DASAR KESELAMATAN ICT

NEGERI KEDAH DARUL AMAN

2020

VERSI 5.1

ISI KANDUNGAN

GLOSARI

TERMINOLOGI	MAKSUD
Antivirus	Perisian yang digunakan untuk mengesan dan membuang malware, seperti: virus komputer, a*dware, backdoors, dialers, fraudtools, hijackers, keyloggers, rootkits, spyware, trojan horses* dan *worms*.
Arahan Keselamatan	Panduan mengenai peraturan-peraturan keselamatan yang perlu dipatuhi oleh semua Kakitangan kerajaan.
Aset ICT	Komponen-komponen yang terdiri daripada Perkakasan, perisian, aplikasi dan sistem rangkaian ICT.
Audit Trail	Satu proses untuk mengenalpasti semua aktiviti yang dilakukan oleh komputer dalam memproses kemasukan data, penjanaan output dan segala aktiviti yang terlibat di antaranya.
Autentikasi	Satu kaedah untuk mengenalpasti identiti pengguna, peralatan atau entiti dalam sistem komputer sebelum kebenaran diberikan untuk mengakses kepada sesuatu sistem.
Backup	Proses Penduaan sesuatu fail atau maklumat
Bandwidth	Lebar jalur. Penandaras yang digunakan untuk menentukan jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan
Biometric	Kaedah yang digunakan untuk pengecamanidentiti individu melalui pengesanan seperti cap jari, suara dan retina.
Business Continuity Planning (BCP)	Pelan tindakan untuk merancang aktiviti-aktiviti kesinambungan perniagaan atau perkhidmatan.
Central Processing Unit (CPU)	Unit Pemprosesan Utama iaitu yang mengandungi pemproses, cakera keras, ingatan dan papan utama.
Computer Emergency Response Team (CERT)	Pasukan yang akan bertindak sekiranya berlaku bencana atau perkara-perkara yang tidak diingini.
Cloud Storage	Media penyimpanan dalam talian yang membolehkan pengguna menyimpan data/maklumat di server virtual (pelayan maya) yang tersedia.

Denial of Services	Penafian memberikan perkhidmatan
Downloading	Pemuat turun sesuatu perisian atau fail
Encryption	Proses Penyulitan data oleh pengirim supaya tidak difahami dan dimanipulasi oleh orang lain kecuali penerima yang sah
Firewall	Sistem yang direka bentuk untuk menapis dan 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*) atau penipuan (*hoaxes*)
Hard Disk	Cakera keras yang berperanan untuk menyimpan data dan boleh diakses lebih pantas
Hub	Peralatan rangkaian menghubung satu stesen kerja dengan stesen kerja yang lain.
Intrusion Detection System (IDS)	Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem.
Intrusion Prevention System (IPS)	Perkakasan keselamatan yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang sebarang aktiviti serangan atau malicious code.
Internet	Perkhidmatan informasi secara global yang menghubungkan semua pengguna seluruh dunia melalui satu protocol rangkaian.
Internet Gateway	Suatu titik yang peranan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik yang betul dati satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Information Security	Proses dan mekanisme untuk melindungi maklumat.
Jawatankuasa Pemandu ICT Negeri	Jawatankuasa ICT Tertinggi di peringkat Kerajaan Negeri Kedah yang diketuai oleh Setiausaha Kerajaan Negeri dan dianggotai oleh semua Ketua-Ketua Jabatan di setiap Jabatan / Agensi Negeri.
Kata Laluan	Satu kumpulan karektor atau gabungan karektor

	dan nombor yang mengesahkan pengenalan diri dan digunakan sebagai satu syarat untuk capaian kepada sesuatu sistem.
Kawalan Akses	Pengawasan terhadap pencapaian untuk perkakasan, perisian dan rangkaian.
Keselamatan Fizikal	Faktor-faktor keselamatan luaran yang perlu diambilkira untuk menjamin keselamatan perkakasan dan perisian.
Keselamatan Sumber Manusia	Persekitaran yang disediakan bagi menjamin keselamatan kakitangan.
Ketua Pegawai Maklumat (CIO)	Pegawai yang dilantik dan bertanggungjawab dalam perancangan dan pembangunan ICT sesebuah agensi kerajaan.
Kriptografi	Kaedah untuk menukar maklumat biasa kepada format yang tidak boleh difahami.
Lightning Arrestor	Peralatan yang digunakan bagi melindungi perkakasan elektrik dari terkena kilat.
Local Area Network (LAN)	Rangkaian Kawasan Setempat yang menghubungkan sebarang peranti atau komputer
Log out	Aktiviti keluar daripada sesuatu sistem atau aplikasi komputer oleh pengguna
Mail Server	Pelayan yang digunakan sebagai platform oleh sesebuah organisasi untuk menguruskan penerimaan dan penghantaran e-mel.
Maklumat Terperingkat	Maklumat rasmi yang telah diklasifikasikan mengikut klasifikasi rahsia besar, rahsia, sulit dan terhad. Maklumat ini boleh didapati dalam bentuk percetakan atau di dalam bentuk digital.
Malicious Code	Perisian hasad yang dimasukkan ke dalam aplikasi atau sistem tanpa kebenaran bagi tujuan tidak baik. Melibatkan serangan virus, worm, trojan horse, spyware dan sebagainya.
Media Storan	Peralatan untuk menyimpan maklumat digital.
Modem (Modulator Demodulator)	Peranti yang menukarkan *bit stream* ke isyarat analog dan sebaliknya. Modem disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer
Mel Elektronik	Mel yang dihantar secara elektronik.

Pegawai Keselamatan ICT (ICTSO)	Pegawai yang bertanggungjawab untuk menjaga keseluruhan keselamatan maklumat.
Pentadbir Sistem ICT	Pegawai yang bertanggungjawab sebagai Pengurus Projek / Pentadbir Rangkaian / Pentadbir Sistem Aplikasi / Pentadbir Pangkalan Data / Pengurus Pusat Data.
Penyenggaraan Pembetulan (Corrective Maintenance)	Pembaikan yang dibuat terhadap perkakasan dan perisian apabila berlaku kerosakan.
Perisian	Merujuk kepada semua aset-aset digital ICT.
Perkakasan	Merujuk kepada semua aset-aset fizikal ICT.
Phishing	Merujuk kepada kaedah memanipulasi kelemahan manusia untuk mendapatkan maklumat dengan menggunakan pemujukan, pengaruh dan penipuan.
Pihak Luar / Ketiga	Kontraktor, pembekal dan lain-lain pihak yang berkepentingan.
Power Surge	Aliran kuasa elektrik yang melebihi had.
Preventive Maintenance	Penyelenggaraan pencegahan berjadual untuk melindungi perkakasan, perisian atau operasi.
Public-Key Infrastructure (PKI)	Kombinasi perisian, teknologi penyulitan (*encryption*) dan perkhidmatan yang membolehkan organisasi melindungi integriti data semasa berkomunikasi dan melakukan transaksi
Bahagian Teknologi Maklumat dan Komunikasi Negeri (BTMK)	Bahagian Teknologi Maklumat dan Komunikasi Negeri (BTMK) adalah satu bahagian di bawah Pejabat Setiausaha Kerajaan Negeri Kedah yang bertanggungjawab dalam perancangan dan pembangunan ICT.
Rangkaian Dalaman (*Private Network*)	Rangkaian komputer persendirian yang digunakan bagi tujuan komunikasi dan hubungan dalam organisasi.
Rangkaian Awam (*Public Network*)	Rangkaian komputer awam yang digunakan secara bersama oleh semua Jabatan / Agensi Negeri untuk membuat capaian ke Internet.
Router	Sejenis peralatan rangkaian yang digunakan untuk menghubungkan antara satu rangkaian dengan rangkaian lain.

Risk Assessment	Analisa risiko untuk mengenalpasti kelemahan-kelemahan yang terdapat dalam sistem yang boleh memberi ancaman kepada keselamatan.
Screen Saver	Imejan yang diaktifkan pada skrin komputer setelah tidak aktif dalam jangka masa tertentu
Secured Network	Sistem rangkaian terselamat di mana maklumat yang melaluinya dikawal dan dilindungi.
Switches	Gabungan hab dan titi (bridges) yang menapis bingkai supaya rangkaian dapat disegmenkan (s*egmentation*). *Switches* berperanan memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD)
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu
Uninterruptible Power Supply (UPS)	Peranti yang mengandungi bateri yang menyimpan kuasa yang bertujuan untuk mengambil alih peranan kuasa elektrik sekiranya berlaku gangguan bekalan kuasa dalam tempoh terhad.
Virtual Private Network (VPN)	Rangkaian Maya Persendirian yang menggunakan infrastruktur telekomunikasi awam, tetapi masih mengekalkan pemilikan (privacy) melalui protokol tertentu dan lain-lain prosedur keselamatan.
Web Server	Pelayan yang digunakan sebagai platform aplikasi web oleh sesebuah organisasi untuk penyampaian maklumat dan perkhidmatan kepada pelanggan melalui internet.

PENDAHULUAN

Penggunaan ICT di kalangan masyarakat dunia semakin menyerlah dengan pelbagai inovasi peralatan komunikasi ICT. Segala maklumat yang diperlukan hanya diperoleh semudah di hujung jari. Kesan penggunaan ICT ini telah mengubah budaya kerja organisasi. Sementara berbangga dengan kemajuan yang dicapai, semua warga Kerajaan Negeri Kedah Darul Aman juga perlu peka terhadap isu keselamatan ICT terutama dari segi peranan, tanggungjawab dan kawalan penggunaannya. Penekanan ke atas kesedaran dan tahap keselamatan ICT adalah penting dan perlu diberi perhatian yang serius disebabkan oleh dua faktor.

Faktor pertama ialah keselamatan ICT merupakan tanggungjawab bersama untuk memastikan sistem ICT yang dikendalikan adalah selamat daripada sebarang penyalahgunaan dan ancaman pencerobohan.

Faktor kedua ialah kewujudan penggunaan pelbagai teknologi dan platform sistem pengoperasian. Keadaan ini menjadikan ia lebih terbuka kepada ancaman keselamatan. Adalah penting di sini supaya penyimpanan maklumat dan penyebaran maklumat perlu dibatasi supaya ia dapat dikawal dengan lebih berkesan.

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

VISI

Mewujudkan persekitaran sistem ICT yang komprehensif, selamat, berkesan, stabil dan boleh dipercayai (reliable).

MISI

Untuk mencapai tahap keselamatan ICT yang menyeluruh bagi menyokong peranan Kerajaan Negeri dalam melindungi kepentingan strategik negeri dan aset-asetnya.

OBJEKTIF

a) Menghebahkan pendirian pihak pengurusan untuk mendukung pelaksanaan keselamatan ICT.
b) Menyediakan Dasar Keselamatan ICT yang komprehensif, sesuai dengan perubahan semasa dan mampu digunapakai oleh semua peringkat pengurusan dan pengguna.
c) Menjamin kesinambungan operasi Kerajaan Negeri dan meminimumkan kerosakan atau kemusnahan.
d) Melindungi kepentingan aset-aset yang bergantung kepada sistem ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi serta mencegah aktiviti penyalahgunaan.

SKOP

Aset ICT Kerajaan Negeri terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan sumber manusia. Dasar Keselamatan ICT Negeri 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 kerahsiannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan orang awam.

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

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Kerajaan Negeri seperti komputer, pelayan, peralatan, komunikasi dan sebagainya.

b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian (Windows-, Linux-based dan iOS), sistem pangkalan data (MySQL/MariaDB), perisian sistem rangkaian (Network Monitoring) atau aplikasi gunasama yang menyediakan kemudahan pemprosesan maklumat kepada pentadbiran Kerajaan Negeri (eDokumen, eBelanja dan sebagainya).

