PEJABAT SETIAUSAHA
KERAJAAN NEGERI PERLIS

PKS
2025

POLISI KESELAMATAN SIBER

VERSI 2.0

KERAJAAN
NEGERI PERLIS

Polisi Keselamatan SIBER

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
7 April 2023	1.0	Minit Mesyuarat Jawatankuasa Pemandu Bil.1/2023	2023
3 Julai 2025	2.0	Minit Mesyuarat Jawatankuasa Pemandu Bil.1/2025	2025

ISI KANDUNGAN

TAKRIFAN

Bagi maksud pemakaian Polisi Keselamatan Siber Kerajaan Negeri Perlis ini:

TAKRIFAN	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Backup (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
CCTV *(ClosedCircuit Television System)*	Sistem TV yang digunakan secara komersial di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CDO	*Chief Digital Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
Escrow (eskrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bilabila masa.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi keduaduanya.

TAKRIFAN	
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat *(information theft/espionage)*, penipuan *(hoaxes)*.
CERT JDN	Pasukan Tindak Balas Insiden Keselamatan (*Computer Emergency Response Team* – CERT) atau ICT JDN.
ICT	*Information and Communication Technology*
ICTSO	*ICT Security Officer* (ICTSO) Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Kesela-matan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafiktrafik dalam rangkaianrangkaian tersebut agar sentiasa berasingan.
Intrusion Detec-tion System (IDS)	Sistem Pengesan Pencerobohan Perisian (Instrusion Detection System – IDS) atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.

TAKRIFAN	
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan (Instrusion Prevention System – IPS) keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: Networkbased IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
ISMS	Sistem Pengurusan Keselamatan Maklumat (*Information Security Management System* – ISMS)
JDN	Jabatan Digital Negara
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
Local Area Network (LAN)	Rangkaian Kawasan Setempat (Local Area Network – LAN) yang menghubungkan komputer.
NACSA	Agensi Keselamatan Siber Negara (National Cyber Security Agency - NACSA) adalah sebagai agensi utama negara bagi hal ehwal keselamatan siber di Malaysia. NACSA ditubuhkan pada Februari 2017 sebagai agensi peneraju dalam usaha memperkukuh keselamatan siber negara.
Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem

TAKRIFAN

	aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
PSUKPs	Pejabat Setiausaha Kerajaan Negeri Perlis
Rollback (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Ruang siber	Sistemsistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistemsistem tersebut, manusia yang berinteraksi dengan sistemsistem tersebut secara fizikal atau maya serta persekitaran fizikal sistemsistem tersebut dan semua aset yang berkaitan dengan ICT.
Screen saver	Paparan yang akan diaktifkan pada sistem komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Adalah sebuah sistem komputer yang menyediakan jenis layanan *(service)* tertentu dalam jaringan komputer.
Source Code	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.

PENGENALAN

Polisi Keselamatan Siber (PKS) Kerajaan Negeri Perlis mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan perkhidmatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan Negeri Perlis. Polisi ini juga menerangkan kepada semua pengguna di bawah Pentadbiran Kerajaan Negeri Perlis mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Kerajaan Negeri Perlis. Polisi ini disediakan berpandu kepada piawaian antarabangsa iaitu ISO/IEC 27001:2022 *Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems*.

OBJEKTIF

Polisi Keselamatan Siber ini diwujudkan untuk menjamin kesinambungan urusan Pentadbiran Kerajaan Negeri Perlis dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi Pentadbiran Kerajaan Negeri Perlis bagi memastikan semua maklumat dilindungi.

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

i. Menerangkan kepada semua pengguna merangkumi warga Pentadbiran Kerajaan Negeri Perlis, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;
ii. Memastikan keselamatan penyampaian perkhidmatan Kerajaan Negeri Perlis di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;
iii. Memastikan kelancaran operasi Kerajaan Negeri Perlis dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

iv. Melindungi kepentingan pihakpihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
v. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT; dan

Polisi Keselamatan Siber ini merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciriciri utama keselamatan maklumat adalah seperti berikut:

i. **Kerahsiaan** – Maklumat tidak boleh didedahkan sewenangwenangnya 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; dan
v. **Ketersediaan** – Data dan maklumat hendaklah boleh diakses pada bi-

Selain dari itu, langkahlangkah 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 langkahlangkah pencegahan yang sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan sistem perisian) dan fizikal (contoh: komputer, peralatan komunikasi dan media magnet). Polisi ini adalah terpakai oleh semua pengguna di bawah Pentadbiran Kerajaan

Negeri Perlis termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan perkhidmatan ICT Kerajaan Negeri Perlis.

PRINSIPPRINSIP

Prinsipprinsip yang menjadi asas kepada Polisi Keselamatan Siber Kerajaan Negeri Perlis 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 atas dasar 'perlu mengetahui' sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).

b) Hak Akses Minimum

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

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap Aset ICT Kerajaan Negeri Perlis.

d) Pengasingan

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak

dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

e) Pengauditan

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

f) Pematuhan

Polisi Keselamatan Siber Kerajaan Negeri Perlis hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan.

h) Saling Bergantungan

Setiap prinsip di atas adalah saling lengkapmelengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan perkhidmatan ICT yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

Kerajaan Negeri Perlis hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kerentanan (*vulnerability*) yang semakin meningkat hari ini. Justeru itu, warga Pentadbiran Kerajaan Negeri Perlis perlu mengambil langkahlangkah proaktif dan bersesuaian untuk menilai tahap risiko perkhidmatan ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas perkhidmatan ICT.

Pentadbiran Kerajaan Negeri Perlis hendaklah melaksanakan Penilaian Risiko Keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan atau langkahlangkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian Risiko Keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat Kerajaan Negeri Perlis termasuklah aplikasi, perisian, pelayan, rangkaian dan proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumbersumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistemsistem sokongan lain.

Kerajaan Negeri Perlis bertanggungjawab melaksanakan dan menguruskan Penilaian Risiko Keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam. Kerajaan Negeri Perlis perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

i. Melaksana proses pengurusan risiko keselamatan maklumat secara berkala yang boleh dibuat secara dalaman (*inhouse*) atau melalui perkhidmatan pihak ketiga yang bertauliah;
ii. Melaksana aktiviti penilaian risiko dan penguraian risiko secara berulang sehingga pengurusan atasan organisasi berpuas hati dengan maklumat

dan hasil bagi aktiviti tersebut;

iii. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

iv. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihakpihak yang berkepentingan.

1. KAWALAN ORGANISASI

Objektif: Memastikan polisi keselamatan maklumat bersesuaian, berterusan dan seiring dengan hala tuju pengurusan dalam menyokong keselamatan maklumat selari dengan fungsi Kerajaan Negeri Perlis, undangundang dan keperluan kontrak perjanjian.

1.1 Polisi Keselamatan Maklumat

1.1.1 Pelaksanaan Polisi

Peranan: YB Setiausaha Kerajaan Negeri Perlis, CDO, ICTSO, SUB dan Ketua Jabatan

Pelaksanaan Polisi ini akan dijalankan oleh YB Setiausaha Kerajaan Negeri Perlis dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan semua Setiausaha Bahagian (SUB) dan Ketua Jabatan Negeri.

1.1.2 Penyebaran Polisi

Peranan: ICTSO

Polisi ini perlu disebarkan kepada semua warga Pentadbiran Kerajaan Negeri Perlis (termasuk kakitangan, pembekal, pakar runding dan lainlain)

1.1.3 Penyelenggaraan Polisi

Peranan: JPICT/CDO/ICTSO

Polisi Keselamatan Siber Kerajaan Negeri Perlis 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 Polisi Keselamatan Siber Kerajaan Negeri Perlis:

i. Kenal pasti dan tentukan perubahan yang diperlukan;
ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada Jawatankuasa Pemandu ICT (JPICT) bagi tujuan pengesahan;
iii. Perubahan yang telah disahkan oleh JPICT dimaklumkan kepada semua warga kerja Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis; dan
iv. Polisi ini hendaklah dikaji semula setiap lima (5) tahun sekali atau mengikut keperluan semasa.

1.1.4 Pengecualian Polisi

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, Pembekal dan Pihak yang mempunyai urusan dengan ICT Kerajaan Negeri Perlis

i. Polisi Keselamatan Siber Kerajaan Negeri Perlis adalah terpakai kepada semua pengguna maklumat Kerajaan Negeri Perlis dan tiada pengecualian diberikan.
ii. Apabila sesuatu keperluan untuk pengecualian terhadap kepatuhan polisi ini harus dikemukakan kepada ICTSO dan mendapat perakuan JPICT.

1.1.5 Pematuhan Polisi

Setiap pengguna di bawah Kerajaan Negeri Perlis hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber Kerajaan Negeri Perlis dan undangundang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di Kerajaan Negeri Perlis termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

1.2 Tanggungjawab dan Peranan Keselamatan Maklumat

Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber Kerajaan Negeri Perlis

1.2.1 YB Setiausaha Kerajaan Negeri

Peranan: YB Setiausaha Kerajaan Negeri Perlis

Peranan dan tanggungjawab YB Setiausaha Kerajaan Negeri Perlis adalah seperti berikut:

i. Memastikan penguatkuasaan pelaksanaan Polisi Keselamatan Siber Kerajaan Negeri Perlis;
ii. Memastikan semua warga kerja Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT memahami dan mematuhi peruntukanperuntukan di bawah polisi ini;
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 Polisi Keselamatan ICT Kerajaan Negeri Perlis;

v. Melantik *Chief Digital Officer* (CDO) dan *ICT Security Officer* (ICTSO); dan

vi. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT

1.2.2. Ketua Pegawai Digital (CDO)

Peranan: CDO

Timbalan Setiausaha Kerajaan (Pengurusan) adalah merupakan CDO. Peranan dan tanggungjawab beliau adalah seperti berikut:

i. Membantu YB Setiausaha Kerajaan Negeri Perlis dalam melaksanakan tugastugas yang melibatkan keselamatan ICT seperti yang ditetapkan di dalam polisi ini;

ii. Memastikan kawalan keselamatan maklumat diseragam dan diselaraskan dengan sebaiknya; dan

iii. Menyelaras pelan latihan dan program kesedaran mengenai keselamatan ICT.

