kawasan tanggungjawab mereka dengan dasar keselamatan JPJ dan piawaian yang berkenaan. Kajian teknikal perlu dilakukan setahun sekali dan sekiranya kajian semula mendapati ada ketidakpatuhan dasar dan piawaian, JPJ perlu; a) Mengenal pasti punca-punca ketidakpatuhan; b) Menilai keperluan tindakan untuk mencapai pematuhan; c) Melaksanakan tindakan pembetulan yang sewajarnya; d) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa; dan e) kekurangan dan kelemahan. *(A.18.2.2 Compliance With Security Policies and Standards)*	Pengurus ICT, ICTSO dan Semua
P11/02/03 Pematuhan Kajian Teknikal	
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat organisasi (contoh: Kajian Security Posture Assessment – SPA). Kajian teknikal perlu dilakukan setahun sekali atau mengikut kesesuaian. *(A.18.2.3 Technical Compliance Review)*	Pentadbir Sistem ICT

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh: cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BCP	*Business Continuity Planning* Pelan tindakan untuk merancang aktiviti-aktiviti kesinambungan perkhidmatan.
CERT JPJ	Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di JPJ
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan(*hoaxes*).
NACSA	*National Cyber Security Agency* atau Agensi Keselamatan Siber Negara. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Harddisk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih

	pantas.
Hub	Hab(*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology*.(Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat

	dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya pencapaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT (DKICT) JPJ

Nama : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya sedia maklum mengenai kewujudan DKICT JPJ;
2. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam DKICT JPJ; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
Tanda Tangan Pegawai

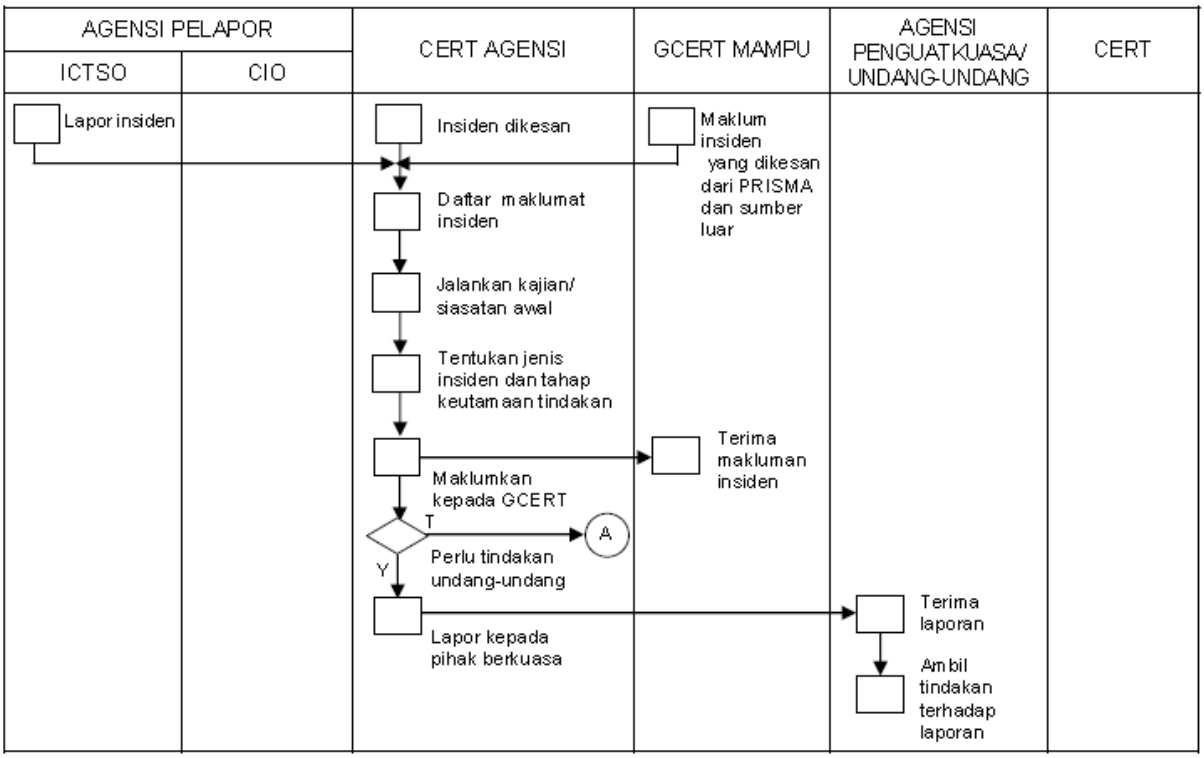
Tarikh: .....