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya seperti contoh:

I. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
II. Sistem halangan akses seperti sistem kad akses; dan
III. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk hardcopy atau softcopy, yang mengandungi maklumat-maklumat untuk digunakan bagi urusan rasmi dan mencapai objektif Kerajaan Negeri. Contohnya, sistem dokumentasi, prosedur operasi standard (SOP), rekod-rekod rasmi, profil-profil kakitangan dan pelanggan, pangkalan data dan fail-fail data serta maklumat-maklumat arkib dan lain-lain.

e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif Kerajaan Negeri. Individu merupakan aset terpenting berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f) Premis Komputer dan Komunikasi

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

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

PERNYATAAN DASAR

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 berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

i. Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah
ii. Menjamin setiap maklumat adalah tepat dan sempurna
iii. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna
iv. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah

Dasar Keselamatan ICT Negeri Kedah 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:

i. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran
ii. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan
iii. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal
iv. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya
v. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

PRINSIP DASAR KESELAMATAN ICT

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT 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 tertentu mengikut dasar perlu mengetahui sahaja. Pertimbangan akses di bawah prinsip ini hendaklah berteraskan kepada klasifikasi maklumat dan tapisan keselamatan yang dihadkan kepada pengguna.

Klasifikasi maklumat hendaklah mematuhi ”Arahan Keselamatan Kerajaan”. Maklumat ini dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Penggunaan encryption, tandatangan digital atau sebarang mekanisma lain yang boleh melindungi maklumat mestilah juga dipertimbangkan. Dasar klasifikasi ke atas sistem aplikasi juga hendaklah mengikut klasifikasi maklumat yang sama.

b) Hak Akses Minimum

Hak akses kepada pengguna hanya diberikan pada tahap yang paling minimum iaitu untuk membaca, melihat atau mendengar sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah dan membatalkan sesuatu data atau maklumat elektronik.

c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mempunyai keupayaan mengesan dan mengesahkan pengguna boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna merangkumi perkara berikut :

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 piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penyelenggaraan, penghantaran, penyampaian, pertukaran dan pemusnahan.

d) Pengauditan Keselamatan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Pentadbir Sistem perlu memastikan semua log / audit trail yang dijanakan oleh aset ICT berkaitan keselamatan disimpan sekurang-kurangnya setahun[1]. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian apabila diperlukan. Ketua Jabatan atau setaraf perlu mempertimbangkan penggunaan perisian tambahan bagi menentukan ketepatan dan kesahihan log / audit trail.

e) Pemulihan

Pemulihan sistem ICT amat diperlukan untuk memastikan kebolehsediaan, kebolehcapaian dan kerahsiaan. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan hendaklah dilakukan melalui tindakan berikut :

i. Pelan Pemulihan Bencana Sistem ICT hendaklah diuji sekurang-kurangnya sekali setahun. Ketua Jabatan atau setaraf dikehendaki menentukan perkara ini dilaksanakan.
ii. Pentadbir sistem dikehendaki melaksanakan sokongan (back up) setiap hari bagi sistem ICT.

f) Pematuhan

Pematuhan Dasar Keselamatan ICT adalah berdasarkan tindakan berikut :

i. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.

ii. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
iii. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing. BTMK / Unit ICT Agensi Negeri berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Jabatan Negeri / Agensi berkaitan.
iv. Menguatkuasakan amalan melapor sebarang insiden yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan / pemulihan.

g) Pengasingan

Pengasingan fungsi perlu diadakan di antara pentadbir dan pengguna. Pengasingan fungsi juga hendaklah dilakukan di antara pentadbir sistem dan pentadbir rangkaian.

h) Integriti

Data dan maklumat hendaklah tepat, lengkap dan sentiasa terkini. Sebarang perubahan terhadap data hendaklah dilaksanakan oleh staf yang diberi kebenaran sahaja.

i) Autentikasi Dan Penyahsangkalan

Proses ini merupakan keupayaan bagi membuktikan bahawa sesuatu mesej atau maklumat tertentu telah dihantar oleh pemilik asal yang dikenalpasti. Setiap sistem ICT berangkaian hendaklah dilengkapi dengan sistem autentikasi yang secukupnya. Bagi sistem yang mengendalikan maklumat terperingkat, ciri penyahsangkalan hendaklah digunakan.

j) Perimeter Keselamatan Fizikal

Perimeter merujuk kepada keadaan persekitaran fizikal di mana aset-aset ICT dilindungi. Perimeter tersebut hendaklah dijaga dengan rapi bagi mengelakkan sebarang pencerobohan. Ketua Jabatan atau setaraf hendaklah memastikan proses ini dilaksanakan.

k) Pertahanan Berlapis (Defence in depth)

Pertahanan berlapis hendaklah diwujudkan untuk melindungi keselamatan aset ICT dari pencerobohan. Ketua Jabatan atau setaraf hendaklah menentukan sistem ICT mempunyai pertahanan berlapis yang lengkap mengikut teknologi semasa.

l) Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip tersebut. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan yang lain. Tindakan mempersepadukan prinsip yang telah dinyatakan perlu dilaksanakan bagi menjamin tahap keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

Bahagaian Teknologi Maklumat dan Komunikasi Negeri Kedah (BTMK) hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu BTMK 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.

BTMK hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat BTMK termasuklah aplikasi, perisian, pelayan, 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.

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

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

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

Perkara 01 Pembangunan Dan Penyelenggaraan Dasar

0101 DASAR KESELAMATAN ICT		
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Kerajaan Negeri dan perundangan yang berkaitan.		
1.0	**Pelaksanaan Dasar**	
	Pelaksanaan Dasar ini dijalankan oleh Setiausaha Kerajaan Negeri dibantu oleh Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan dan Setiausaha Bahagian.	Setiausaha Kerajaan Negeri
2.0	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan / Agensi Negeri (termasuk kakitangan, pembekal, pakar runding dll).	ICTSO
3.0	**Penyelenggaraan Dasar**	
	Dasar Keselamatan ICT Negeri ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT : i. Kenalpasti dan tentukan perubahan yang diperlukan ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO masing-masing untuk dibentangkan kepada Jawatankuasa CERT Negeri bagi mendapatkan persetujuan Mesyuarat Jawatankuasa Pemandu ICT Negeri iii. Perubahan yang telah dipersetujui oleh Jawatankuasa Pemandu ICT Negeri dimaklumkan kepada semua pengguna iv. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut	ICTSO

	keperluan semasa	
4.0	**Pengecualian Dasar**	
	Dasar Keselamatan ICT Negeri adalah terpakai kepada semua pengguna ICT Jabatan / Agensi dan tiada pengecualian diberikan	Semua

Perkara 02 Organisasi Pengurusan Keselamatan ICT

0201 INFRASTRUKTUR ORGANISASI DALAMAN		
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi		
1.0	**Setiausaha Kerajaan Negeri**	
	Peranan dan tanggungjawab adalah seperti berikut : i. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Negeri ii. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Negeri iii. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi iv. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Negeri	Setiausaha Kerajaan Negeri
2.0	**Ketua Pegawai Maklumat (CIO)**	
	Ketua Pegawai Maklumat (CIO) bagi Kerajaan Negeri adalah Timbalan Setiausaha Kerajaan (Pengurusan) . Peranan dan tanggungjawab CIO adalah seperti berikut : i. Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan	CIO

	keselamatan ICT ii. Menentukan keperluan keselamatan ICT iii. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT iv. Memastikan setiap pegawai dan kakitangan menandatangani surat akuan mematuhi Dasar Keselamatan ICT Negeri v. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Negeri	
3.0	**Pegawai Keselamatan ICT (ICTSO)**	
	Pegawai Keselamatan ICT (ICTSO) bagi bagi Kerajaan Negeri adalah Pengarah Bahagian Teknologi Maklumat dan Komunikasi Negeri Kedah (BTMK). Peranan dan tanggungjawab ICTSO di semua Jabatan / Agensi Negeri yang dilantik adalah seperti berikut : i. Mengurus keseluruhan program-program keselamatan ICT ii. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT Negeri iii. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Negeri kepada semua pengguna iv. Melaksanakan garis panduan, prosedur dan tatacara yang berkaitan selaras dengan keperluan Dasar Keselamatan ICT Negeri v. Menjalankan pengurusan risiko vi. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan Kerajaan Negeri berdasarkan hasil penemuan dan menyediakan laporan mengenainya vii. Memberi amaran terhadap kemungkinan	ICTSO

	berlakunya ancaman berbahaya seperti malware dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian viii. Menentukan tahap keutamaan insiden ICT dan melaporkan insiden keselamatan ICT kepada Pasukan CERT Negeri dan memaklumkan kepada CIO serta mengambil langkah pemulihan awal ix. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan mengesyorkan langkah-langkah baik pulih dengan segera x. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan xi. Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Negeri xii. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT xiii. Penyelaras Pengurusan Kesinambungan Perkhidmatan ICT Kerajaan Negeri	
4.0	**Pengurus ICT**	
	Pengurus ICT bagi Negeri Kedah ialah Ketua Penolong Pengarah, Bahagian Teknologi Maklumat dan Komunikasi Negeri Kedah (BTMK). Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: i. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan	Pengurus ICT

	Kerajaan Negeri Kedah; ii. Menentukan kawalan akses pengguna terhadap aset ICT Negeri Kedah; iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; iv. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Negeri.	
5.0	**Pentadbir Sistem ICT**	
	Pentadbir Sistem ICT bagi Agensi ialah Penolong Pengarah Kanan, Seksyen Pembangunan dan Pengurusan Sistem, Penolong Pengarah Kanan, Unit Pusat Data/DRC dan Keselamatan Siber, Penolong Pengarah, Seksyen Rangkaian dan Komunikasi, Penolong Pengarah, Unit Portal/Laman Web dan Multimedia dan Penolong Pengarah, Unit Perkhidmatan ICT. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : i. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas ii. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT iii. Memantau aktiviti capaian harian pengguna iv. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta v. Menyimpan dan menganalisis rekod audit trail	Pentadbir Sistem ICT

	vi. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala	
6.0	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut : i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT ii. Mengetahui dan memahami implikasi keselamatan ICT, kesan dan tindakannya iii. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat iv. Melaksanakan langkah-langkah perlindungan seperti 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 panduankeselamatan yang ditetapkan f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum v. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera vi. Menghadiri program-program kesedaran mengenai keselamatan ICT	Semua

	vii. Menandatangani surat akuan mematuhi Dasar Keselamatan ICT	
7.0	**Jawatankuasa Pemandu Keselamatan ICT**	
	Keahlian dan bidang rujukan jawatankuasa ini dilaksanakan di bawah Jawatankuasa Pemandu ICT. Tanggungjawab khusus berkaitan dengan aspek keselamatan ICT adalah seperti berikut : i. Merangka dasar, hala tuju, garis panduan dan piawaian keselamatan ICT ii. Meneliti, meluluskan dan menguatkuasakan Dasar Keselamatan ICT iii. Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT iv. Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan v. Meluluskan inisiatif untuk peningkatan keselamatan ICT vi. Memantau ancaman-ancaman utama terhadap aset-aset ICT vii. Memastikan pengauditan sistem ICT dilaksanakan sekurang-kurangnya sekali setahun	
8.0	**Jawatankuasa CERT Negeri**	
	Skop tanggungjawab CERT Negeri merangkumi semua jabatan negeri di negeri Kedah Darul Aman. Keahlian jawatankuasa ini adalah seperti berikut : **Pengurus :** Pengarah Bahagian Teknologi Maklumat dan Komunikasi Negeri Kedah (BTMK) **Ahli :** 1) Penolong Pengarah Kanan, Unit Pusat Data/DRC dan Keselamatan Siber 2) Penolong Pengarah, Seksyen Pembangunan dan	