1.2.3. Pegawai Keselamatan ICT (ICTSO)

Peranan: ICTSO

Setiausaha Bahagian (SUB) Teknologi Maklumat (TM) adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab SUB (TM) adalah seperti berikut:

i. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan polisi ini;

ii. Menjalankan pengurusan risiko;

iii. Menjalankan audit keselamatan ICT, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

iv. Menyedia dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi

khidmat nasihat serta menyediakan langkahlangkah perlindungan yang bersesuaian;

v. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkahlangkah baik pulih dengan segera;

vi. Melaporkan insiden keselamatan ICT kepada pihak *National Cyber Security Agency* (NACSA) dan seterusnya membantu dalam penyiasatan atau pemulihan; dan

vii. Menyedia dan merangka programprogram kesedaran

1.2.4. Setiausaha Bahagian (SUB) dan Ketua Jabatan Negeri Perlis

Peranan: SUB dan Ketua Jabatan

SUB adalah pengurusan atasan bagi bahagian di bawah pentadbiran SUK Negeri Perlis manakala Pengarah Jabatan Negeri Perlis adalah pengurusan atasan bagi jabatan dan agensi di bawah Kerajaan Negeri Perlis. Peranan dan tanggungjawab SUB dan Pengarah Jabatan Negeri dalam melaksanakan Polisi ini di dalam operasi semasa adalah seperti yang berikut:

i. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkuatkuasa;

ii. Memastikan setiap warga kerja di bahagian/jabatan menandatangani Akuan Pematuhan PKS seperti di Lampiran A; dan

iii. Memastikan pembekal dan rakan usaha sama menjalani tapisan keselamatan.

1.2.5. Pentadbir Sistem ICT

Peranan: Pentadbir Sistem 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 kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber Kerajaan Negeri Perlis;
iii. Memantau aktiviti capaian sistem aplikasi;
iv. Mengenal pasti aktivitiaktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;
v. Menyimpan dan menganalisis rekod jejak audit; dan
vi. Menyediakan laporan mengenai aktiviti capaian kepada pemilik

1.2.6. Jawatankuasa Pemandu ICT (JPICT) Negeri Perlis

Peranan: YB Setiausaha Kerajaan Negeri Perlis dan CDO

Peranan dan tanggungjawab JPICT seperti berikut:

i. Menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT Jabatan;
ii. Merancang, menyelaras dan memantau pelaksanaan program atau projek ICT Jabatan;
iii. Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Pendigitalan (PSP) PSUKPs dan Pelan Strategik Pendigitalan Sektor Awam (PSPSA);

iv. Meluluskan projekprojek ICT;

v. Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isuisu yang dihadapi dalam pelaksanaan ICT;

vi. Merancang dan menentukan langkahlangkah keselamatan ICT;

vii. Mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTICT/JPICT;

viii. Menetapkan dasar dan prosedur pengurusan portal Jabatan;

1.2.7. Jawatankuasa Pelaksana ISMS Pejabat Setiausaha Kerajaan Negeri Perlis

Peranan: Jawatankuasa Pelaksana ISMS

Keanggotaan Jawatankuasa Pelaksana ISMS adalah seperti berikut:

Pengerusi : SUB (Teknologi Maklumat)
Pejabat Setiausaha Kerajaan Negeri Perlis

Ahli :

i. Pegawai Teknologi Maklumat
Bahagian Pengurusan Teknologi Maklumat

ii. Penolong Pegawai Teknologi Maklumat
Bahagian Pengurusan Teknologi Maklumat

Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS Pejabat Setiausaha Kerajaan Negeri Perlis seperti berikut:

i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan Pejabat Setiausaha Kerajaan Negeri Perlis yang telah dikenalpasti;

ii. Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS daripada ahli Mesyuarat Kajian Semula Pengurusan (MKSP) ISMS Pejabat Setiausaha Kerajaan Negeri Perlis;

Treatment Plan;

iv. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatanperkhidmatan Pejabat Setiausaha Kerajaan Negeri Perlis yang dikenal pasti;

v. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik Pejabat Setiausaha Kerajaan Negeri Perlis;

vi. Keperluan ISMS diterapkan dalam budaya kerja warga pentadbiran Kerajaan Negeri Perlis;

vii. Pencapaian sasaran ISMS seperti yang dirancang; dan

viii. Pelaksanaan program penambahbaikan dan peningkatan

1.2.8. Pasukan Tindak Balas Insiden Keselamatan ICT Perlis (PCERT)

Peranan: PCERT (Perlis CERT)

PCERT juga dikenali sebagai Pasukan Tindak Balas Insiden Keselamatan Siber (Cyber Security Incident Response Team (CSIRT)). Keanggotaan PCERT adalah seperti berikut:

Pengerusi : Timbalan Setiausaha Kerajaan (Pengurusan)/CDO, Pejabat Setiausaha Kerajaan Negeri Perlis

Ahli :

i. SUB (Teknologi Maklumat) Bahagian Pengurusan Teknologi Maklumat

ii. Pegawai Teknologi Maklumat Bahagian Pengurusan Teknologi Maklumat

iii. Pegawai Teknologi Maklumat Pejabat Perbendaharaan Negeri Perlis

iv. Pegawai Teknologi Maklumat Jabatan Tanah dan Galian Negeri Perlis

v. Pegawai Teknologi Maklumat Jabatan Kehakiman Syariah Negeri Perlis

vi. Penolong Pegawai Teknologi Maklumat

Bahagian Pengurusan Teknologi Maklumat

Peranan dan tanggungjawab Perlis CERT 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 insiden keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan;

iv. Menghubungi dan melaporkan insiden yang berlaku kepada *National Cyber Security Agency* (NACSA) sama ada sebagai input atau untuk tindakan seterusnya;

v. Merujuk jabatanjabatan di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; dan

vi. Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT

1.2.9. Pasukan Pemulihan Bencana ICT

Pengerusi :	Timbalan Setiausaha Kerajaan (Pengurusan), Pejabat Setiausaha Kerajaan Negeri Perlis
Ahli :	i. SUB (Teknologi Maklumat) Bahagian Pengurusan Teknologi Maklumat
	ii. Pegawai Teknologi Maklumat Bahagian Pengurusan Teknologi Maklumat

iii. Penolong Pegawai Teknologi Maklumat
Bahagian Pengurusan Teknologi Maklumat

Peranan dan tanggungjawab Pasukan Pemulihan Bencana adalah seperti berikut:

i. Mengenalpasti dan menentukan fungsi kritikal PSUK Perlis;
ii. Melaksanakan penilaian risiko dan analisis impak perkhidmatan bagi fungsi kritikal yang telah dikenalpasti;
iii. Menyediakan dan mendokumentasi Pelan Pemulihan Bencana (Disaster Recovery Plan – DRP) PSUKPs;
iv. Menyedia dan menguji Pelan Simulasi DRP PSUKPs;
v. Menyelaras dan melaksanakan tanggungjawab serta peranan seperti yang telah ditetapkan;
vi. Memperaku cadangan spesifikasi keperluan fizikal DRP bagi setiap fungsi kritikal; dan
vii. Menyedia dan mengemaskini (jika perlu) dan edarkan semula DRP setiap kali terdapat perubahan.

1.2.10 Pengguna

Peranan: Pengguna

Peranan dan tanggungjawab pengguna adalah seperti berikut:

i. Membaca, memahami dan mematuhi Polisi Keselamatan Siber Kerajaan Negeri Perlis;
ii. Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya;
iii. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
iv. Mematuhi prinsipprinsip keselamatan polisi ini dan menjaga kerahsiaan maklumat Kerajaan;
v. Menandatangani Akuan Pematuhan Polisi Keselamatan Siber Kerajaan Negeri Perlis;

vi. Melaksanakan langkahlangkah 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 maklumat;
e) Mematuhi dasar, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;
f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
g) Menjaga kerahsiaan langkahlangkah keselamatan ICT dari diketahui umum.

vii. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada PCERT dengan segera;
viii. Menghadiri programprogram kesedaran mengenai keselamatan siber; dan
ix. Bersetuju dengan terma dan syarat yang terkandung di dalam

1.3 Pengasingan Tugas Dan Tanggungjawab

1.3.1 Pengasingan Tugas

Peranan: Setiausaha Bahagian, Ketua Jabatan Negeri Perlis, Pentadbir Sistem ICT

Tugas dan bidang bertanggungajawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalahguna aset.

Perkaraperkara yang perlu dipatuhi adalah seperti berikut:

i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
ii. Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;
iii. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan
iv. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

1.4 Tanggungjawab Pengurusan

Peranan: CDO dan ICTSO

Pengurusan hendaklah memastikan warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding, dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

Perkaraperkara yang perlu dipatuhi adalah seperti berikut:

i. Memastikan Warga PSUKPs dan pihak ketiga diberi taklimat berkaitan pematuhan PKS;

ii. Memastikan Warga PSUKPs dan pihak ketiga bertanggungjawab ke atas keselamatan ICT berdasarkan kepada peraturan yang telah ditetapkan; dan

iii. Memastikan sumber yang mencukupi untuk melaksanakan proses dan kawalan yang berkaitan keselematan ICT di

1.5 Hubungan Dengan Pihak Berkuasa

Objektif: Menyediakan senarai perhubungan pihak berkuasa berkaitan sekiranya berlaku kejadian yang menjejaskan kese-lamatan maklumat dan perkhidmatan ICT.

Peranan: Bahagian Khidmat Pengurusan (BKP), ICTSO dan Pasukan PCERT.

Hubungan dengan pihak berkuasa berkaitan perlulah diwujudkan dan dikekalkan. Perkaraperkara yang perlu dipatuhi adalah seperti berikut:

i. Mengenalpasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab Pejabat Setiausaha Kerajaan Negeri Perlis;

ii. Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan atau pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia, NACSA dan CyberSecurity Malaysia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan

iii. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.

1.6 Hubungan Dengan Pihak Berkepentingan

Objektif: Memastikan maklumat yang diperlukan oleh pihak berkepentingan dengan PSUKPs disediakan.

Peranan: ICTSO dan Pentadbir Sistem

Pihak berkepentingan terdiri daripada pembekal, perunding, pemegang taruh, pelawat dan pihakpihak lain yang terlibat dalam pengurusan, penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan. Perkara yang perlu dipatuhi:

i. Mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut;
ii. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; dan
iii. Memastikan pihak ketiga menandatangani Surat Akuan Pematuhan PKS seperti di Lampiran A.

1.7 Risikan Ancaman

Objektif: Memastikan semua bentuk ancaman keselamatan ICT difahami, dianalisis dan ditetapkan tindakan yang bersesuaian.

Peranan: Bahagian Pengurusan Teknologi Maklumat (BPTM)

Langkah dan tindakan perlu diambil bagi mengumpul dan menganalisa berbagai jenis ancaman perisikan daripada sumber dalaman dan luaran yang timbul kepada keselamatan ICT PSUKPs.