Pengesahan Pegawai Keselamatan ICT

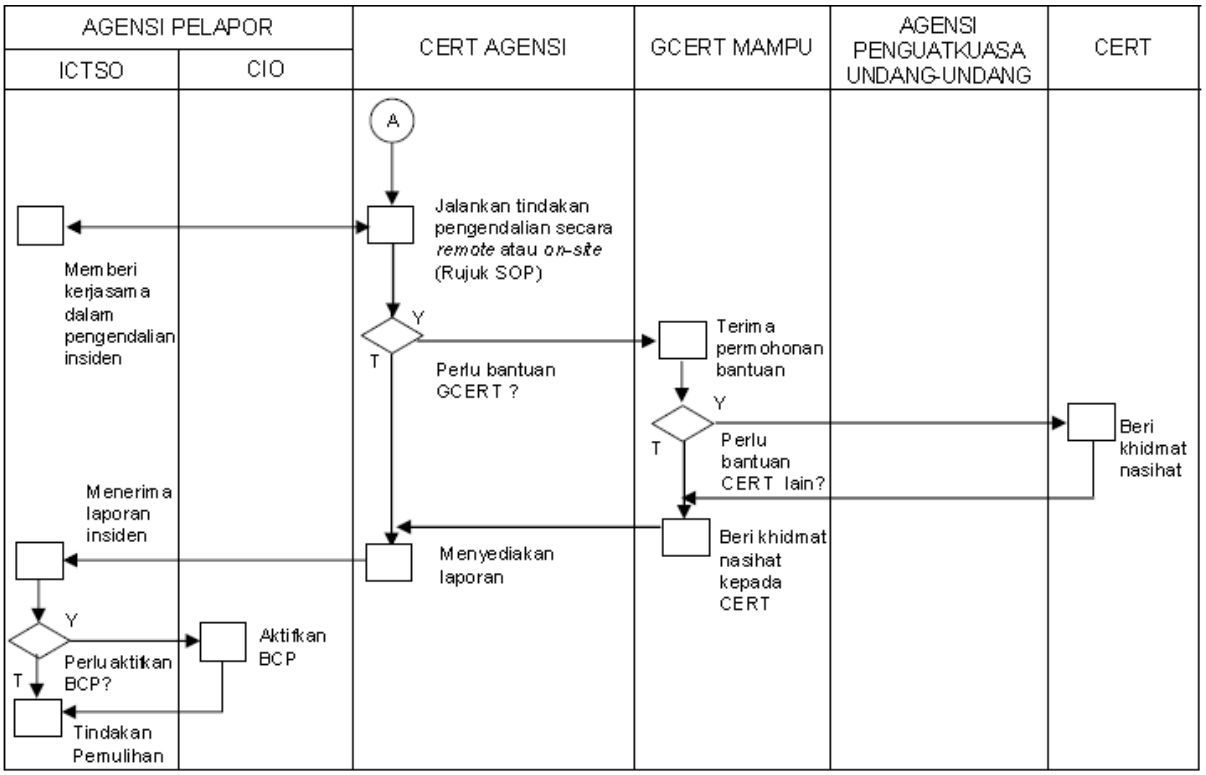
.....
(Pegawai Keselamatan ICT)
b.p Ketua Pengarah Pengangkutan Jalan Malaysia
Tarikh: .....

LAMPIRAN 2

RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT JPJ



semua



BAHAGIAN TEKNOLOGI DIGITAL
JABATAN PENGANGKUTAN JALAN MALAYSIA
JALAN TEKNOKRAT 5,
CYBERJAYA, 63000,
SELANGOR DARUL EHSAN.