	Pengurusan Sistem 3) Penolong Pengarah, Seksyen Rangkaian dan Komunikasi 4) Penolong Pengarah, Unit Pusat Data/DRC dan Keselamatan Siber Tugas dan tanggungjawab jawatankuasa ini adalah seperti berikut : i. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden ii. Merekod dan menjalankan siasatan awal insiden yang diterima iii. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum. iv. Menasihati agensi mengambil tindakan pemulihan dan pengukuhan v. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Kerajaan Negeri	
9.0	**Jawatankuasa CERT Agensi/Jabatan**	
	Keahlian ditentukan oleh agensi masing-masing berpandukan kepada Pekeliling Am Bil. 4 Tahun 2006 dan pekeliling-pekeliling yang berkaitan	Ketua Jabatan
0202 PIHAK KETIGA		
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)		
1.0	**Keperluan Keselamatan Kontrak Dengan Pihak Ketiga**	
	Bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal Perkara yang perlu dipatuhi termasuk yang berikut:	Semua

	a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Negeri 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 Negeri perlu berlandaskan kepada perjanjian kontrak Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Kandungan perjanjian kontrak dengan pihak ketiga perlu merangkumi perkara-perkara berikut : i. Dasar Keselamatan ICT Negeri ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972 iv. Akuan Pematuhan Dasar Keselamatan ICT v. Hak Harta Intelek e) Pihak ketiga perlu menandatangani dokumen-dokumen berikut bagi melindungi aset ICT kerajaan : i. Akuan Pematuhan Dasar Keselamatan ICT (**LAMPIRAN A**) ii. Perakuan Akta Rahsia Rasmi 1972 (**LAMPIRAN B**) Penggunaan *outsourcing* perlu dikawal daripada segi pelaksanaannya bagi menjamin keselamatan terhadap sistem yang akan dilaksanakan secara outsource. Kaedah pelaksanaan outsourcing adalah berdasarkan kepada Garis Panduan IT Outsource Agensi-Agensi Sektor Awam	

Perkara 03 Pengurusan Pengendalian Insiden Keselamatan

0301 Mekanisme Pelaporan Insiden Keselamatan ICT		
Objektif : Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.		
1.0	**Mekanisme 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 ICTSO dan GCERT Negeri 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) Kata laluan atau mekanisme 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 komunikasi tersalah hantar; e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	Semua

	Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT Negeri sepertimana **LAMPIRAN C.** Prosedur pelaopran insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam	
0302 Pengurusan Maklumat Insiden Keselamatan ICT		
Objektif : Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.		
1.0	**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 Kerajaan Negeri. 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	ICTSO

	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; e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

Perkara 04 Pengurusan Risiko

0401 RISIKO KESELAMATAN ICT		
Objektif: Mengenalpasti tahap keselamatan, *vulnerabilities* dan kelemahan infrastruktur dan aset ICT untuk proses pembaikan dan peningkatan keselamatan yang berterusan		
1.0	**Pengurusan Risiko Keselamatan ICT**	
	Proses analisis risiko keselamatan ICT disyorkan dilakukan oleh Bahagian ICT Jabatan / Agensi masing-masing. Laporan penilaian hendaklah dimajukan kepada Jawatankuasa Pemandu ICT Negeri. Perkara-perkara berikut perlu diambil perhatian dalam melaksanakan analisis risiko : i. Aset-aset ICT (perkakasan, perisian dan maklumat) ii. Sumber manusia (kakitangan, sub-kontraktor dan lain-lain personel luaran) iii. Persekitaran ICT (bangunan dan kemudahan) iv. Aktiviti-aktiviti ICT (operasi, senggaraan dan pembangunan)	Bahagian ICT Jabatan / Agensi Negeri

2.0	***Security Posture Assessment* (*SPA*)**	
	Melaksanakan program SPA ke atas infrastruktur dan sistem ICT Jabatan / Agensi Negeri sekurang-kurangnya sekali setahun	Bahagian ICT Jabatan / Agensi Negeri

Perkara 05 Pengurusan Aset ICT

0501 AKAUNTABILITI		
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Negeri		
1.0	**Inventori Aset ICT**	
	Semua aset ICT hendaklah direkodkan. Ini termasuk mengenalpasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya	Pentadbir Sistem dan Semua
2.0	**Tanggungjawab Terhadap Aset**	
	Semua aset ICT di semua agensi mestilah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa. Setiap aset ICT hendaklah didaftarkan. Ketua jabatan atau ketua bahagian adalah bertanggung jawab mengenal pasti pemilik aset ICT tersebut. Semua aset ICT yang dimiliki atau digunakan oleh setiap seksyen/unit hendaklah diberikan kawalan dan tahap perlindungan yang sesuai oleh ketua seksyen/unit mengikut peraturan yang berkuat kuasa seperti berikut: (a) Pemilik aset hendaklah menentukan tahap sensitiviti (terperingkat) yang bersesuaian bagi setiap maklumat aset di agensi. Pemilik aset juga hendaklah	Semua

	membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut; (b) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contoh : kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset; (c) Semua pengguna aset ICT di agensi mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. Pengguna adalah terdiri daripada kakitangan agensi (lantikan tetap, pinjaman, kontrak dan sambilan), konsultan, kontraktor atau pihak ketiga yang terlibat secara langsung; dan (d) Kehilangan/kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan/kecurian aset berpandukan Arahan Perbendaharaan yang telah ditetapkan. Senarai maklumat aset di agensi hendaklah diwujudkan. Setiap aset perlu ditentukan dengan jelas dan pemilikan aset mestilah dipersetujui dan didokumenkan berserta lokasi semasa aset tersebut. Senarai aset hendaklah disimpan oleh ketua jabatan atau ketua bahagian. Setiap pengguna adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset ICT di bawah tanggungannya.	
0502 PENGELASAN DAN PENGENDALIAN		
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian		
1.0	**Klasifikasi Maklumat**	
	Prosedur mengklasifikasikan maklumat yang diuruskan	Semua

	melalui aset ICT hendaklah berpandukan kepada Arahan Keselamatan Kerajaan seperti berikut : i. Rahsia Besar ii. Rahsia iii. Sulit iv. Terhad Ketua Jabatan atau setaraf dipertanggungjawabkan mengeluarkan Arahan Khas jika perlu untuk dilaksanakan di bahagian masing-masing	
2.0	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : i. Menghalang pendedahan maklumat 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, prosedur, langkah dan garis panduan keselamatan yang ditetapkan vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum	Semua

Perkara 06 Keselamatan Sumber Manusia

0601 KESELAMATAN SUMBER MANUSIA DALAM TUGASAN HARIAN		
Objektif : Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan Kerajaan Negeri, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua kakitangan Kerajaan Negeri hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan yang berkuatkuasa.		
1.0	**Terma Dan Syarat Perkhidmatan**	
	Semua kakitangan yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa. Semua kakitangan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972	Ketua Jabatan / Ketua Pegawai Maklumat (CIO)
2.0	**Menangani Insiden Keselamatan ICT**	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera : i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau dideahkan kepada pihak-pihak yang tidak diberi kuasa ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan atau disyaki hilang, dicuri atau didedahkan iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar	Semua

	v. Berlaku cubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.	
3.0	**Latihan Kesedaran Keselamatan ICT**	
	Program kesedaran keselamatan ICT dilaksanakan kepada semua peringkat kakitangan. Pengguna dan pentadbir komputer perlu menghadiri latihan, memahami dasar dan tatacara penggunaan terutamanya yang melibatkan keselamatan ICT	Pegawai Keselamatan ICT (ICTSO)
4.0	**Kejuruteraan Sosial (Social Engineering)**	
	Semua kakitangan Jabatan / Agensi Negeri perlu berhati-hati dengan kejuruteraan sosial yang menggunakan pengaruh, pemujukan dan penipuan untuk mendapatkan maklumat daripada manusia. Teknik yang sering digunakan adalah seperti berikut : i. *Emel dan Telefon Phishing - Memancing Maklumat Peribadi* ii. *Baiting* - Mengumpan pengguna mendedahkan maklumat iii. *Pretexting* - Tindakan mewujudkan dan menggunakan senario yang dicipta (preteks) untuk melibatkan mangsa yang disasarkan dengan cara yang meningkatkan kemungkinan mangsa akan mendedahkan maklumat atau melakukan tindakan yang mungkin tidak mungkin dalam keadaan biasa iv. *Tailgating* - Pencerobohan/Perolehan maklumat dengan mengikut/meniru akses pengguna yang sah v. *Quid Pro Quo* - Menjanjikan kebaikan kepada pengguna dalam pertukaran maklumat umum atau sulit	Semua

	Semua kakitangan Kerajaan Negeri perlu segera memaklumkan kepada ICTSO masing-masing atau BTMK bagi mendapatkan pengesahan sekiranya berlaku perkara seperti berikut : i. Menerima sebarang mel elektronik yang meminta pengesahan nombor akaun / id pengguna dan kata laluan atas alasan sesuatu masalah telah berlaku dengan masuk ke laman web khas yang disediakan atau menelefon ke nombor bebas tol yang disediakan ii. Menerima panggilan telefon yang meminta nombor akaun / id pengguna dan kata laluan atas alasan sesuatu masalah berlaku pada akaun tersebut iii. Menjumpai media seperti thumb drive / disket / CD yang mempunyai label kononnya terdapat maklumat sulit kerajaan di dalamnya iv. Menerima kunjungan dari orang yang tidak dikenali yang mengakui pegawai baru / wakil daripada Jabatan / Agensi / Kementerian untuk temuduga atau mendapatkan maklumat sulit. Sekiranya ini berlaku, sila buat panggilan segera ke Jabatan / Agensi / Kementerian berkaitan untuk pengesahan identiti individu tersebut sebelum menjawab sebarang pertanyaan. Sekiranya didapati identiti individu tersebut adalah palsu, sila buat laporan polis	
5.0	**Perlanggaran Dasar**	
	Perlanggaran Dasar Keselamatan ICT akan dikenakan tindakan tatatertib	Semua
6.0	**Keselamatan ICT Dalam Senarai Tugas**	
	Peranan dan tanggungjawab dalam keselamatan ICT hendaklah didokumenkan di dalam senarai tugas.	Semua

	Senarai tugas mesti mengandungi perkara berikut: (a) Tanggungjawab kakitangan; (b) Hubungan dengan pegawai atasan; dan (c) Tanggungjawab kakitangan dalam keselamatan ICT.	