Perkaraperkara yang perlu dipatuhi adalah seperti yang berikut:

i. Sistem Pemantauan (*Security Monitoring*) bagi mengesan aktiviti yang mencurigakan atau ancaman perisikan yang mungkin terjadi di dalam rangkaian atau sistem.

ii. Memasang pendinding api *(Firewall)* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan.

iii. Setiap data yang disimpan hendaklah di enkripsi (*Encryption*) bagi melindungi data daripada dicapai oleh orang tidak sah.

iv. Memastikan semua perisian yang digunakan adalah versi terkini dan sentiasa kemas kini dari semasa ke semasa.

v. Mengawal akses setiap pengguna aplikasi sistem mengikut skop tugas yang telah ditetapkan oleh BPTM.

1.8 Keselamatan Maklumat Dalam Pengurusan Projek

Objektif: Memastikan keselamatan maklumat diambil kira dalam pengurusan projek.

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis (Pasukan Projek), ICTSO dan Pentadbir Sistem ICT

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan dan keperluan projek sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Perkarap-erkara yang perlu dipatuhi adalah seperti yang berikut:

i. Keselamatan maklumat perlu diterapkan dalam setiap pengurusan projek di pentadbiran Kerajaan Negeri Perlis;
ii. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
iii. Pengurusan risiko ke atas keselamatan maklumat hen-daklah dikendalikan di awal projek untuk mengenal pasti kawalankawalan yang diperlukan;
iv. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber Kerajaan Negeri Perlis; dan
v. Penyediaan spesifikasi perolehan digalakkan untuk memasukkan elemen keselamatan dalam pembangunan projek.
vi. Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk konsep perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan

pelupusan;

vii. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber Pentadbiran Kerajaan Negeri Perlis;

viii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan

ix. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

1.9 Pengurusan Aset

Peranan: Pegawai Aset ICT

Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalan bagi menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT di bawah Pentadbiran Kerajaan Negeri Perlis. Tanggungjawab yang perlu dipatuhi adalah termasuk perkaraperkara berikut:

i. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuatkuasa dari semasa ke semasa;

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

iii. Pegawai Aset hendaklah mengesahkan penempatan aset ICT;

iv. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;

v. Memastikan aset telah dikelaskan dan dilindungi;

vi. Kenal pasti dan mengkaji semula capaian ke atas aset penting

secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;

vii. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan

1.10 Penggunaan Maklumat yang Diterima dan Aset Lain yang berkaitan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkahlangkah keselamatan bagi memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan seperti berikut:

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

1.11 Pemulangan Aset

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Warga Pentadbiran Kerajaan Negeri Perlis hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak dan direkod serta dikemaskini dalam Borang KEW.PA 2.

1.12 Pengelasan Maklumat

Peranan: Pegawai Pengelas bahagian/jabatan

Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan (Semakan dan Pindaan 2017) yang berkuatkuasa.

1.13 Pelabelan Maklumat

Peranan: Pegawai Rekod bahagian/jabatan

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017) yang telah ditetapkan.

1.14 Pemindahan Maklumat

Peranan: ICTSO dan Pentadbir Sistem

Penghantaran atau pemindahan maklumat yang mengandungi maklumat terperingkat boleh dilaksanakan melalui medium elektronik atau media storan fizikal.

Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi

pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;

ii. Terma pemindahan data, maklumat dan perisian antara Pentadbiran Kerajaan Negeri Perlis dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;

iii. Media yang mengandungi maklumat perlu dilindungi; dan

iv. Memastikan maklumat yang terdapat dalam emel hendaklah

1.14.1 Perjanjian Mengenai Pemindahan Data dan Maklumat

Peranan: ICTSO, Pentadbir Sistem dan Warga PSUKPs

Pentadbiran Kerajaan Negeri Perlis perlu mengambil kira keselamatan maklumat apabila berlaku pemindahan data dan maklumat organisasi antara Pentadbiran Kerajaan Negeri Perlis dengan pihak luar. Perkara yang perlu dipertimbangkan ialah:

i. SUB dan Ketua Jabatan hendaklah mengawal penghantaran dan penerimaan maklumat;

ii. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat;

iii. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

iv. Pentadbiran Kerajaan Negeri Perlis hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

1.14.2 Pesanan Elektronik

Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan

undangundang bertulis lain yang berkuat kuasa adalah seperti berikut:

i. Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensiagensi Kerajaan Bilangan 1 Tahun 2003;
ii. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 - Pematuhan Tatacara Penggunaan Emel dan Internet;
iii. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkahlangkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan;
iv. Undangundang bertulis yang berkuatkuasa; dan
v. Akaun atau alamat mel elektronik (emel) yang diperuntukkan oleh Pentadbiran Kerajaan Negeri Perlis sahaja boleh

1.14.3 Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality or Non- Disclosure Agreements*)

Syaratsyarat perjanjian kerahsiaan atau *nondisclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.

1.15 Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini secara berkala atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Keperluan keselamatan aplikasi;
ii. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian;
iii. Undangundang dan peraturan berkaitan yang berkuat kuasa semasa;
iv. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
v. Pengasingan peranan kawalan capaian;
vi. Kebenaran rasmi permintaan akses;
vii. Keperluan semakan hak akses berkala;
viii. Pembatalan hak akses;
ix. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan
x. Capaian *privilege*.

1.15.1 Capaian Rangkaian

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pentadbiran Kerajaan Negeri Perlis. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

i. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian Kerajaan Negeri Perlis, rangkaian agensi lain dan rangkaian awam;
ii. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan
iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

1.16 Pengurusan Identiti

Peranan: ICTSO, Pentadbir Sistem dan Pihak Ketiga

1.16.1 Pengurusan Identiti Pengguna

Proses pengurusan identiti pengguna perlu bagi memastikan ID pengguna yang diwujudkan adalah unik dan menepati tugasan dan keperluan untuk mengakses sesuatu sistem. Perkara yang perlu dipatuhi dalam pengurusan identiti pengguna adalah:

i. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan;
ii. Akaun pengguna mestilah unik;
iii. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada Pentadbiran Kerajaan Negeri Perlis terlebih dahulu;
iv. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
v. Memastikan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Pentadbiran Kerajaan Negeri Perlis.
vi. Penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT; dan
vii. Proses semakan akses pengguna perlu dilaksanakan untuk mengkaji semula kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan.

1.16.2 Pembatalan atau Pelarasan Hak Akses

Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara yang perlu dilakukan adalah seperti berikut:

i. Memastikan akaun pengguna yang diwujudkan memenuhi tugasan yang diperlukan;
ii. Mengesahkan identiti pengguna yang memohon sebelum akaun diwujudkan;
iii. Mewujudkan ID pengguna;

iv. Mengkonfigurasi dan mengaktifkan ID pengguna; dan

v. Menyediakan atau membatalkan hak akses berdasarkan

1.17 Pengesahan Maklumat

Objektif: Memastikan pengesahan entiti yang betul bagi mengelakkan kesalahan dan kegagalan capaian maklumat

1.17.1 Sistem Pengurusan Kata Laluan

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

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

ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan;

iii. Panjang kata laluan mestilah sekurangkurangnya lapan (8) aksara dengan kombinasi alphanumeric dan simbol. (contoh: <>?nokia.#3$) KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad;

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

v. Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

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

vii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

viii. Mengelakkan penggunaan semula kata laluan yang pernah digunakan sebelum ini; dan

ix. Pengguna hendaklah menukar kata laluan sekurangkurangnya tiga (3) bulan sekali.

1.17.2 Kawalan Akses Kepada Kod Sumber Program

Capaian kepada kod sumber hendaklah dihadkan. Perkaraperkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Log audit perlu dikekalkan kepada semua akses kepada kod sumber;
ii. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan
iii. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik Kerajaan Negeri.

1.18 Hak Akses

1.18.1 Pendaftaran dan Pembatalan Hak Akses

Proses bagi pendaftaran atau pembatalan hak akses yang melibatkan elemen fizikal dan logikal dilaksanakan berdasarkan garis panduan berikut:

i. Mendapatkan kelulusan daripada pemilik maklumat serta pihak yang mempunyai kaitan dengan aset yang ingin diakses;
ii. Memastikan pertimbangan terhadap dasar atau peraturan khas berkaitan kawalan akses diambil kira;
iii. Menetapkan pengasingan peranan bagi mengelakkan konflik kepentingan dalam pemberian akses;
iv. Menghentikan akses kepada pengguna yang tidak lagi memerlukan capaian terhadap maklumat tersebut;
v. Menyediakan akses bersifat sementara kepada pegawai kontrak atau staf yang hanya memerlukan capaian dalam tempoh tertentu;

vi. Menilai tahap akses yang diberikan agar ianya bersesuaian dengan keperluan dan tidak melebihi tahap keselamatan maklumat yang ditetapkan;

vii. Mengaktifkan hak akses hanya setelah melalui dan meluluskan prosedur pengesahan yang berkaitan;

viii. Merekodkan semua hak akses secara berpusat untuk tujuan rujukan dan pemantauan;

ix. Mengemas kini atau menukar hak akses bagi pengguna yang telah berubah peranan atau meninggalkan organisasi;

x. Menamatkan atau menyemak semula hak akses yang telah diberikan, sama ada berbentuk fizikal atau logikal; dan

xi. Menyimpan rekod lengkap mengenai sebarang perubahan terhadap hak akses pengguna secara sistematik.

1.18.2 Semakan Hak Akses

Pemeriksaan berkala terhadap hak akses pengguna hendaklah dilaksanakan berdasarkan situasi berikut:

i. Selepas berlakunya perubahan status dalam organisasi seperti pertukaran jawatan, kenaikan atau penurunan pangkat, serta penamatan perkhidmatan;

ii. Pengesahan terhadap hak akses istimewa (*privileged access*) yang telah diberikan;

iii. Selepas sesuatu akses diluluskan, bagi memastikan kesahihan dan keperluannya masih relevan; dan

iv. Melaksanakan semakan hak akses secara berkala, sekurangkurangnya sekali dalam setahun atau mengikut keperluan semasa organisasi.

1.18.3 Pertimbangan Sebelum Pertukaran dan Penamatan Pekerjaan

Sebarang perubahan atau penamatan hak akses pengguna terhadap maklumat dan aset berkaitan perlu melalui proses

semakan, pelarasan, atau dinyahaktifkan terlebih dahulu, dengan mengambil kira penilaian risiko berdasarkan faktorfaktor berikut:

i. Permintaan rasmi daripada pengguna atau pihak pengurusan berkaitan penamatan atau perubahan hak akses;
ii. Skop dan tanggungjawab semasa pengguna dalam organisasi; dan

1.19 Keselamatan Maklumat dengan Pihak Pembekal

Langkahlangkah berikut perlu diambil dalam menguruskan penglibatan pihak luar yang mempunyai kaitan dengan aspek keselamatan maklumat organisasi:

i. Mengenal pasti serta mendokumentasikan pihak luar yang terlibat secara langsung dengan kerahsiaan, integriti dan ketersediaan maklumat organisasi;
ii. Menyediakan mekanisme penilaian dan pemilihan pihak luar yang sesuai berdasarkan tahap klasifikasi maklumat, jenis produk dan perkhidmatan yang ditawarkan;
iii. Membuat penilaian terhadap produk atau perkhidmatan pihak luar yang mempunyai kawalan keselamatan maklumat, serta melaksanakan semakan secara berkala bagi menjamin tahap keselamatan dan integriti maklumat;
iv. Mengenal pasti kategori maklumat PSUKPs, perkhidmatan ICT serta infrastruktur fizikal yang boleh dicapai, diawasi, dikawal atau digunakan oleh pihak luar;
v. Mengenal pasti komponen dan perkhidmatan dalam infrastruktur ICT yang disediakan oleh pihak luar yang berpotensi memberi kesan kepada keselamatan maklumat dari sudut kerahsiaan, integriti dan ketersediaan;
vi. Memastikan semua pihak luar mematuhi keperluan keselamatan maklumat yang telah ditetapkan melalui pemantauan berterusan;

vii. Mengambil langkah untuk mengelakkan ketidakpatuhan oleh pihak luar, sama ada melalui pemantauan langsung atau maklumat daripada sumber lain;

viii. Menangani sebarang insiden berkaitan produk atau perkhidmatan yang berada di bawah bidang kuasa organisasi dan pihak luar;

ix. Menyediakan pelan pemulihan dan pelan kontingensi bagi memastikan maklumat kekal tersedia sekiranya berlaku gangguan;

x. Melaksanakan program latihan dan kesedaran keselamatan maklumat untuk warga PSUKPs yang terlibat dengan pihak luar, khususnya yang mempunyai akses kepada maklumat;

xi. Memastikan maklumat dan aset berkaitan dilindungi sepenuhnya sepanjang proses pemindahan antara organisasi dan pihak luar;

xii. Pematuhan terhadap keperluan keselamatan fizikal dan keselamatan kakitangan oleh pihak luar, termasuk mematuhi dokumendokumen seperti PKS dan Akta Rahsia Rasmi 1972; dan

xiii. Melaksanakan proses tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO).

1.20 Keselamatan Maklumat Dalam Perjanjian Pihak Luaran

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada Pentadbiran Kerajaan Negeri Perlis selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Pentadbiran Kerajaan Negeri Perlis hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;
ii. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan;
iii. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;
iv. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;
v. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan Pentadbiran Kerajaan Negeri Perlis; dan
vi. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Pentadbiran Kerajaan Negeri Perlis.

1.21 Pengurusan Keselamatan Maklumat Dalam Rantaian Komunikasi

Peranan: SUB, Ketua Jabatan, Pemilik Projek dan Pembekal

Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta

rantaian bekalan produk. Perkaraperkara yang perlu diambil kira adalah seperti yang berikut:

i. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;
ii. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekalpembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan
iii. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.

1.22 Pemantauan, Semakan dan Perubahan Pengurusan Perkhidmatan Pembekal

Peranan: SUB, Ketua Jabatan, Pemilik Projek dan Pembekal Pentadbiran Kerajaan Negeri Perlis hendaklah sentiasa memantau dan mengaudit perkhidmatan pembekal secara berkala. Perkaraperkara yang perlu diambil kira adalah seperti yang berikut:

i. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;
ii. Menyemak laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan
iii. Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan menyemak maklumat tersebut seperti yang dikehendaki dalam perjanjian.

1.23 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Awan

Peranan: ICTSO, SUB, Ketua Jabatan dan Pemilik Projek/Sistem Aplikasi

Perkhidmatan pengkomputeran awan dilihat mampu menawarkan penjimatan kos disamping meningkatkan kecekapan perkhidmatan ICT. Walau bagaimanapun Pentadbiran Kerajaan Negeri Perlis hendaklah memastikan penyedia perkhidmatan pengkomputeran awan yang dipilih mempunyai tahap keselamatan yang tinggi. Antara langkahlangkah yang perlu dipatuhi adalah seperti berikut:

i. Penilaian hendaklah dibuat secara terperinci berdasarkan kepada keperluan, pematuhan kepada dasar sedia ada dan kekangan undangundang yang berkaitan sebelum sebarang keputusan untuk menggunakan perkhidmatan pengkomputeran awan dibuat;
ii. Memastikan isi kandungan kontrak perjanjian seperti *Customer Agreement*, *Service Level Agreement* (SLA) atau *Acceptable Use Policy* (AUP) difahami sebelum mendaftar untuk menggunakan sebarang perkhidmatan;
iii. Mempertimbangkan *Cloud Service Provider* (CSP) lain sekiranya sebarang terma di dalam kontrak tidak difahami dan meragukan;
iv. Data atau maklumat adalah hak milik eksklusif PSUKPs sepenuhnya dan tidak boleh dianggap sebagai aset kepada CSP;
v. PSUKPs hendaklah diberikan hak untuk melaksanakan audit ke atas CSP untuk tujuan semakan seperti yang dinyatakan di dalam *Terms of Service* CSP; dan
vi. Klausa berhubung dengan pelucutan pentauliahan *(decommisioning)* atau penamatan kontrak hendaklah dinyatakan dengan jelas di dalam kontrak perjanjian dengan CSP.

1.24 Perancangan, Penyediaan dan Pengurusan Insiden Keselamatan Maklumat

Peranan: ICTSO, SUB, Ketua Jabatan dan Pemilik Projek/Sistem Aplikasi

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden Pentadbiran Kerajaan Negeri Perlis adalah berpandukan Prosedur Operasi Standard (SOP) Pengendalian Insiden. Perkaraperkara yang perlu dipatuhi adalah seperti berikut:

i. Mewujudkan Prosedur Operasi Standard (SOP) Pengendalian Insiden;
ii. Memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat;
iii. Memaklumkan kepada agensi kerajaan pusat yang bertanggungjawab dalam menangani insiden keselamatan; dan
iv. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan dengan menyediakan latihan dan kursus yang bersesuaian.

1.25 Penilaian dan Tindakan Insiden Keselamatan Maklumat

Peranan: ICTSO

Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. Perkara yang perlu diambil kira adalah seperti yang berikut:

i. Mengenal pasti dan mengesahkan kategori serta keutamaan insiden maklumat; dan
ii. Merekodkan dan menyimpan semua tindakan serta keputusan insiden keselamatan maklumat untuk tujuan rujukan masa hadapan.

1.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Peranan: ICTSO, PCERT

Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengendalian Insiden Kerajaan Negeri Perlis.

Kawalankawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:

i. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;

ii. Menjalankan kajian dan analisis;

ii. Menghubungi pihak berkuasa atau agensi yang berkenaan dengan secepat mungkin;

iii. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;

iv. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

v. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan sekiranya perlu;

vi. Menyediakan tindakan pemulihan (*restoration*) dengan kadar segera;

vii. Menangani insiden keselamatan maklumat berdasarkan peraturan yang berkuat kuasa;

viii. Menutup insiden secara rasmi dan rekodkan setelah insiden berjaya ditangani; dan

ix. Melaksanakan pasca insiden untuk mengenal pasti punca

1.27 Pembelajaran daripada Insiden Keselamatan Maklumat

Peranan: ICTSO dan PCERT

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 Pentadbiran Kerajaan Negeri Perlis.

1.28 Pengumpulan Bukti

Peranan: ICTSO dan PCERT

Pihak pengurusan perlu memastikan penyimpanan bukti direkodkan secara konsisten bagi insiden keselamatan maklumat untuk tindakan tatatertib dan undangundang. Perkara yang perlu dipatuhi adalah seperti berikut:

i. Mengenal pasti, mengumpul, menyimpan dan melindungi bahan bukti untuk mengelakkan pengubahsuaian tanpa kebenaran;
ii. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti bahan bukti; dan
iii. Sistem maklumat perlu merekodkan semua bukti insiden selaras dengan tarikh dan masa kejadian.

1.29 Keselamatan Maklumat Semasa Gangguan

1.29.1 Perancangan Kesinambungan Keselamatan Maklumat

Peranan: Pasukan Pemulihan Bencana ICT

Pentadbiran Kerajaan Negeri Perlis hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan,

contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, Pentadbiran Kerajaan Negeri Perlis perlu mengambil kira isuisu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Pentadbiran Kerajaan Negeri Perlis.

Pentadbiran Kerajaan Negeri Perlis juga perlu mengambil kira keperluan dan ekspektasi pihakpihak berkepentingan serta keperluan undangundang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) Pentadbiran Kerajaan Negeri Perlis;

ii. Menetapkan polisi PKP;

iii. Mengenalpasti perkhidmatan kritikal;

iv. Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Pemulihan Bencana ICT, Pelan Tindak Balas Kecemasan dan Pelan Komunikasi Krisis;

v. Melaksanakan program kesedaran dan latihan pasukan PKP dan warga Pentadbiran Kerajaan Negeri Perlis;

vi. Melaksanakan simulasi ke atas dokumen Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Pemulihan Bencana ICT, Pelan Tindak Balas Kecemasan dan Pelan Komunikasi Krisis; dan

vii. Melaksanakan penyelenggaraan ke atas dokumen Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Pemulihan Bencana ICT, Pelan Tindak Balas Kecemasan dan Pelan

1.29.2 Pelaksanaan Kesinambungan Keselamatan Maklumat

Pentadbiran Kerajaan Negeri Perlis hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses,

prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang boleh menjejaskan operasi. Antara perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal Pentadbiran Kerajaan Negeri Perlis yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini; dan
ii. Melaksanakan postmortem dan mengemaskini pelanpelan PKP.