Perkara 07 Keselamatan Fizikal Dan Persekitaran

0701 KESELAMATAN KAWASAN		
Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan		
1.0	**Perimeter Keselamatan Fizikal**	
	Keselamatan fizikal dan persekitaran adalah merupakan komponen keselamatan ICT yang penting bagi melindungi aset-aset ICT dan maklumat terperingkat daripada diakses secara tidak sah atau dimusnahkan oleh sama ada kerosakan secara fizikal atau individu. Kerosakan fizikal tersebut boleh disebabkan oleh kecuaian individu dan bencana alam seperti kebakaran dan banjir. Terdapat beberapa ancaman terhadap keselamatan fizikal dan persekitaran yang perlu diambil kira seperti berikut : i. Kebakaran ii. Banjir iii. Keupayaan akses secara tidak sah iv. Kehilangan v. Senggaraan vi. Kecuaian vii. Pengawasan	Pejabat Ketua Pegawai Keselamatan / Pegawai Keselamatan Pejabat, Ketua Pegawai Maklumat (CIO) dan Pegawai Keselamatan ICT (ICTSO)

	Semua ancaman tersebut boleh diatasi dengan kesedaran semua peringkat pengguna sistem ICT menerusi budaya kerja yang cekap mengikut kaedah dan prosedur yang ditetapkan	
2.0	**Kawalan Fizikal**	
	Semua perkakasan, perisian dan peralatan rangkaian komputer hendaklah diletakkan di tempat yang selamat dan terkawal. Penempatan perkakasan komputer mestilah dihindar daripada punca kecuaian dan unsur-unsur sabotaj. Semua kabel rangkaian yang digunakan hendaklah mempunyai salutan (coating) yang tebal dan sukar untuk pecah serta dimasukkan ke dalam saluran paip (conduit) mengikut piawaian antarabangsa dan undang-undang siber negara. Setiap pemasangan kabel rangkaian hendaklah dilabelkan di kedua-dua hujung antara punca dan destinasi kabel tersebut bagi memudahkan proses penjejakan (tracing) apabila berlaku sesuatu insiden keselamatan ICT. Lokasi kritikal yang menyimpan maklumat terperingkat hendaklah diasingkan daripada lokasi yang menyimpan maklumat tidak terperingkat	Pentadbir Sistem ICT dan Pihak Ketiga
3.0	**Kawalan Akses Pusat Data / Bilik Server**	
	Kawalan akses ke pusat data / bilik server hendaklah ditentukan keselamatannya. Kawalan akses boleh diadakan dalam bentuk seperti berikut : i. Biometrik ii. Kata laluan iii. Sistem elektronik kad pintar dan mekanikal Semua akses yang dibenarkan ke kawasan persekitaran pusat data / bilik server hendaklah diiringi oleh Pentadbir Sistem atau kakitangan teknikal yang dilantik bagi menentukan dan mengawal selia penugasan yang	Semua dan Pihak Ketiga

	diperlukan. Buku log juga perlu disediakan untuk tujuan merekodkan maklumat dan aktiviti yang dilaksanakan oleh Pentadbir Sistem ICT atau Pihak Ketiga. Sebarang pemindahan maklumat daripada pusat data / bilik server hendaklah dipohon dan mendapat kebenaran daripada pemilik data (data owner) dan Ketua Jabatan masing-masing	
4.0	**Kawalan Persekitaran**	
	Bangunan yang menempatkan pusat data / bilik server hendaklah mempunyai kawalan persekitaran seperti berikut : i. Susun atur hendaklah dirancang dengan teliti dan mengambil kira ancaman yang akan dihadapi ii. Mempunyai alat penghawa dingin yang mempunyai keupayaan mengawal kelembapan udara bagi mengelak kerosakan komponen elektronik pada perkakasan berkenaan. Pemeriksaan hendaklah dilaksanakan setiap enam bulan bagi menentukan keberkesanannya iii. Menyediakan sistem pengudaraan (ventilation) yang mencukupi iv. Penggunaan lantai bertingkat (raised floor) dalam pusat data / bilik server v. Penggunaan kamera boleh dilaksanakan bagi meningkatkan kawalan keselamatan Bangunan yang menempatkan pusat data / bilik server hendaklah menentukan ciri-ciri keselamatan seperti berikut : i. Bekalan kuasa elektrik mesti dari punca yang berasingan dan berkemampuan menampung	Semua

	semua beban termasuk server, alat penghawa dingin, alat penggera dan lain-lain ii. ”Centralized Uninterruptable Power Supply” (UPS) dan / atau janakuasa sokongan (back up) hendaklah disediakan dan diuji setiap tiga bulan bagi menentukan bekalan kuasa berterusan iii. Sistem pengaliran air yang sempurna bagi mengelakkan banjir. Pemeriksaan terhadap bangunan yang berkenaan hendaklah dilaksanakan setiap enam bulan oleh penyelia bangunan yang bertauliah atau dilantik	
5.0	**Kawalan Perkhidmatan Dan Penyelenggaraan**	
	a) Naziran boleh dilaksanakan secara mengejut atau secara berjadual bagi memastikan keselamatan ICT. b) Bangunan yang mempunyai kuasa yang tidak stabil hendaklah dipasang dengan UPS atau ”Automatic Voltage Regulator” (AVR) pada komputer bagi menentukan ketahanan komponen elektronik komputer berkaitan. c) Semua penyelenggaraan terhadap ”Central Processing Unit” (CPU) hendaklah dibuat secara dalaman. Sekiranya perlu dibaiki oleh pihak swasta, cakera keras hendaklah dikeluarkan terlebih dahulu dari CPU setelah mendapat kebenaran pegawai ICT yang bertanggungjawab. d) Penyelenggaraan secara pencegahan (preventive) dan pembetulan (corrective) perlu dirancang secara berjadual bagi menentukan kesinambungan perjalanan sistem berkenaan. Kontrak penyelenggaraan hendaklah disediakan mengikut prosedur semasa. e) Perangkap kilat (lighting arrestor) hendaklah	Semua

	disediakan di semua bangunan penempatan pusat data / bilik server bagi mengelakkan kemasukan kuasa elektrik berlebihan (power surge) yang disebabkan oleh pancaran kilat	
0702 KESELAMATAN PERALATAN		
Objektif : Melindungi peralatan ICT Kerajaan Negeri dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut		
1.0	**Kawalan Peralatan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem	Semua

	komputer adalah diwajibkan; h) Semua peralatan sokongan ICT hendaklah dilindungi daripada Semua kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j) Semua peralatan ICT hendaklah disimpan atau diletakkan ditempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. k) Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; m) Peralatan ICT yang hendak dibawa keluar dari jabatan, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan; n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; p) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; q) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; r) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;	

	s) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; t) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; u) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; v) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; w) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; x) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
2.0	**Penyelenggaraan Peralatan**	
	Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriri Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan; d) Menyemak dan menguji semua peralatan sebelum	Semua

	dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
3.0	**Peralatan di Luar Premis**	
	Peralatan yang dibawa keluar dari premis Kerajaan Negeri adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	
4.0	**Pembudayaan Penggunaan Teknologi Hijau**	
	Bagi pembudayaan penggunaan ICT Hijau, agensi hendaklah melaksanakan langkah-langkah amalan seperti berikut : a) Komputer Peribadi dan Komputer Riba (i) Tidak menggunakan atau mengaktifkan *screen saver.* Ini disebabkan penggunaan *screen saver* akan menggunakan jumlah tenaga yang sama dengan penggunaan skrin yang aktif; (ii) Memastikan monitor dalam keadaan *stanby/hibernate* selepas 5 minit tidak aktif; (iii) Memastikan kemudahan *power management* untuk komputer peribadi dan komputer riba diaktifkan; (iv) Memastikan komputer ditutup dan suis dimatikan	

	serta plug komputer dicabut dari soket elektrik apabila tidak digunakan untuk jangka masa panjang. Ini untuk mengelakkan arus elektrik masih aktif dalam sistem pendawaian menerusi plug komputer yang tidak dimatikan dan dicabut; (v) Menggantikan monitor *Calthode Ray Tube (CRT)* dengan monitor *Liquid Crystal Display (LCD*). Ini adalah kerana penggunaan LCD boleh menjimatkan 30% hingga 50% tenaga elektrik berbanding CRT; (vi) Menimbangkan penggunaan saiz monitor yang bersesuaian kerana saiz monitor yang besar akan mengggunakan tenaga eletrik yang lebih; dan (vii) Menimbangkan penggunaan *Teknologi Thin Client* di mana ia dapat mengurangkan penggunaan tenaga elektrik dan kos penyelenggaraan. b) Pencetak (i) Mengaktifkan kemudahan *duplex* dan mode draf pada pencetak sebagai *default*. Ini adalah untuk menjimatkan penggunaan kertas dan dakwat pencetak; (ii) Mengaktifkan kemudahan *power-saving sleep* mode pada pencetak (jika ada); (iii) Mengurangkan bilangan pencetak *stand-alone* dengan pewujudan pencetak rangkaian yang dapat dikongsi bersama oleh penjawat awam; (iv) Mengawal dokumen yang berkenaan sahaja untuk dicetak; (v) Menimbangkan kawalan mencetak di pencetak rangkaian berdasarkan ID pengguna; (vi) Memastikan supaya penggunaan kertas secara	

	optimum; dan (vii) Mengurangkan penggunaan bahan seperti riben, kertas dan *toner*. c) Pelayan (*Server*) (i) Mengoptimumkan penggunaan server dengan melaksanakan kaedah konsolidasi menerusi teknologi *virtualisation*; (ii) Memastikan server-server yang tidak aktif penggunaannya hendaklah *shut down* dan suis dimatikan; dan (iii) Menimbang penggunaan *Keyboard, Virtual Display Unit, Mouse (KVM)* kepada server-server bagi mengurangkan jumlah tenaga elektrik yang diperlukan dan haba yang dihasilkan oleh monitor. d) Aplikasi (i) Menggandakan penggunaan perkhidmatan *online* kearah pengurangan penggunaan kertas dan bahan cetak; (ii) Mempertingkatkan penggunaan kemudahan e-mel untuk berkomunikasi tanpa kertas bagi tujuan rasmi sahaja; (iii) Mempertimbangkan kemudahan penggunaan saluran baru untuk mendapatkan maklum balas dan aduan secara rasmi; dan (iv) Mempertingkatkan pembangunan aplikasi *online* yang menggantikan proses kerja secara manual.	
5.0	**Peringkat Pelupusan**	
	Produk ICT yang perlu dilupuskan hendaklah mengikut tatacara yang digariskan melalui Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 “Tatacara	

	Pengurusan Aset Alih Kerajaan" dan mengambil kira pemuliharaan alam sekitar serta amalan hijau sama ada ianya masih boleh diguna pakai *(reuse)* dan dikitar semula *(Recycle).*	

Perkara 08 Keselamatan Komunikasi Dan Rangkaian

0801 PERANCANGAN DAN PENERIMAAN SISTEM		
Objektif : Bahagian ini adalah tertumpu kepada infrastruktur rangkaian komunikasi iaitu rangkaian internet, intranet dan secured network. Ini juga meliputi aset rangkaian (*router, switch, hub, modem dan server*), sistem pengkabelan dan segala perkhidmatan pengkomputeran. Ini bertujuan menjaga keselamatan rangkaian dan komunikasi komputer.		
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
1.0	**Perancangan Kapasiti**	
	a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawalselia oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 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. c) Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan atau dipersetujui	Pentadbir Sistem ICT dan Pegawai Keselamatan ICT (ICTSO)

2.0	**Kawalan Perisian**	
	a) Pentadbir sistem dikehendaki menentukan penggunaan perisian-perisian daripada sumber-sumber yang sah sahaja. Penggunaan perisian-perisian daripada sumber yang tidak sah dilarang sama sekali bagi mengelakkan sebarang kod malicious tersebar / disebar dalam sistem ICT. b) Perisian-perisian yang berfungsi sebagai audio / video streaming dan peer to peer adalah dilarang sama sekali. c) Setiap komputer dipasang dengan perisian antivirus yang terkini dan patern virus mestilah dikemaskini. d) Untuk mengelak penyebaran atau jangkitan daripada perisian malicious, semua perisian atau sistem mestilah diimbas dengan antivirus dan diperiksa dan disahkan selamat sebelum digunakan. Ia merangkumi juga setiap media storan luar yang dibawa masuk. e) Semua sistem ICT tidak dibenarkan menggunakan perisian yang tidak berlesen kecuali perisian open source yang dibenarkan. f) 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 prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua

0802 PERISIAN BERBAHAYA		
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.		
1.0	**Perlindungan dari Perisian Berbahaya**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemaskini antivirus dengan *pattern* antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi semua program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua

2.0	**Perlindungan dari *Mobile Code***	
	Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
0803 HOUSEKEEPING		
Objektif : Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.		
1.0	***Backup***	
	a) Salinan penduaan hendaklah dilakukan seperti berikut : i. Salinan direkodkan dan disimpan di off-site. Lokasi off-site tidak boleh di bangunan yang sama dan pemilihan lokasi mestilah praktikal dengan mengambilkira aspek geografi, kemudahan, keselamatan, kos dan persekitaran. ii. Salinan dilakukan setiap kali konfigurasi berubah. iii. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. iv. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. v. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. b) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. c) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan.	Semua BTMK
0804 PENGURUSAN RANGKAIAN		
Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan		

1.0	**Pengurusan Infrastruktur Rangkaian**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengurusan rangkaian di jabatan-jabatan negeri adalah di bawah penyelarasan BTMK. Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi BTMK. b) Pengurusan rangkaian di agensi-agensi negeri adalah di bawah penyelarasan Bahagian ICT masing-masing. Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi Bahagian ICT masing-masing. c) *Secured Network* adalah tidak dibenarkan sama sekali disambungkan dengan sebarang rangkaian awam (Internet). d) Intranet tidak dibenarkan disambungkan kepada rangkaian awam tanpa menggunakan mekanisme keselamatan yang diluluskan oleh Jawatankuasa CERT Negeri. e) Semua jabatan / agensi negeri hendaklah mewujudkan mekanisme untuk memastikan pematuhan terhadap segala arahan keselamatan setiap rangkaian di bawah tanggungjawabnya. f) Penggunaan administrator tools dan hacking tools tidak dibenarkan dipasang pada komputer pengguna melainkan mendapat kebenaran ICTSO. g) Sebarang pengujian perkakasan dan perisian aplikasi sistem hendaklah mendapat kebenaran daripada Pentadbir Sistem. h) Kawalan capaian yang selamat (*VPN Connection*) hendaklah diwujudkan untuk akses kepada komponen-komponen rangkaian komunikasi. i) Semua konfigurasi dan infrastruktur rangkaian	BTMK BTMK

	hendaklah diklasifikasikan, didokumenkan dan sentiasa dikemaskini oleh Pentadbir Rangkaian dari semasa ke semasa. j) Semua capaian jarak jauh (*remote access*) tidak dibenarkan melainkan dengan menggunakan sistem autentikasi dan ciri-ciri keselamatan yang dibenarkan oleh Jawatankuasa CERT Negeri. k) Capaian ke Internet dan sistem yang terletak di dalam Secured Network yang melalui infrastruktur rangkaian awam hendaklah mempunyai ciri-ciri keselamatan tambahan. l) Memasang Web Content Filter pada Internet Gateway untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam PKPA Bil 1 Tahun 2003 atau pekeliling-pekeliling terkini.	
0805 PENGURUSAN MEDIA		
Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.		
1.0	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
2.0	**Prosedur Pengendalian Media**	
	Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut : i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat. ii. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja. iii. Menghadkan pengedaran data atau media untuk	

	tujuan yang dibenarkan. iv. Menyimpan dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. v. Menyimpan semua media di tempat yang selamat. vi. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapuskan atau dimusnahkan mengikut prosedur yang betul dan selamat.	
3.0	**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) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	
0806 KESELAMATAN KOMUNIKASI DAN PERTUKARAN MAKLUMAT		
Objektif : Memastikan keselamatan komunikasi dan pertukaran maklumat antara Pejabat SUK Negeri dan Agensi Luar terjamin.		
1.0	**Pertukaran Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;	

	b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara Kerajaan Negeri dan Agensi Luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Kerajaan Negeri; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
2.0	**Perkhidmatan Mel Elektronik (E-mel)**	
	Penggunaan e-mel di Kerajaan Negeri hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk " Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan' dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a) Pentadbir E-mel wajib memastikan setiap pelayan e-Mel dipasang dengan pelayan antivirus E-mel bagi membolehkan pengimbasan dilakukan sebelum E-mel sampai kepada pengguna. b) Penggunaan kemudahan ini adalah untuk tujuan perkhidmatan rasmi sahaja. c) Semua pihak bertanggungjawab sepenuhnya terhadap semua kandungan E-mel di dalam akaun sendiri. d) Kelayakan kakitangan untuk mendapat akaun E-mel sesuai dengan jawatan dan mengikut polisi semasa.	Semua dan Pentadbir Sistem ICT

	Sebarang perubahan status penggunaan (bertukar keluar atau berhenti) hendaklah dimaklumkan kepada Pentadbir E-mel. e) Penghantaran maklumat terperingkat melalui Internet mestilah menggunakan kaedah penyulitan yang dibenarkan. f) Sebarang penggunaan E-mel yang boleh memudaratkan nama baik jabatan / agensi serta Kerajaan Negeri Kedah adalah dilarang sama sekali. g) Komunikasi E-mel bagi tujuan rasmi mestilah menggunakan akaun e-Mel rasmi kerajaan sahaja. h) Segala akaun E-mel yang diberi adalah bukan hak persendirian. Pentadbir E-mel berhak mengakses mana-mana akaun bagi tujuan pengurusan akaun E-mel, keselamatan dan undang-undang. i) Elakkan dari membuka E-mel daripada penghantar yang tidak diketahui dan diragui. j) Mengimbas bahan-bahan yang hendak dimuat naik atau dimuat turun supaya bebas virus sebelum digunakan. k) Semua pihak dilarang daripada melakukan aktiviti yang melanggar tatacara penggunaan E-mel rasmi kerajaan seperti : i. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain. ii. Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah. iii. Menggunakan E-mel bagi tujuan peribadi (bukan rasmi), komersial atau politik. iv. Menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah. v. Menghantar dan melibatkan diri dalam E-mel	Semua

	yang berunsur hasutan, E-mel sampah, E-mel bom, E-mel spam, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang. vi. Menyebarkan kod perosak seperti virus, worm, trojan dan trap door yang boleh merosakkan sistem komputer dan maklumat pengguna lain. vii. Menghantar semula E-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian. viii. Membenarkan pihak ketiga untuk menjawab E-mel kepada penghantar asal bagi pihaknya.	
3.0	**Perkhidmatan Internet**	
	Perkara-perkara yang perlu dipatuhi dalam pengendalian perkhidmatan Internet adalah seperti berikut: a) Semua pihak dikehendaki menyediakan kawalan terhadap penggunaan kemudahan Internet. b) Hak akses hendaklah dilihat sebagai satu kemudahan yang disediakan untuk membantu melicinkan pentadbiran atau memperbaiki perkhidmatan yang disediakan. c) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan. d) Kemudahan ini disediakan untuk tujuan capaian hal yang bersangkutan dengan perkhidmatan dan dibenarkan untuk tujuan-tujuan produktif. e) Bahan rasmi yang hendak dimuat naik ke Internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik. f) Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan	Semua

	untuk tujuan yang dibenarkan oleh Ketua Jabatan sahaja. g) Semua pihak dilarang daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti : i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen. ii. Menyedia dan menghantar maklumat berulang-ulang berupa gangguan. iii. Melayari, menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah. iv. Melayari, menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej kerajaan. v. Menyalahguna kemudahan perbincangan awam dan jaringan sosial atas talian seperti newsgroup, bulletin board, facebook, twitter dan sebagainya. vi. Memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain. vii. Melayari, memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti perjudian, permainan elektronik, video dan lagu. viii. Menggunakan kemudahan chatting melalui Internet dalam hal yang tidak berkaitan dengan urusan kerja. ix. Memuat turun, menyimpan dan menggunakan	

	perisian peer to peer. x. Menggunakan kemudahan Internet untuk tujuan peribadi. xi. Menjalankan aktiviti-aktiviti komersial dan politik. xii. Melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas. xiii. Menggunakan sebarang perkakasan yang berfungsi sebagai modem ke atas komputer dalam rangkaian kerajaan untuk membuat capaian terus ke Internet. h) Komputer peribadi yang digunakan untuk mencapai Internet mesti dilengkapi dengan ciri-ciri keselamatan tambahan seperti perisian antivirus dan anti-spyware.	
4.0	**Pengendalian Portal/Laman Web Rasmi Agensi**	
	Perkara-perkara yang perlu dipatuhi oleh Pentabir Portal/Laman Web Rasmi dalam pengendalian perkhidmatan Portal/Laman Web adalah seperti berikut: a) Notis hakcipta perlu diletakkan pada semua laman web rasmi seperti berikut : ”Hakcipta Portal Rasmi (nama Agensi) dan kandungannya yang termasuk maklumat, teks, imej, grafik, fail suara, fail video dan susunannya serta bahan-bahannya ialah kepunyaan (nama agensi) kecuali dinyatakan sebaliknya. Tiada mana-mana bahagian portal ini boleh diubah, disalin, diedar, dihantar semula, disiarkan, dipamerkan, diterbitkan, dilesenkan, dipindah, dijual atau diuruskan bagi tujuan komersial dalam apa bentuk sekalipun tanpa mendapat kebenaran secara bertulis yang jelas terlebih dahulu daripada (nama agensi). Produk-produk lain, logo dan syarikat atau organisasi yang tercatat di dalam portal ini adalah kepunyaan syarikat atau organisasi tersebut.” b) Kenyataan Penafian (Disclaimer) perlu diletakkan pada semua laman web rasmi seperti : ”Kerajaan Malaysia dan (nama agensi) adalah tidak	Pentadbir Portal Laman Web

	bertanggungjawab bagi apa-apa kehilangan atau kerugian yang disebabkan oleh penggunaan mana-mana maklumat yang diperolehi dari portal ini serta tidak boleh ditafsirkan sebagai ejen kepada, ataupun syarikat yang disyorkan oleh (nama agensi)." c) Dasar Privasi dan Keselamatan perlu diletakkan pada semua laman web rasmi seperti : "Halaman ini menerangkan dasar privasi yang merangkumi penggunaan dan perlindungan maklumat yang dikemukakan oleh pengunjung. Sekiranya anda membuat transaksi atau menghantar e-mel mengandungi maklumat peribadi, maklumat ini mungkin akan dikongsi bersama dengan agensi awam lain untuk membantu penyediaan perkhidmatan yang lebih berkesan dan efektif. Contohnya seperti di dalam menyelesaikan aduan yang memerlukan maklumbalas dari agensi-agensi lain."	
5.0	**Perkhidmatan Simpanan Data Atas Talian (*Cloud Storage*)**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap dokumen rasmi hanya dibenarkan disimpan di Perkhidmatan Cloud Storage yang disediakan. b) Dokumen terperingkat yang disimpan di public cloud storage hendaklah menggunakan kaedah encryption terlebih dahulu sebelum dimuatnaik. c) Setiap dokumen yang disimpan di atas talian perlu ditetapkan kata laluan untuk membuka dokumen. d) Memuatnaik data peribadi ke dalam perkhidmatan cloud storage rasmi adalah dilarang sama sekali.	
0807 PEMANTAUAN		
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan		
1.0	**Pengauditan dan Forensik Digital**	
	ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem	