1.29.3 Menentusah, Mengkaji Semula dan Menilai Pelan Kesinambungan Maklumat

Peranan: Pengurusan Atasan Pentadbiran Kerajaan Negeri Perlis, Koordinator PKP, Pasukan Tindak balas Kecemasan dan Pemulihan Bencana ICT serta Warga Pentadbiran Kerajaan Negeri Perlis

Pentadbiran Kerajaan Negeri Perlis hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

1.30 Ketersediaan ICT bagi Kesinambungan Perkhidmatan

Peranan: Pasukan Tindak balas Kecemasan dan Pemulihan Bencana ICT

Ketersediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT. Ketersediaan ICT untuk kesinambungan perkhidmatan adalah komponen penting dalam

pengurusan kesinambungan perkhidmatan dan pengurusan keselamatan maklumat untuk memastikan objektif organisasi dapat terus dipenuhi semasa gangguan. Pasukan Tindak balas Kecemasan dan Pemulihan Bencana ICT hendaklah memastikan bahawa:

i. Struktur organisasi yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan yang disokong oleh kakitangan yang mempunyai tanggungjawab, kuasa dan kecekapan yang diperlukan;

ii. Pelan kesinambungan ICT, termasuk tindak balas dan prosedur pemulihan yang memperincikan bagaimana organisasi merancang untuk menguruskan gangguan perkhidmatan ICT, adalah:

    a. Kerap dinilai melalui latihan dan ujian;

1.31 Keperluan UndangUndang, Berkanun, Peraturan Dan Kontrak

1.31.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, Pembekal dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

Setiap pengguna di bawah Kerajaan Negeri Perlis hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber Kerajaan Negeri Perlis dan undangundang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di Kerajaan Negeri Perlis termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

1.31.2 Kawalan Kriptografi

Peranan: Pentadbir Sistem/Aplikasi

Kunci enkripsi hendaklah dilindungi menggunakan kawalan keselamatan yang paling berkesan serta dirahsiakan. Sepanjang keseluruhan kitar hayatnya, kunci tersebut perlu dilindungi daripada sebarang pengubahsuaian, kemusnahan, dan penyebaran tanpa kebenaran.

Kriptografi juga merangkumi kaedahkaedah berikut:

i. Semua pelaksanaan sistem perlu menggunakan ID atau kata laluan yang dienkripsi; dan
ii. Penggunaan Perkhidmatan Prasarana Kunci Awam Kerajaan (MyGPKI) yang selamat serta dibekalkan oleh pihak Kerajaan.

1.32 Hak Harta Intelek

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, Pembekal dan Pihak Luaran

Warga Pentadbiran Kerajaan Negeri Perlis perlu memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak intelektual. Perkara yang perlu dipatuhi adalah:

i. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah;
ii. Mematuhi had pengguna yang telah ditetapkan atau dibenarkan; dan
iii. Pematuhan yang berterusan dengan sekatan hak cipta produk dan keperluan perlesenan.

1.33 Perlindungan Rekod

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, Pembekal dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

Rekod (fizikal atau digital) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.

1.34 Privasi dan Perlindungan Maklumat Peribadi

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, Pembekal dan Pihak yang mempunyai urusan dengan ICT Kerajaan Negeri Perlis

Pentadbiran Kerajaan Negeri Perlis hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undangundang dan peraturanperaturan Kerajaan Malaysia.

1.35 Kajian Bebas Keselamatan Maklumat

Peranan: Jawatankuasa Pelaksana ISMS dan Audit Luaran (SIRIM)

Kajian bebas secara berkala perlu dilaksanakan bagi menilai keberkesanan dan kecekapan Sistem Pengurusan Keselamatan Maklumat. Ini bagi memastikan tahap keselamatan maklumat berfungsi dengan baik dan memenuhi keperluan undangundang dan peraturan yang berkaitan dengan keselamatan. Kajian tersebut hendaklah melibatkan beberapa langkah termasuk :

i. Penilaian Risiko
ii. Penilaian Kecekapan
iii. Penilaian Pematuhan
iv. Penyediaan laporan

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

1.36 Pematuhan kepada Polisi, Peraturan dan Piawaian

Peranan: Jawatankuasa Pelaksana ISMS

Pentadbiran Kerajaan Negeri Perlis hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.

1.37 Dokumentasi Prosedur Operasi

Peranan: Jawatankuasa Pelaksana ISMS

Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkaraperkara berikut:

i. Semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;
ii. Setiap prosedur mestilah mengandungi arahanarahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
iii. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.

2 KAWALAN SUMBER MANUSIA

Objektif: Memastikan semua kakitangan dan orang awam memahami peranan serta tanggungjawab mereka berkaitan aspek keselamatan ICT sepanjang tempoh perkhidmatan.

2.1 Tapisan Keselamatan

Tapisan keselamatan hendaklah dijalankan terhadap warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT yang terlibat selaras dengan keperluan perkhidmatan. Perkaraperkara yang perlu dipatuhi adalah seperti yang berikut:

i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga Pentadbiran Kerajaan Negeri Perlis, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan

ii. Menjalankan tapisan keselamatan untuk warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

2.2 Terma dan syarat Perkhidmatan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT perlu melaksanakan perkara seperti berikut:

i. Membaca, memahami dan memperakui Surat Akuan Pematuhan Polisi Keselamatan Siber (PKS) Kerajaan Negeri Perlis seperti di Lampiran A;

ii. Memahami dan bersetuju ke atas tanggungjawab serta hak berkaitan perlindungan keselamatan maklumat;

iii. Mematuhi semua terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan;

iv. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT yang terlibat dalam menjamin keselamatan aset ICT; dan

2.3 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Peranan: ICTSO

Warga Pentadbiran Kerajaan Negeri Perlis dan Pihak Luaran perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugastugas dan tanggungjawab mereka. Perkaraperkara yang perlu dipatuhi adalah seperti yang berikut:

i. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber Pentadbiran Kerajaan Negeri Perlis, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan disampaikan secara berterusan dalam melaksanakan tugastugas dan tanggungjawab mereka;

ii. Mendapatkan sokongan pengurusan atasan berkaitan keselamatan maklumat; dan

iii. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

2.4 Proses Tatatertib

Peranan: Setiausaha Bahagian (Sumber Manusia), Ketua Unit Integriti, Warga PSUKPs dan Pihak Luaran

Proses tatatertib yang formal dan disampaikan kepada warga Pentadbiran Kerajaan Negeri Perlis dan Pihak Luaran hendaklah tersedia bagi membolehkan tindakan diambil terhadap mereka yang melakukan pelanggaran keselamatan maklumat. Perkaraperkara yang perlu dipatuhi adalah seperti yang berikut:

i. Memastikan adanya proses tindakan disiplin atau undan-gundang ke atas Pihak Luaran sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang telah ditetapkan oleh Pentadbiran Kerajaan Negeri Perlis; dan
ii. Warga Pentadbiran Kerajaan Negeri Perlis yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT.

2.5 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, Pegawai Aset ICT dan Pentadbir Sistem ICT

Warga pentadbiran Kerajaan Negeri Perlis yang telah bertukar/tamat perkhidmatan perlu mematuhi perkaraperkara berikut berdasarkan kepada pekeliling dan peraturan yang sedang berkuat kuasa:

i. Memastikan semua aset ICT dikembalikan kepada Pegawai Aset ICT mengikut peraturan dan terma perkhidmatan yang ditetapkan; dan
ii. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan Pentadbiran Kerajaan Negeri Perlis dan/atau terma perkhidmatan.

2.6 Perjanjian Kerahsiaan atau *NonDisclosure Agreement*

Peranan: ICTSO dan Pihak Luaran

Syaratsyarat perjanjian kerahsiaan atau *nondisclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.

2.7 Telekerja

Telekerja meliputi semua bentuk pelaksanaan tugasan yang dilaksanakan di luar tempat kerja. Dasar dan langkahlangkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.

Perkara yang perlu dipatuhi bagi memastikan keselamatan kerja jarak jauh terjamin adalah seperti berikut:

i. Mengenal pasti lokasi persekitaran fizikal untuk bekerja jarak jauh seperti di rumah atau lokasi yang dibenarkan sahaja;

ii. Penggunaan kawalan peralatan atau perisian keselamatan;

iii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;

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

v. Menetapkan klafisikasi maklumat dan sistem yang boleh diakses oleh individu bekerja jarak jauh; dan

vi. Membatalkan hak akses dan pemulangan peralatan apabila

2.8 Pelaporan Kejadian Keselamatan Maklumat

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada ICTSO dan PCERT dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Maklumat didapati hilang, didedahkan kepada pihakpihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihakpihak yang tidak diberi kuasa;
ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
iii. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan;
iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan siber berdasarkan:

i. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
ii. Prosedur Operasi Standard: Pengendalian Insiden Kerajaan Negeri Perlis.

3 KAWALAN FIZIKAL

3.1 Perimeter Keselamatan Fizikal

Objektif: Memastikan kawalan keselamatan fizikal dilaksanakan bagi melindungi maklumat, premis dan kemudahan ICT.

Peranan: ICTSO, Bahagian Khidmat Pengurusan dan Warga Pentadbiran Kerajaan Negeri Perlis

Keselamatan fizikal adalah bertujuan untuk menghalang mengesan dan mencegah cubaan untuk menceroboh terhadap premis dan Aset ICT Kerajaan Negeri Perlis. Langkahlangkah keselamatan yang perlu dipatuhi termasuk yang berikut:

i. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
ii. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
iii. Mereka bentuk dan melaksanakan perlindungan fizikal di dalam pejabat, bilik dan kemudahan daripada kebakaran, banjir, letupan dan sebarang bencana alam atau perbuatan manusia;
iv. Menyediakan kaunter kawalan;
v. Memasang dan menguji alat penggera kebakaran;
vi. Memasang alat penggera atau kamera keselamatan (CCTV);
vii. Mewujudkan perkhidmatan kawalan keselamatan; dan
viii. Kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan

3.2 Kawalan Kemasukan Fizikal

Peranan: ICTSO, Warga Pentadbiran Kerajaan Negeri Perlis dan Pihak Luaran

Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis pentadbiran Kerajaan Negeri Perlis. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Setiap warga pentadbiran Kerajaan Negeri Perlis hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas;
ii. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di pos pengawal keselamatan dan hendaklah dikembalikan selepas tamat lawatan;
iii. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT Kerajaan Negeri Perlis; dan

3.3 Keselamatan Pejabat, Bilik Dan Kemudahan

Peranan: Bahagian Khidmat Pengurusan dan Warga Pentadbiran Kerajaan Negeri Perlis,

Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Kawasan tempat bekerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;
ii. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan
iii. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan

3.4 Pemantauan Keselamatan Fizikal

Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera penceroboh, sistem pemantauan video seperti kamera litar tertutup (CCTV) dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan. Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada diakses oleh orang yang tidak dibenarkan atau sistem dilumpuhkan dari jauh.

3.5 Perlindungan daripada Ancaman Fizikal dan Persekitaran

Peranan: ICTSO dan Setiausaha Bahagian (Khidmat Pengurusan)

Memberi perlindungan fizikal terhadap sebarang bentuk ancaman persekitaran yang disebabkan oleh kebakaran, banjir, letupan, bencana alam, serangan berniat jahat dan sebagainya.

3.6 Bekerja Di Kawasan Selamat

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga Pentadbiran Kerajaan Negeri yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis Kerajaan Negeri termasuklah Pusat Data.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:

i. Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di Pusat Data yang mempunyai ciriciri keselamatan yang tinggi termasuk sistem pencegahan

kebakaran;

ii. Akses adalah terhad kepada warga Pentadbiran Kerajaan Negeri yang diberi kuasa sahaja dan dipantau setiap masa;

iii. Melakukan pemantauan melalui CCTV kamera atau lainlain peralatan yang sesuai;

iv. Merekodkan butiran keluar masuk pelawat ke kawasan larangan;

v. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam.