	ICT Kerajaan Negeri Kedah; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), 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 mengedar 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 jalur lebar (*bandwidth*) rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	ICTSO
2.0	**Jejak Audit**	
	Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod 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 maklumat-maklumat berikut: a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan	Pentadbir Sistem ICT

	aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa 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.	
3.0	**Sistem Log**	
	Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
4.0	**Pemantauan Log**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log Audit yang merekodkan semua aktiviti perlu	Pentadbir Sistem ICT

	dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; f) Waktu yang berkaitan dengan sistem pemprosesan maklumat atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	
5.0	**Lain-Lain Perkhidmatan**	
	Lain-lain perkhidmatan atau utiliti yang mempunyai risiko terhadap pendedahan maklumat rasmi jabatan /agensi negeri serta Kerajaan Negeri Kedah dan keselamatan ICT secara langsung atau tidak langsung adalah dilarang tanpa kebenaran CIO dan / atau ICTSO	Semua

Perkara 09 Kawalan Capaian

0901 DASAR KAWALAN CAPAIAN		
Objektif : Mengawal capaian ke atas maklumat		
1.0	**Keperluan Kawalan Capaian**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendakalah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	Semua
0902 PENGURUSAN CAPAIAN PENGGUNA		
Objektif : Mengawal capaian pengguna ke atas aset ICT Kerajaan Negeri		
1.0	**Akaun Pengguna**	
	Setiap pengguna adalah bertanggungjawab ke atas	Semua

	sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Semua pengguna sistem ICT mestilah mempunyai ID pengguna (user ID) dan kata laluan (password) masing-masing dan bertanggungjawab terhadapnya. b) Penggunaan teknologi tambahan seperti kad-kad pintar dan teknologi biometric authentication perlu dipertimbangkan untuk sistem yang terperingkat. c) Pengguna disarankan mengadakan kemudahan password screen saver atau log off sekiranya meninggalkan komputer. d) ID pengguna dan kata laluan tidak boleh dikongsi. e) Kata laluan mesti sekurang-kurangnya lapan aksara dan mempunyai kombinasi huruf, nombor dan aksara khas. f) Kata laluan perlu ditukar sekurang-kurangnya setiap tiga (3) bulan sekali. g) Pemilikan akaun pengguna bukanlah hak milik mutlak seseorang dan ia tertakluk kepada peraturan jabatan / agensi. Akaun boleh ditarik balik jika penggunanya melanggar peraturan. h) Akaun pengguna akan ditamatkan atas sebab-sebab seperti berikut : i. Bersara ii. Ditamatkan perkhidmatan iii. Bertukar ke jabatan / agensi lain iv. Bertukar bidang tugas kerja v. Menyalahguna kemudahan akaun ICT yang diberikan i) Akaun pengguna disaran dibekukan sepanjang tempoh pengguna bercuti panjang atau menghadiri	

	kursus di luar pejabat dalam tempoh melebihi sebulan.	
2.0	**Kawalan Akses**	
	Setiap keperluan akses mestilah dirancang dan didokumentasikan berdasarkan kawalan akses dan klasifikasi maklumat. Pengguna mestilah dimaklumkan mengenai tahap akses yang ditetapkan	Pemilik Sistem dan Pentadbir Sistem ICT
3.0	**Perakaunan Dan Jejak Audit (Audit Trail)**	
	a) Semua perkakasan / utiliti mestilah mengaktifkan audit log. Audit log perlu disimpan sekurang-kurangnya dalam tempoh setahun sebelum dilupuskan. b) Semua laporan log / audit trail dan program atau utiliti mestilah dikawal dan hanya boleh diakses oleh Pentadbir Sistem dan personel keselamatan sahaja. c) Aktiviti-aktiviti Pentadbir Sistem mestilah dilogkan. d) Sebarang cubaan memasuki sistem (login) yang tidak berjaya mestilah dilogkan dan perlu diberi perhatian. e) Penggera keselamatan boleh dipertimbangkan untuk memberikan amaran kepada Pentadbir Sistem secara automatik sebagai tanda peringatan. f) Pentadbir Sistem dan Pentadbir Rangkaian dikehendaki menganalisa log / audit trail sekurang-kurangnya sekali dalam seminggu. g) Semua sistem komputer dan peranti rangkaian mestilah mempunyai catatan masa yang seragam bagi memastikan kesahihan masa yang tercatat dalam audit log. Pentadbir Sistem harus menentukan penyatuan masa sekurang-kurangnya sekali dalam sebulan.	Pemilik Sistem dan Pentadbir Sistem ICT

4.0	***Clear Desk* dan *Clear Screen***	
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan *password screen saver* atau *logout* 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 faksimile dan mesin fotostat.	Semua
0903 KAWALAN CAPAIAN APLIKASI DAN SISTEM MAKLUMAT		
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi		
1.0	**Capaian Aplikasi dan Sistem Maklumat**	
	Bertujuan melindungi aplikasi dan sistem maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian aplikasi dan sistem maklumat yang kukuh, perkara-perkara berikut hendaklah dipatuhi: a) Capaian sistem dan aplikasi adalah terhad kepada pengguna dan tujuan yang dibenarkan.	Pentadbir Sistem ICT dan ICTSO

	b) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan. c) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini. d) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dan sebarang bentuk penyalahgunaan. e) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. f) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	
0904 KAWALAN CAPAIAN RANGKAIAN		
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.		
1.0	**Capaian Rangkaian**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Kedah*Net, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT dan ICTSO

2.0	**Capaian Internet**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ 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	Pentadbir Rangkaian Pengurus ICT Semua

	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; j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; k) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
0905 KAWALAN CAPAIAN SISTEM PENGOPERASIAN		
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.		
1.0	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer.	Pentadbir Sistem ICT dan ICTSO

	Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian system pengoperasian terutama pengguna bertaraf *super user;* c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Menghadkan dan mengawal penggunaan program; d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
2.0	**Kad Pintar**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;	Semua

	c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian Pentadbiran.	
0906 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH (*REMOTE*)		
Objektif : Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh (*remote*)		
1.0	**Keselamatan Aset ICT Mudah Alih / Komputer Riba**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. b) Instalasi perisian komputer mudah alih mestilah dilaksanakan oleh kakitangan ICT. c) Komputer mudah alih hendaklah sentiasa di bawah penjagaan yang rapi bagi menjamin keselamatannya dari kecurian dan kerosakan. d) Pengguna yang membawa maklumat terperingkat dikehendaki mengisytiharkannya dengan mendapat kebenaran bertulis dari Ketua Jabatan atau setaraf. e) Pengguna yang menggunakan komputer mudah alih persendirian untuk tugas perkhidmatan mestilah mendapat kelulusan bertulis daripada Ketua Jabatan dan setaraf serta tertakluk kepada tindakan, pengawasan dan pemantauan bahagian ICT jabatan / agensi yang berkaitan. f) ICTSO dengan bantuan bahagian ICT jabatan / agensi yang berkaitan mempunyai hak untuk	Semua

	membuat sebarang proses penghapusan atau pemindahan sebarang maklumat jabatan daripada pegawai yang menggunakan komputer riba persendirian sekiranya pegawai tersebut berpindah, bersara atau diberhentikan perkhidmatannya.	
2.0	**Kerja Jarak Jauh (*Remote*)**	
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan b) Menggunakan perisian yang sah yang dibekalkan oleh Sistem Pengoperasian (*Operating System*) c) Mendapatkan kebenaran dari pemilik sistem jika ingin akses ke komputer/pelayan dari luar premis	Semua

Perkara 10 Pengurusan Keselamatan Sistem Aplikasi

1001 KESELAMATAN DALAM MEMBANGUNKAN SISTEM DAN APLIKASI		
Objektif : Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian		
1.0	**Keperluan Keselamatan Sistem Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pembangunan 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 : i. Sistem input untuk menyemak pengesahan dan	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

	integriti data yang dimasukkan. ii. Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna. iii. 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. 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.	
2.0	**Pengesahan Data *Input* Dan *Output***	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT
1002 KAWALAN KRIPTOGRAFI (*CRYPTOGRAPHY*)		
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi		
1.0	**Pengurusan**	
	a) Maklumat terperingkat atau maklumat rahsia rasmi hendaklah melalui proses penyulitan (*encryption*) setiap masa sebelum dihantar atau disalurkan ke dalam sistem rangkaian yang umum seperti Internet, Mobil-GSM, Infrared dan sebagainya. b) Penggunaan tandatangan digital adalah disyorkan	Semua

	kepada semua pengguna khususnya mereka yang menguruskan transaksi atau maklumat rahsia rasmi secara elektronik setiap masa. c) Pengurusan Infrastruktur Kunci Awam (*Public Key Infrastructure - PKI*) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	
1003 KESELAMATAN FAIL SISTEM		
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat		
1.0	**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) Mengawal capaian ke atas kod aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. c) Mengaktifkan audit log bagi merekodkan semua pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem ICT
1004 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN		
Objektif : Menjaga dan menjamin keselamatan maklumat dan aplikasi		
1.0	**Prosedur Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut; a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji,	Pentadbir Sistem ICT

	direkodkan dan disahkan sebelum digunapakai. b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan buruk terhadap operasi dan keselamatan agensi. Individu atau sesuatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor. c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja d) Akese kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan dan e) Menghalang sebaran peluang untuk membocorkan maklumat.	
2.0	**Pembangunan Perisian Secara Outsource**	
	Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (Source Code) bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan Negeri.	Seksyen Pembangunan dan Pengurusan Sistem
1005 KAWALAN TEKNIKAL KETERDEDAHAN (*VULNERABILITY*)		
Objektif : Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.		
1.0	**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:	Pentadbir Sistem ICT

	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; c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

Perkara 11 Pengurusan Kesinambungan Perkhidmatan Dan Pemulihan Bencana

1101 KESINAMBUNGAN PERKHIDMATAN		
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan		
1.0	**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 hendaklah dibentang dan dipersetujui oleh Jawatankuasa Pemandu ICT. Perkara-perkara berikut perlu diberi perhatian: I. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; II. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut akibat terhadap keselamatan ICT; III. Melaksanakan prosedur-prosedur kecemasa	Ketua Jabatan Dan ICTSO

	bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; IV. Mendokumentasikan proses dan prosedur yang telah dipersetujui; V. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; VI. Membuat backup; dan VII. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: I. Senarai aktiviti teras yang dianggap kritikal mengikut sususan keutamaan; II. Senarai personel kakitangan terlibat dan vendor beserta nombor yang boleh dihubungi (Telefon dan emel). senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir bagi menangani insiden; III. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; IV. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan V. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana yang boleh. Salinan Pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana alam atau bencana manusia di lokasi utama.	

2.0	**Perubahan atau Pengecualian BCM**	
	Sekiranya terdapat perubahan/pengemaskinian atau pengecualian yang perlu dilakukan, permintaan secara bertulis termasuk keterangan dan kebenaran untuk pengecualian/perubahan hendaklah dikemukakan kepada Ketua Jabatan atau Ketua Bahagian.	
3.0	**Program Latihan dan Kesedaran Terhadap BCM**	
	Semua penjawat awam perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap BCP. Ketua Jabatan atau Ketua Bahagian bertanggung jawab dalam memastikan latihan dan program kesedaran terhadap BCM dilaksanakan.	ICTSO
5.0	**Pengujian BCM**	
	Pelan BCM perlu diuji satu kali setahun atau selepas perubahan utama, atau yang mana terdahulu bagi memastikan semua pihak yang berkenaan mengetahui dan maklum akan pelaksanaannya; Salinan BCM mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; Ujian BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; SUK hendaklah memastikan salinan Pelan Kesinambungan Perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama; dan Komponen BCM seperti Pelan Pemulihan Bencana (*Disaster Recovery Plan–DRP*), Pelan Komunikasi Krisis (*Crisis Communication Plan–CCP*) dan Pelan Tindak Balas Kecemasan (*Emergency Response Plan–ERP*)	Ketua Jabatan Dan ICTSO

	perlu diuji satu kali setahun atau selepas perubahan utama, atau yang mana terdahulu.	

Perkara 12 Pematuhan

1201 PEMATUHAN DASAR DAN TERMA		
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT Negeri		
1.0	**Pematuhan Dasar**	
	a) Setiap pengguna hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Negeri serta undang-undang atau peraturan-peraturan lain yang berkaitan yang telah berkuatkuasa. b) Semua aset ICT termasuk maklumat yang disimpan di dalamnya adalah hak milik kerajaan dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. c) Sebarang penggunaan aset ICT Kerajaan Negeri selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan Negeri.	Semua
2.0	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

3.0	**Pematuhan Keperluan Audit**	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. 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
4.0	**Keperluan Perundangan Dan Peraturan**	
	Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di Kerajaan Negeri adalah seperti di Lampiran	Semua
5.0	**Perlindungan dan Privasi Data Peribadi**	
	Semua penjawat awam perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik agensi. Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT. Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian. Pihak pengurusan agensi berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi dasar ini. Pihak agensi menggalakkan dasar privasi yang adil. Pihak pengurusan perlu bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat. Pendedahan maklumat peribadi tentang kakitangan agensi kepada pihak ketiga	Semua

	tidak sepatutnya berlaku kecuali: (a) Dikehendaki oleh undang-undang atau peraturan; (b) Dengan persetujuan yang jelas dan nyata daripada kakitangan tersebut; atau (c) Setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh Unit Undang-undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia.	
6.0	**Akuan Pematuhan Dasar Keselamatan ICT**	
	Adalah menjadi tanggungjawab Ketua Jabatan dan Ketua Bahagian untuk memastikan setiap penjawat awam negeri Kedah menandatangani Akuan Pematuhan Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT). Akuan Pematuhan adalah seperti di **LAMPIRAN A(I)**	Semua

LAMPIRAN A(I)

A) Kakitangan Kerajaan Negeri/Persekutuan

AKUAN PEMATUHAN
DASAR KESELAMATAN ICT
PEJABAT SETIAUSAHA KERAJAAN NEGERI KEDAH

NAMA (HURUF BESAR) : _____
NO. KAD PENGENALAN : _____
JAWATAN DAN GRED : _____
AGENSI/JABATAN : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Negeri Kedah*; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN : _____
TARIKH : _____

Pengesahan Pegawai Keselamatan ICT

_____
(Tandatangan dan Cop Jawatan)
Tarikh : _____

*Dasar Keselamatan ICT Negeri Kedah boleh dicapai menerusi http://www.kedah.gov.my

LAMPIRAN A(II)

B) Firma/Syarikat

AKUAN PEMATUHAN
DASAR KESELAMATAN ICT
PEJABAT SETIAUSAHA KERAJAAN NEGERI KEDAH

NAMA (HURUF BESAR) : _____
NO. KAD PENGENALAN : _____
JAWATAN : _____
FIRMA/SYARIKAT : _____
NO. PENDAFTARAN SYARIKAT : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

3. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Negeri Kedah*; dan

4. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN : _____
TARIKH : _____

Pengesahan Pegawai Keselamatan ICT

_____
(Tandatangan dan Cop Jawatan)
Tarikh : _____

*Dasar Keselamatan ICT Negeri Kedah boleh dicapai menerusi http://www.kedah.gov.my

LAMPIRAN B(I)

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM NEGERI ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN NEGERI BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah Seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Kebawah Duli Yang Maha Mulia Tuanku Sultan Kedah Darul Aman atau perkhidmatan mana-mana Agensi dan Jabatan Kerajaan Negeri, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Kebawah Duli Yang Maha Mulia Tuanku Sultan Kedah Darul Aman atau dengan mana-mana Agensi dan Jabatan Kerajaan Negeri dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Kebawah Duli Yang Maha Mulia Tuanku Sultan Kedah Darul Aman atau perkhidmatan mana-mana Agensi dan Jabatan Kerajaan Negeri telah selesai.

TANDATANGAN : _____
NAMA (HURUF BESAR) : _____
NO. KAD PENGENALAN : _____
JAWATAN : _____
AGENSI/JABATAN : _____
TARIKH : _____

DISAKSIKAN OLEH

_____
(Tandatangan)

NAMA (HURUF BESAR) : _____
NO. KAD PENGENALAN : _____
JAWATAN : _____
AGENSI/JABATAN : _____
TARIKH : _____

CAP AGENSI/JABATAN

LAMPIRAN B(II)

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM NEGERI ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN NEGERI APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN KERAJAAN NEGERI BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah Seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Kebawah Duli Yang Maha Mulia Tuanku Sultan Kedah Darul Aman atau dengan mana-mana Agensi dan Jabatan Kerajaan Negeri, sama ada di Malaysia atau di luar negara, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Kebawah Duli Yang Maha Mulia Tuanku Sultan Kedah Darul Aman atau dengan mana-mana Agensi dan Jabatan Kerajaan Negeri.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri atau cap bagi atau yang dipunyai atau diguna, dibuat atau diadakan oleh mana-mana Agensi dan Jabatan Kerajaan Negeri yang tidak dibenarkan berada dalam milikan atau kawalan saya

TANDATANGAN : _____
NAMA (HURUF BESAR) : _____
NO. KAD PENGENALAN : _____
JAWATAN : _____
AGENSI/JABATAN : _____
TARIKH : _____

DISAKSIKAN OLEH

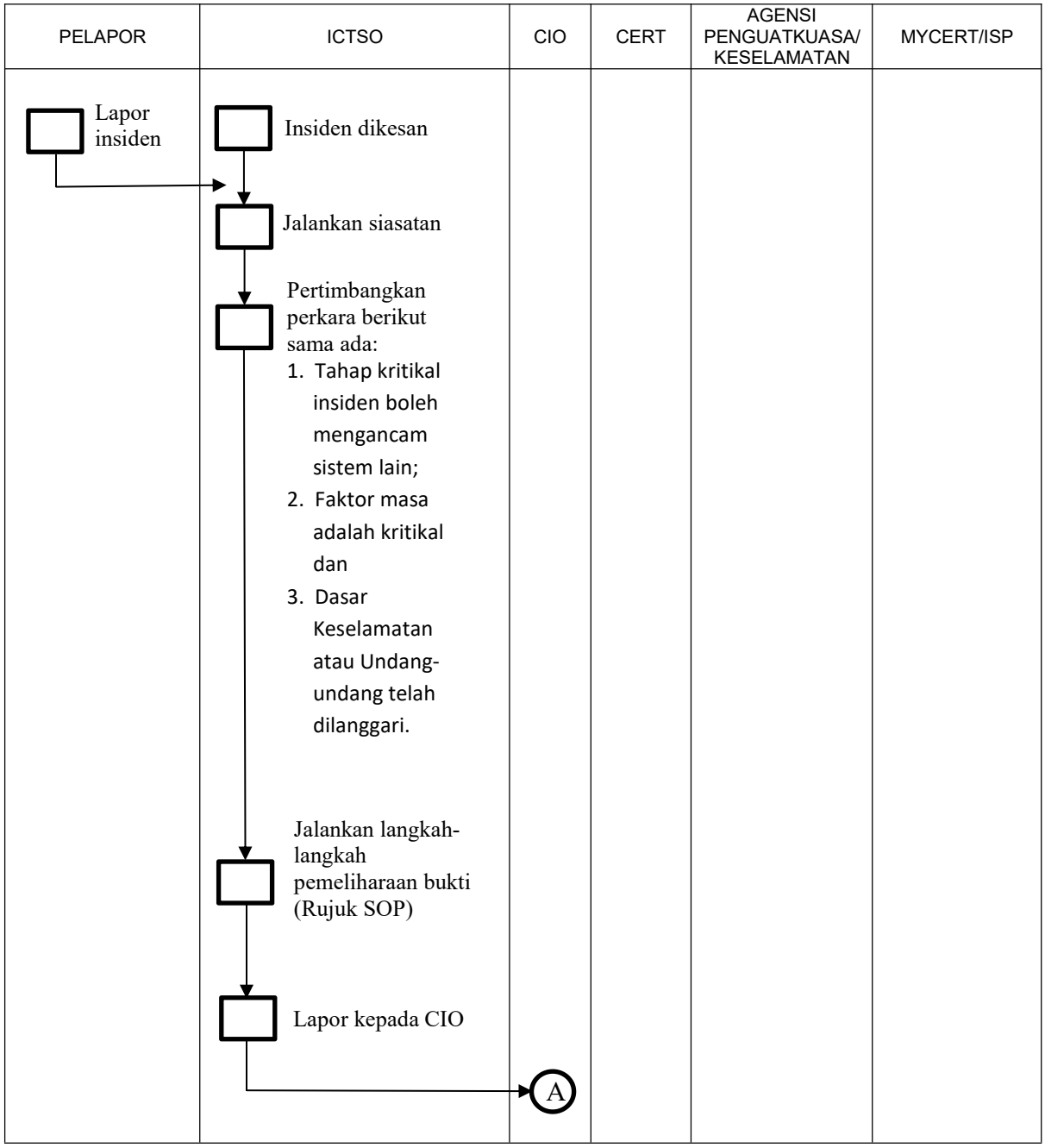
_____
(Tandatangan)

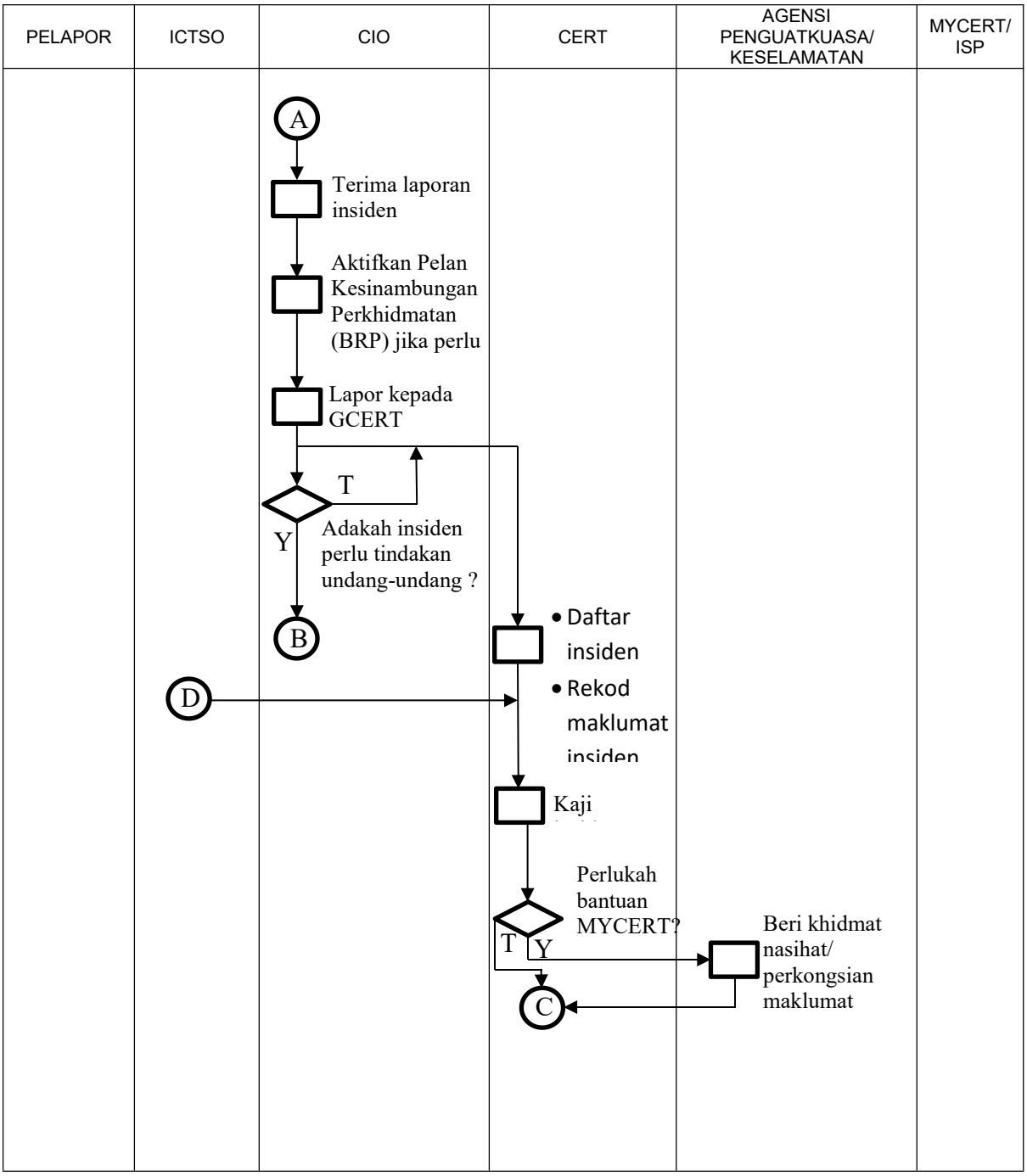
NAMA (HURUF BESAR) : _____
NO. KAD PENGENALAN : _____
JAWATAN : _____
AGENSI/JABATAN : _____
TARIKH : _____