3.7 *Clear Desk And Clear Screen*

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Clear Desk and Clear Screen bermaksud tidak meninggalkan dan mendedahkan bahanbahan yang sensitif sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkahlangkah yang perlu diambil termasuklah seperti yang berikut:

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

ii. Menyimpan bahanbahan sensitif di dalam laci atau kabinet fail yang berkunci;

iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat;

iv. Emel masuk dan keluar hendaklah dikawal; dan

v. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas

3.8 Penempatan dan Perlindungan Aset ICT

Peranan: ICTSO, Warga Pentadbiran Kerajaan Negeri Perlis dan Pihak Luaran

Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkahlangkah keselamatan yang perlu diambil adalah seperti yang berikut:

i. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
ii. Pengguna bertanggungjawab sepenuhnya ke atas komputer masingmasing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
iii. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;
iv. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;
v. 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;
vi. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;
vii. Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;
viii. Peralatanperalatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Genset);
ix. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciriciri keselamatan;
x. Peralatan rangkaian seperti suis, penghala, hab dan peralatanperalatan lain perlu diletakkan di dalam rak khas dan berkunci;

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

xii. Peralatan ICT yang hendak dibawa ke luar premis Kerajaan Negeri, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

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

xiv. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

xv. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

xvi. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;

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

xviii. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;

xix. Pengguna dilarang sama sekali mengubah kata laluan *administrator* yang telah ditetapkan oleh pihak ICT; dan

xx. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan

3.9 Keselamatan Aset di Luar Premis

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis. Peralatan yang dibawa keluar dari premis adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Aset ICT yang dibawa keluar perlu dilindungi dan dikawal sepanjang masa;
ii. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciriciri keselamatan yang bersesuaian; dan
iii. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

3.10 Media Storan

3.10.1 Media Storan Digital

Peranan: ICTSO, Pentadbir Sistem dan Warga Pentadbiran Kerajaan Negeri Perlis

Media storan berfungsi untuk menyimpan data dan maklumat, contohnya seperti pemacu kilat (thumb drive), cakera keras luaran (external drive) dan pelbagai jenis media storan yang lain. Prosedur pengurusan media storan hendaklah dilaksanakan mengikut pengkelasan yang diguna pakai oleh Pentadbiran Kerajaan Negeri Perlis. Prosedurprosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
ii. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
iii. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
iv. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan

3.10.2 Pemindahan dan Pelupusan Media

Peranan: ICTSO, Pentadbir Sistem dan Warga Pentadbiran Kerajaan Negeri Perlis

Prosedur bagi pelupusan dan penggunaan semula media storan perlu diwujudkan bagi mengurangkan risiko kebocoran maklumat. Antara perkara yang perlu dipatuhi adalah seperti berikut:

i. Pemindahan dan pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan;
ii. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa;
iii. Pelupusan media storan oleh Pihak Luaran hendaklah mematuhi kawalan keselamatan dan dilaksanakan oleh pihak yang berpengalaman;
iv. Pelupusan maklumat mengikut Tatacara Pelupusan Arkib Negara (Akta Arkib Negara 2003 [Akta 629]);

3.10.3 Pengalihan Aset

Peranan: Pengguna dan Pegawai Aset

Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

i. Peralatan ICT yang hendak dibawa keluar dari premis pentadbiran Kerajaan Negeri Perlis untuk tujuan rasmi, perlulah mendapat kelulusan pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan

ii. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

3.11 Utiliti Sokongan

Objektif: Memastikan kawalan terhadap perkhidmatan sokongan ICT sentiasa dilindungi daripada gangguan fasiliti dan kegagalan bekalan kuasa.

Peranan: ICTSO dan Pentadbir Sistem

Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurangkurangnya setahun sekali). Perkara yang perlu dipatuhi adalah seperti berikut:

i. Memastikan semua peralatan dalam fasiliti perkhidmatan sokongan beroperasi, dikonfigurasi, dan diselenggara mengikut spesifikasi pengeluar yang ditetapkan;
ii. Memastikan fasiliti perkhidmatan sokongan dinilai semula keupayaannya secara berkala bagi memenuhi keperluan PSUKPs;
iii. Memastikan peralatan sokongan disemak dan diselenggara secara berkala mengikut ketetapan dalam Perjanjian Tahap Perkhidmatan (SLA);
iv. Menyediakan fasiliti sokongan kedua sebagai langkah persediaan bagi mengelakkan gangguan perkhidmatan;
v. Memastikan peralatan dalam fasiliti perkhidmatan sokongan disokong sepenuhnya oleh sistem Bekalan Kuasa Tanpa Gangguan (UPS);
vi. Menjamin bekalan kuasa berterusan kepada fasiliti sokongan seperti UPS dan penjana kuasa (generator) bagi memastikan operasi pusat data berjalan dengan lancar dan perkhidmatan fasiliti sokongan tidak terjejas; dan

vii. Memastikan peralatan sokongan diperiksa dan diuji secara berkala oleh pihak yang berkenaan bagi menjamin kebolehoperasian dan keselamatan.

3.12 Keselamatan Kabel

Objektif: Memastikan kabel rangkaian dan kabel kuasa elektrik sentiasa dilindungi daripada sebarang bentuk gangguan serta pencerobohan.

Peranan: ICTSO, Pentadbir Sistem dan Pihak Luaran

Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkahlangkah keselamatan yang perlu diambil adalah seperti yang berikut:

i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
ii. Mengasingkan kabel kuasa elektrik dan rangkaian untuk mencegah gangguan penghantaran data;
iii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
iv. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan
v. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.

3.13 Penyelenggaraan Peralatan

Peranan: Pegawai Aset dan Pentadbir Sistem ICT

Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan,

kerahsiaan dan integriti. Langkahlangkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

i. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;
ii. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;
iii. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
iv. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan
v. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.
vi. Menyimpan rekod penyelenggaraan pencegahan dan pemulihan;
vii. Melaksanakan kawalan yang sesuai bagi tujuan penyelenggaraan pencegahan dan pemulihan sama ada di dalam atau luar premis;
viii. Menyelia kerjakerja penyelenggaraan yang dilakukan oleh Pihak Luaran;
ix. Mengawal akses bagi penyelenggaraan yang dilaksanakan secara jarak jauh (remote); dan
x. Menyemak dan menguji semua peralatan selepas proses penyelenggaraan bagi memastikan tiada pengubahsuaian yang tidak dibenarkan.

3.14 Pelupusan yang Selamat atau Penggunaan Semula Peralatan

Peranan: ICTSO dan Warga Pentadbiran Kerajaan Negeri Perlis

Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan

atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan atau ditempatkan di bawah Pentadbiran Kerajaan Negeri Perlis.

Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan Pentadbiran Kerajaan Negeri Perlis. Langkahlangkah seperti yang berikut hendaklah diambil:

i. Bagi peralatan ICT yang akan dilupuskan sebelum proses pemindahan milik, data yang disimpan di dalam peranti storan hendaklah dipastikan telah dihapuskan dengan kaedah yang selamat;
ii. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
iii. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciriciri keselamatan bagi menjamin keselamatan peralatan tersebut;
iv. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;
v. Pengguna ICT adalah dilarang sama sekali daripada melakukan perkaraperkara seperti yang berikut:

    a) Menyimpan manamana peralatan ICT yang hendak dilupuskan untuk milik peribadi.
    b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *Hardisk, Motherboard* dan sebagainya.
    c) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan manamana peralatan yang berkaitan ke manamana bahagian di bawah Pentadbiran Kerajaan Negeri Perlis.

d) Memindah keluar dari pejabat bagi manamana peralatan ICT yang hendak dilupuskan.

e) Melupuskan sendiri peralatan ICT kerana kerjakerja pelupusan di bawah tanggungjawab Pentadbiran Kerajaan Negeri Perlis.

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

vii. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;

viii. Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan yang berkuatkuasa;

ix. Pelupusan dokumendokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan

x. Pegawai aset bertanggungjawab merekod butirbutir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam

4 KAWALAN TEKNOLOGI

4.1 Peranti Akhir Pengguna

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Maklumat yang disimpan, diproses atau boleh diakses melalui peranti pengguna hendaklah dilindungi. Langkah ini adalah bagi melindungi maklumat daripada terdedah kepada risiko yang dibawa oleh penggunaan peranti oleh pengguna. Organisasi hendaklah menetapkan prosedur khusus berkenaan konfigurasi dan pengendalian yang selamat bagi peranti pengguna. Prosedur ini hendaklah mengambil kira perkaraperkara berikut:

i. Pentadbir Sistem hanya menyediakan sokongan terhad (*reasonable endeavors*) kepada pengguna bagi tujuan konfigurasi, tetapan dan penggunaan bagi capaian ke sistem aplikasi yang dibenarkan untuk urusan rasmi sahaja;
ii. Memasang dan menggunakan kata laluan bagi mengelakkan akses yang tidak dibenarkan;
iii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;
iv. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT yang digunakan;
v. Peralatan yang digunakan hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan;
vi. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan;

4.1.1 Polisi Peranti Mudah Alih

Peranan: BPTM, JPICT, Warga Pentadbiran Kerajaan Negeri Perlis

Membangun serta menyebarkan dasar dan langkahlangkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.

Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga pentadbiran Kerajaan Negeri Perlis.

Perkaraperkara yang perlu dipatuhi:

i. Pendaftaran ke atas peralatan mudah alih;
ii. Keperluan ke atas perlindungan secara fizikal;
iii. Kawalan ke atas pemasangan perisian peralatan mudah alih;
iv. Kawalan ke atas versi dan *patches* perisian;
v. Sekatan ke atas akses perkhidmatan maklumat secara dalam talian;
vi. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan
vii. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.

4.1.2 *Bring Your Own Device* (BYOD)

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, tablet dan komputer riba yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian Jabatan. Pengguna yang menggunakan kemudahan WiFi jabatan atau data persendirian untuk akses kepada Internet tertakluk kepada PKS Kerajaan Negeri Perlis.

i. Pengguna bertanggungjawab memastikan langkahlangkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut:

a. Mengasingkan penggunaan bagi tujuan peribadi dan tugasan rasmi. Instalasi perisian yang dibekalkan oleh Jabatan pada aset ICT persendirian hendaklah mendapatkan kelulusan Pengurus ICT;
b. Membenarkan akses kepada maklumat yang berkaitan dengan tugasan rasmi dan menghapuskan data rahsia rasmi pada aset ICT memastikan hak harta intelek adalah di bawah tanggungjawab pengguna aset ICT persendirian;
c. Penyalahgunaan aset ICT persendirian adalah di bawah tanggungjawab pengguna sendiri;
d. Jabatan menghormati privasi aset ICT persendirian dengan mengambil langkah pencegahan yang terbaik untuk memastikan keselamatan maklumat. Jabatan mempunyai hak untuk menjejaki dan meminta akses kepada aset ICT persendirian sekiranya terdapat pelanggaran keselamatan maklumat yang dikenal pasti

4.1.3 Sambungan Rangkaian Tanpa Wayar

Peranan: Pentadbir Sistem/Aplikasi dan Warga Pentadbiran Kerajaan Negeri Perlis

Perkara yang perlu dipatuhi bagi memastikan keselamatan penggunaan rangkaian tanpa wayar adalah seperti berikut:

i. Menetapkan konfigurasi rangkaian tanpa wayar bagi aset ICT bagi memastikan perlindungan daripada protokol yang terdedah kepada kelemahan;
ii. Menetapkan *bandwidth* rangkaian yang bersesuaian bergantung kepada jenis akses; dan
iii. tidak mendedahkan identiti dan kata laluan sambungan rangkaian tanpa wayar.

4.2 Hak Akses Istimewa

Peranan: Pentadbir Sistem ICT

Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. Prosedur penetapan dan penggunaan ke atas hak akses hendaklah mengambil kira perkara berikut:

i. Mengenal pasti pengguna yang memerlukan hak akses untuk sistem aplikasi, sistem pengoperasian dan pengurusan pangkalan data;
ii. Keperluan capaian hendaklah sentiasa dipantau dan dikemaskini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja;
iii. Memastikan perbezaan peranan akses untuk pentadbir dan pengguna;
iv. Melarang penggunaan ID pentadbir seperti *root* bagi akses ke konfigurasi sistem;
v. Memberikan hak akses sementara untuk perubahan atau penyelenggaraan yang dilaksanakan oleh Pihak Luaran;
vi. Merekodkan semua log masuk untuk kegunaan jejak audit;
vii. Tidak berkongsi ID pengguna dengan orang lain;
viii. Menggunakan ID pengguna berdasarkan skop tugas (melaksanakan tugasan harian) dan tidak menggunakan ID pentadbir; dan
ix. Sebarang perubahan mestilah mendapat kebenaran secara bertulis

4.3 Sekatan Capaian Maklumat

Peranan: ICTSO dan Pentadbir Sistem/Aplikasi

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan capaian. Perkara berikut hendaklah dipatuhi:

i. Tidak membenarkan akses kepada maklumat terperingkat bagi pengguna yang tidak diberi kebenaran;

ii. Mengawal data yang boleh diakses mengikut kategori pengguna;
iii. Mengawal individu dan kumpulan yang telah dikenal pasti mempunyai akses seperti membaca (read), menulis (write), memadam (delete) dan melaksanakan (execute);
iv. Menyediakan kawalan fizikal atau kawalan hak akses untuk aplikasi, data atau sistem;
v. Aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan sebarang aktiviti yang tidak diingini;
vi. Mengehadkan percubaan kemasukan kata laluan bagi capaian ke aplikasi kepada maksimum tiga (3) kali sahaja. Setelah mencapai had maksimum, capaian akan disekat sehingga ID capaian diaktifkan semula; dan
vii. Akses maklumat melalui capaian jarak jauh tidak digalakkan dan hanya

4.4 Akses kepada Kod Sumber

4.4.1 Kawalan Capaian Kepada Kod Sumber (*Source Code*)

Peranan: Pengurus Projek dan Pentadbir Sistem ICT

Kawalan capaian kepada kod sumber atau aturcara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan Negeri Perlis. Perkara berikut hendaklah dipatuhi:

i. Mengawal selia akses terhadap kod sumber dan program;
ii. Memberikan akses baca dan tulis berdasarkan kelulusan serta mengurus risiko penyalahgunaan kod sumber;
iii. Sebarang kemas kini dan pemberian akses kepada kod sumber hendaklah mematuhi prosedur kawalan perubahan yang telah diluluskan;
iv. Pengatur cara sistem tidak dibenarkan mengakses repositori kod sumber secara langsung, sebaliknya melalui perisian pembangunan yang mengawal aktiviti serta kebenaran terhadap kod sumber;
v. Menyimpan senarai kod sumber di lokasi yang selamat serta memberikan kawalan akses hanya kepada individu yang dibenarkan; dan

vi. Merekod log audit bagi setiap akses dan perubahan yang dilakukan terhadap kod sumber.

4.5 Pengesahan Selamat (*Secure Authentication*)

4.5.1 Prosedur Log Masuk yang Selamat

Peranan: ICTSO dan Pentadbir Sistem ICT

Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut:

i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Kerajaan Negeri Perlis;
ii. Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;
iii. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;
iv. Mewujudkan satu teknik pengesahan bagi pengenalan diri pengguna;
v. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan

4.6 Pengurusan Kapasiti

Peranan: ICTSO dan Pentadbir Sistem/Aplikasi

Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkaraperkara yang perlu dipatuhi adalah seperti yang berikut:

i. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan

ii. Keperluan kapasiti ini juga perlu mengambil kira ciriciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

4.7 Perlindungan daripada Perisian Hasad *(Malware)*

Peranan: Pentadbir Sistem ICT dan Pengguna

Perisian atau sistem yang digunakan mesti bebas daripada kod berbahaya *(malicious code).* Perkaraperkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:

i. 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;

ii. Memasang dan menggunakan hanya perisian yang berdaftar dan tulen di bawah manamana undangundang bertulis yang berkuat kuasa;

iii. Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya;

iv. Mengemaskini *antivirus* dengan *signature/pattern antivirus* yang terkini;

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

vi. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

vii. Memasukkan klausa tanggungan di dalam manamana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program

berbahaya; dan

viii. Mengadakan program dan prosedur jaminan kualiti ke atas semua

4.8 Pengurusan Kerentanan Teknikal *(Technical Vulnerability Management)*

4.8.1 Mengenal Pasti Kerentanan Teknikal

Peranan : ICTSO dan Pentadbir Sistem/Aplikasi

Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkahlangkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut :

i. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;

ii. Menganalisis tahap risiko kerentanan; dan

4.8.2 Kajian Semula Pematuhan Teknikal *(Technical Compliance Review)*

Peranan : Bahagian Pengurusan Teknologi Maklumat (BPTM)

BPTM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.

4.9 Pengurusan Konfigurasi

Semua peralatan *server*, perkakasan, keselamatan, perisian dan rangkaian perlu mempunyai tatacara pengkonfigurasian.

Aktiviti ini hendaklah diurus dan dipantau bagi menjamin peralatan *server*, perkakasan, keselamatan, perisian dan rangkaian beroperasi selaras dengan dasar dan prosedur yang ditetapkan.

4.10 Penghapusan Maklumat

Data yang disimpan di dalam pelayan, cakera keras, rangkaian, USB atau media storan yang lain hendaklah dihapuskan setelah ia tidak diperlukan lagi. Ini termasuklah data yang disimpan oleh kakitangan, pengguna dan pelanggan. Ia selaras dengan pematuhan Akta 629 Akta Arkib Negara 2003.

4.11 Penyamaran Data (*Data Masking*)

Peranan: Pentadbir Sistem ICT

Organisasi perlu menggunakan salah satu daripada teknik data penyamaran untuk melindungi data yang sensitif. Di antaranya ialah :

i. Obfuscation
ii. Encryption
iii. Tokenization

Apabila menggunakan salah satu daripada teknik ini, organisasi harus mempertimbangkan:

i. Penyamaran data hendaklah digunakan pada semua data sensitif tanpa mengira format dan lokasi.
ii. Data sensitif hendaklah dienkripsi (*Encryption*) menggunakan *algorithm* khas yang tidak dapat dipulihkan.

4.12 Pencegahan Pencerobohan Data

Peranan: Pentadbir Sistem ICT

Pencegahan Kebocoran Data adalah proses kerja untuk mengesan dan menghalang sebarang pendedahan atau aktiviti pengekstrakan data tanpa

kebenaran yang dilakukan oleh individu atau sistem. Langkahlangkah berikut perlu dibuat bagi mencegah kebocoran data :

i. Mengenalpasti dan mengklasifikasikan maklumat untuk dilindungi daripada kebocoran data;
ii. Memantau sumber atau saluran kebocoran maklumat;
iii. Melaksanakan langkah pencegahan untuk mengelakkan kebocoran data;
iv. Mengehadkan capaian pengguna; dan
v. Memastikan proses sandaran maklumat dilindungi seperti penyulitan

4.13 Sandaran Maklumat (Backup)

Peranan: ICTSO, Pentadbir Pusat Data dan Pentadbir Sistem/Aplikasi

Proses sandaran data dan maklumat perlu dilaksanakan secara berkala bagi memastikan pemulihan data dapat dilakukan sekiranya berlaku kehilangan, kerosakan, atau insiden keselamatan siber yang tidak dijangka. Perkarap-erkara yang perlu dipatuhi adalah seperti yang berikut:

i. Sandaran daripada *server* atau komputer ke media storan lain perlu dilakukan dari masa ke semasa untuk mengelak kehilangan data sekiranya berlaku kerosakan *hard disk*;
ii. Kekerapan sandaran data bergantung kepada keperluan operasi dan kepentingan data tersebut sama ada secara harian, mingguan atau pun bulanan;
iii. Sandaran sistem aplikasi dan sistem pengoperasian perlu diadakan sekurangkurang sekali bagi setiap versi;
iv. Sandaran yang melibatkan saiz data yang besar hendaklah dibuat di luar waktu bekerja untuk mengelakkan kesesakan rangkaian serta mengganggu prestasi server;
v. Sandaran data yang penting dan kritikal dicadangkan dibuat di satu (1) salinan dan disimpan di lokasi *offsite* yang berasingan bagi mengelakkan kemusnahan atau kerosakan fizikal disebabkan oleh bencana seperti

kebakaran, banjir atau sebagainya;

vi. Sistem sandaran sedia ada hendaklah diuji bagi memastikan ianya dapat berfungsi, boleh dipercayai dan berkesan apabila digunakan (restoration) khususnya pada waktu kecemasan; dan

vii. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam melakukan sandaran serta merancang penyalinan semula kepada media storan yang baru.