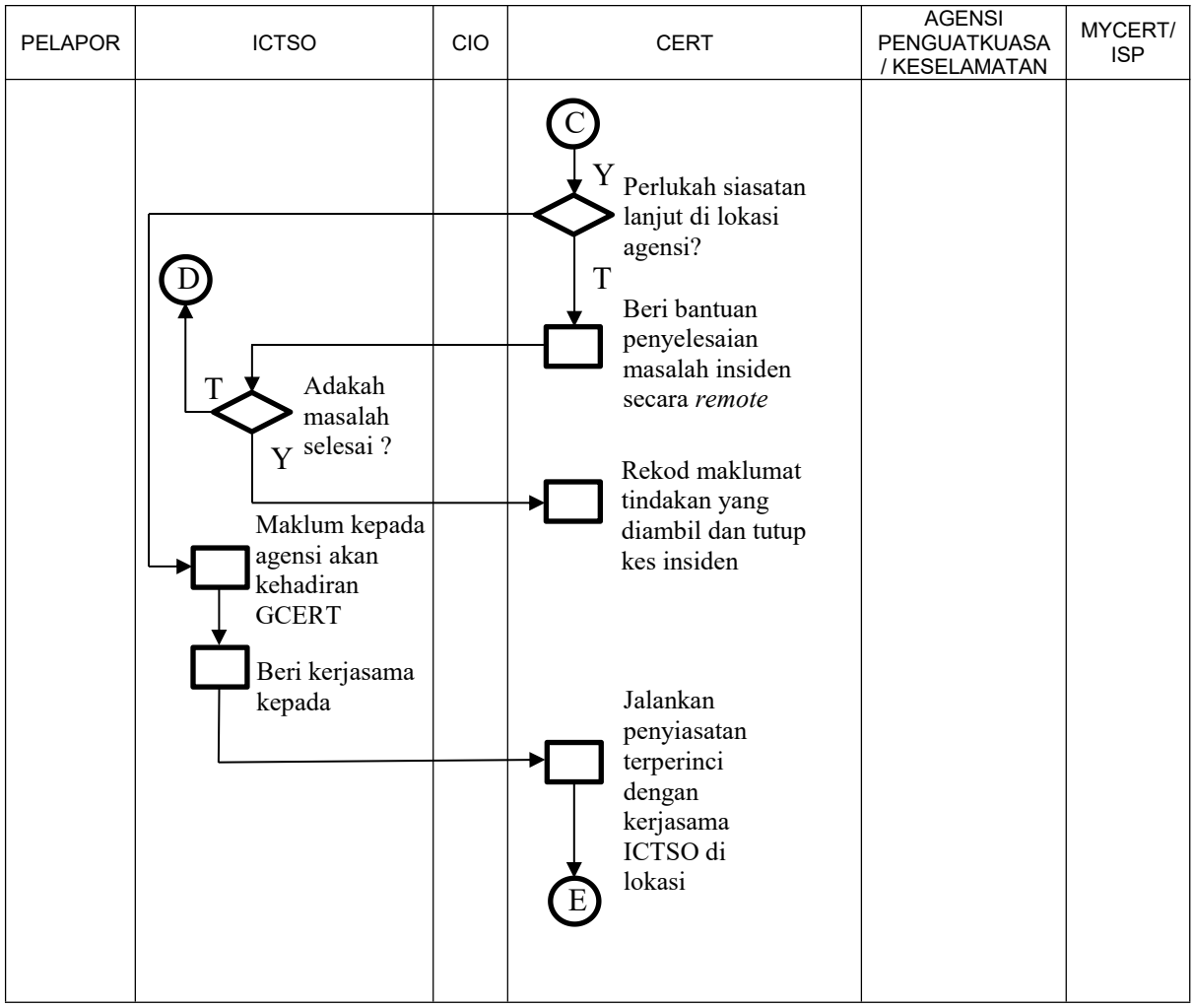
CAP AGENSI/JABATAN

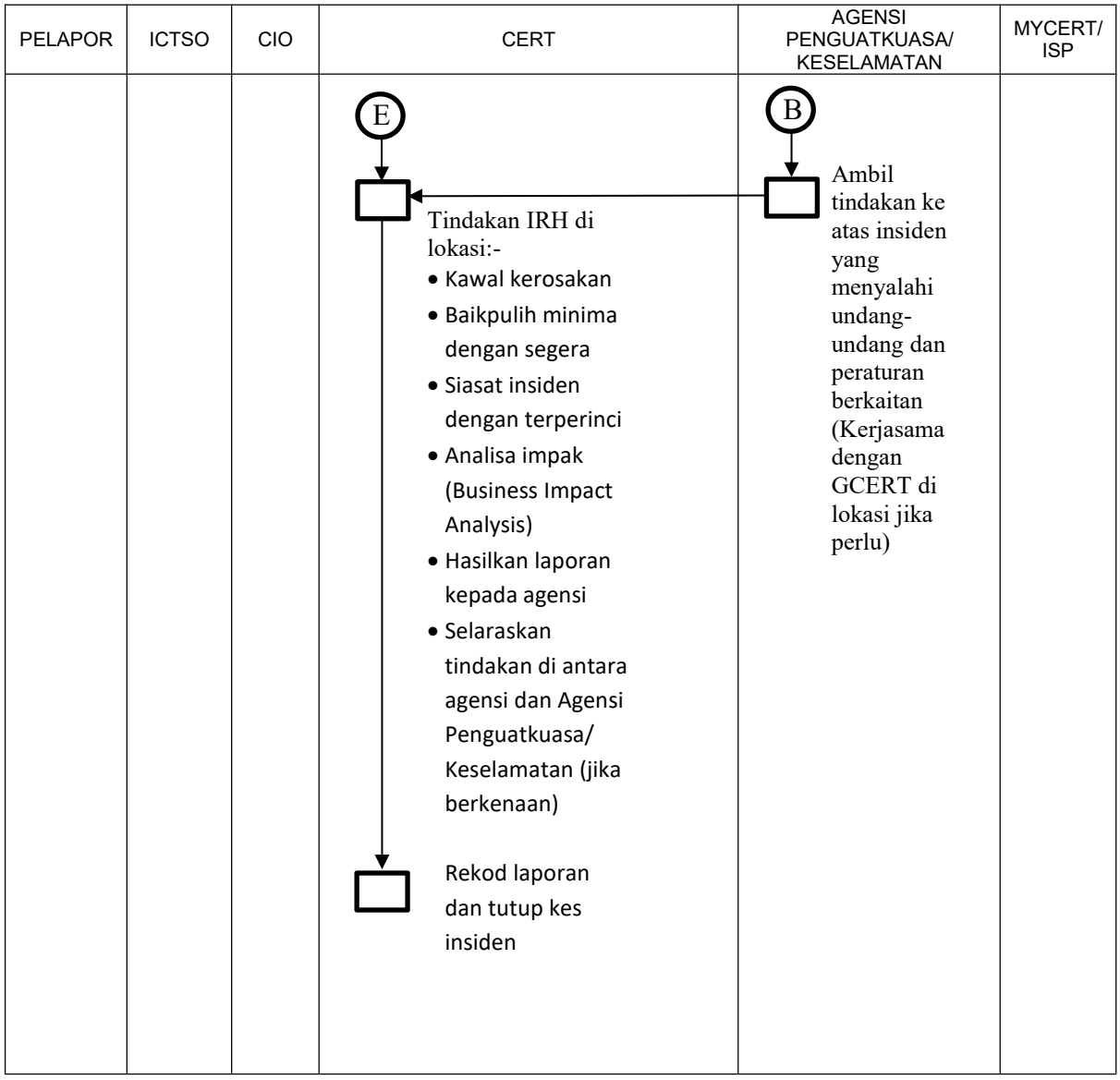
LAMPIRAN C

Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Pejabat SUK Kedah




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


PELAPOR
ICTSO
CIO
CERT
AGENSI PENGUATKUASA / KESELAMATAN
MYCERT/ ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
Beri bantuan penyelesaian masalah insiden secara *remote*
D
T
Adakah masalah selesai ?
Y
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran GCERT
Beri kerjasama kepada
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E


PELAPOR
ICTSO
CIO
CERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
E
B
Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan (Kerjasama dengan GCERT di lokasi jika perlu)
Tindakan IRH di lokasi:-
• Kawal kerosakan
• Baikpulih minima dengan segera
• Siasat insiden dengan terperinci
• Analisa impak (Business Impact Analysis)
• Hasilkan laporan kepada agensi
• Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)
Rekod laporan dan tutup kes insiden

RUJUKAN

1. ”Dasar Keselamatan ICT”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2006
2. ”Malaysian Public Sector ICT Security Risk Assessment Methodology”, Surat Pekeliling Am Bilangan 6, Jabatan Perdana Menteri, 2005
3. “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan“, Pekeliling Am Bilangan 1, Jabatan Perdana Menteri, 2003
4. “Dasar Keselamatan ICT”, Bahagian Teknologi Maklumat, Kementerian Pertahanan Malaysia, 2002
5. ”Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”, Pekeliling Am Bilangan 1, Jabatan Perdana Menteri, 2001
6. ”Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan”, Pekeliling Am Bilangan 3, Jabatan Perdana Menteri, 2000
7. Arahan Keselamatan Malaysia
8. ”Dasar Keselamatan ICT”, Bahagian Teknologi Maklumat, Kementerian Kesihatan Malaysia, 2007
9. Arahan Teknologi Maklumat, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2007
10. ”Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2006
11. ”Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2002
12. “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan“, Pekeliling Kemajuan dan Pentadbiran Am, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2003
13. SIRIM, MS ISO / IEC 27001 Information Security Management System Standard Malaysia, 2006
14. ”Dasar Keselamatan ICT”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, Versi 5.3 Mei 2010