4.14 Lewahan (*Redundancy*) Kemudahan Pemprosesan Maklumat

Peranan: Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem ICT

Kemudahan pemprosesan maklumat Kerajaan Negeri Perlis perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji keberkesanannya dari semasa ke semasa melalui aktiviti simulasi. Perkara yang perlu dipatuhi adalah seperti berikut:

i. Memastikan rangkaian mempunyai ciri *redundancy* bagi menyokong kelangsungan operasi ICT;

ii. Menyediakan sekurangkurangnya satu (1) pusat data dan satu (1) pusat pemulihan bencara (DRC) yang terletak di lokasi berbeza;

iii. Menggunakan sumber kuasa elektrik yang mempunyai sistem *redundancy* bagi menjamin bekalan kuasa berterusan;

iv. Mengaplikasikan perkakasan atau perisian yang menyokong fungsi pengimbangan beban secara automatik (automatic load balancing); dan

v. Memastikan server atau peralatan rangkaian dilengkapi dengan komponen pendua sebagai langkah sokongan.

4.15 Logging

4.15.1 Sistem Log

Peranan: ICTSO dan Pentadbir Sistem ICT

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula bagi menghalang daripada akses yang tidak dibenarkan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:

i. Fail log sistem pengoperasian;
ii. Fail log servis (contoh: web, emel); dan
iii. Fail log aplikasi (*audit trail*).

4.16 Aktiviti Pemantauan

Peranan: Pentadbir Sistem ICT

Aktiviti pemantauan perlu dilakukan bagi memastikan rangkaian, sistem, dan aplikasi dipantau daripada sebarang aktiviti anomali agar tindakan yang sesuai dapat diambil.

Operasi pemantauan merangkumi aktiviti berikut:

a) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari masa ke semasa;
b) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya;
c) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
d) Sekiranya wujud aktivitiaktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah mel-

aporkan kepada ICTSO; dan

e) Memantau trafik keluar dan masuk dalam rangkaian dan sistem aplikasi.

4.17 Penyeragaman Waktu

Peranan: ICTSO san Pentadbir Sistem ICT

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Pentadbiran Kerajaan Negeri Perlis atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang diguna pakai berdasarkan Waktu Piawai Malaysia.

4.18 Penggunaan Program Utiliti Khas

Peranan: Pentadbir Sistem ICT, SUB dan Ketua Jabatan

Bagi memastikan penggunaan program utiliti khas tidak menjejaskan keselamatan maklumat dan sistem aplikasi, perkaraperkara yang berikut hendklah dipatuhi:

a) Hanya program utiliti yang diperakui sahaja dibenarkan;
b) Penggunaan program atau perisian khas utiliti yang membebankan kapasiti (*bandwidth*) rangkaian perlu dihadkan;
c) Mengawal bilangan pengguna yang dibenarkan untuk menggunakan program utiliti;
d) Memastikan penggunaan ID yang unik sebagai pengesahan untuk akses;
e) Menutup program utiliti yang tidak berkaitan; dan
f) Menyimpan log program utiliti

4.19 Pemasangan Perisian pada Sistem Pengoperasian

Peranan: ICTSO, Pentadbir Sistem/Aplikasi, Pentadbir Rangkaian dan Keselamatan dan Pentadbir Pusat Data

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkahlangkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:

i. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;
ii. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan
iii. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.
iv. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga Pentadbiran Kerajaan Negeri Perlis, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT;
v. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah manamana undangundang bertulis yang berkuat kuasa; dan
vi. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

4.20 Keselamatan Rangkaian

Peranan: SUB, Pentadbir Sistem ICT dan Pentadbir Rangkaian

Kawalan keselamatan rangkaian perlu dilaksanakan bagi melindungi daripada akses yang tidak dibenarkan dan bagi melindungi maklumat dan kemudahan ICT daripada ancaman.

Perkaraperkara yang perlu dipatuhi adalah seperti berikut:

a) Menetapkan tanggungjawab dan prosedur bagi pengurusan rangkaian;
b) Mengemas kini maklumat rangkaian secara berterusan seperti diagram rangkaian dan fail konfigurasi peranti;
c) Memantau secara berkala log masuk untuk mengesan insiden keselamatan;
d) Mengehadkan akses peranti rangkaian bagi pentadbir rangkaian dan keselamatan berbanding pengguna biasa;
e) Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti yang ditetap-

kan;

f) Sebarang cubaan menceroboh dan aktiviti yang boleh mengancam sistem dan maklumat perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan seperti *Web Application Firewall* (WAF);
g) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan Pejabat Setiausaha Kerajaan Negeri Perlis;
h) Capaian ke atas kemudahan port diagnostik dan konfigurasi hendaklah dikawal;

4.21 Keselamatan Perkhidmatan Rangkaian

Peranan: ICTSO, Pentadbir Rangkaian dan Pentadbir Keselamatan

Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.

4.22 Pengasingan dalam Rangkaian

Peranan: ICTSO, Pentadbir Rangkaian dan Pentadbir Keselamatan

Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian di bawah Pentadbiran Kerajaan Negeri Perlis. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Menyediakan segmen yang hanya untuk kegunaan warga PSUKPs;
ii. Menetapkan segmen yang berbeza bagi pengguna biasa, pentadbir, pelayan, sistem aplikasi dan pihak luaran;
iii. Mengasingkan akses rangkaian mengikut tahap kritikal dan sensitiviti atau lainlain keperluan;
iv. Memastikan penggunaan peralatan keselamatan seperti *firewall* atau *router* bagi mengawal segmen rangkaian;
v. Mengasingkan rangkaian tanpa wayar dengan rangkaian dalaman;
vi. Mengasingkan akses rangkaian tanpa wayar untuk pelawat dan warga

PSUKPs; dan

vii. Mengawal akses kepada peralatan rangkaian bagi pengguna yang dibenarkan sahaja.

4.23 *Web Flitering*

Peranan: ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem/Aplikasi

Kawalan atau penapisan web perlu dilakukan bagi memastikan akses ke laman web dilindungi dan menyekat akses dan aktiviti yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Menyekat akses kepada alamat IP atau domain laman web yang tidak dibenarkan;

ii. Memantau laman web yang menawarkan fungsi muat naik maklumat;

iii. Menyekat laman web yang mengandungi ancaman seperti *phishing* dan kod hasad;

iv. Mengemas kini pangkalan data tandatangan (signature database) peralatan keselamatan web melalui sumber yang dipercayai;

v. Menyekat laman web perkongsian maklumat yang menyalahi undan-gundang;

vi. Menyediakan latihan teknikal kepada kakitangan berkaitan pengendalian peralatan keselamatan laman web; dan

vii. Melaksanakan program kesedaran kepada pengguna tentang amalan

4.24 Penggunaan Kriptografi

Peranan: ICTSO dan Pentadbir Sistem/Aplikasi

Penggunaan Kriptografi adalah untuk melindungi kerahsiaan dan integriti maklumat. Kriptografi merangkumi kaedahkaedah seperti yang berikut:

i. **Enkripsi**

Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*).

ii. **Tandatangan Digital**

Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. Pengurusan ke atas Perkhidmatan Prasarana Kunci Awam Kerajaan (MyGPKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

4.25 Kitaran Hidup Pembangunan Selamat

Peranan: ICTSO, Ketua Jabatan dan Pentadbir Sistem ICT

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Keselamatan persekitaran pembangunan;
ii. Keselamatan pangkalan data;
iii. Keperluan keselamatan dalam fasa reka bentuk;
iv. Keperluan *check point* keselamatan dalam carta perbatuan projek;
v. Keperluan pengetahuan ke atas keselamatan aplikasi;
vi. Keselamatan dalam kawalan versi.

Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

4.26 Keperluan Keselamatan Aplikasi

Peranan: Pentadbir Sistem ICT

Perkara yang perlu dipertimbangkan adalah seperti berikut:

i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Kerajaan Negeri Perlis. Contoh perkhidmatan sumber luaran ialah:

a) Perisian Sebagai Satu Perkhidmatan;

b) Platform Sebagai Satu Perkhidmatan;

c) Infrastruktur Sebagai Satu Perkhidmatan;

d) Storan pengkomputeran Awan; dan

e) Pemantauan Keselamatan.

ii. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

iii. Tahap kerahsiaan bagi mengenal pasti identiti masingmasing, misalnya melalui pengesahan (authentication);

iv. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

v. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT;

vi. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak; dan

vii. Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, panduan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

1. Penggunaan tanda tangan elektronik oleh setiap pihak yang terlibat dalam transaksi.

2. Memastikan semua aspek transaksi dipatuhi:
   a) Maklumat pengesahan pengguna adalah sah digunakan dan

telah disahkan;

b) Mengekalkan kerahsiaan maklumat;

c) Mengekalkan privasi pihak yang terlibat; dan

d) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.

4.27 Senibina Sistem Selamat dan Prinsip Kejuruteraan

Peranan: SUB, Ketua Jabatan dan Pentadbir Sistem ICT

Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

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

ii. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

iii. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan

iv. Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

4.28 *Secure Coding*

Peranan: ICTSO dan Pentadbir Sistem/Aplikasi

Secure coding atau pengekodan selamat adalah bagi memastikan kod pengaturcaraan yang selamat digunakan dalam pembangunan sistem dan

aplikasi bagi meminimumkan kelemahan dalam sistem yang dibagunkan. Amalan dan prosedur pengekodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengekodan:

i. Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan.
ii. Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan yang hendak dilakukan hendaklah dibuat pengujian dan pengaturcaraan pasangan.
iii. Penggunaan kaedah pengaturcaraan yang berstruktur.
iv. Dokumentasi kod dan penyingkiran kecacatan kod.
v. Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan berkod keras.
vi. Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan

4.29 Ujian Keselamatan Dalam Pembangunan dan Penerimaan

Peranan: Pentadbir Sistem ICT dan ICTSO

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;
ii. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan
iii. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.

4.29.1 Pengujian Penerimaan Sistem

Peranan: Pengguna, Pentadbir Sistem ICT dan ICTSO

Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan

ii. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner/penetration test*).

4.30 Pembangunan Sistem Secara Luaran

Peranan: ICTSO, Pentadbir Sistem/Aplikasi dan Pihak Ketiga

Pentadbiran Kerajaan Negeri Perlis hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) adalah menjadi HAK MILIK Pentadbiran Kerajaan Negeri Perlis. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Perkiraan perlesenan, kod sumber ialah HAK MILIK Pentadbiran Kerajaan Negeri Perlis dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*;

ii. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko";

iii. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar

mengikut amalan terbaik;

iv. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;

v. Mengguna pakai prinsip dan tatacara *escrow*; dan

vi. Mematuhi keberkesanan kawalan dan undangundang dalam

4.31 Persekitaran Pembangunan Perisian, Pengujian dan Pengeluaran

Peranan: ICTSO, Pentadbir Sistem/Aplikasi dan Pihak Ketiga

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkaraperkara yang perlu dipatuhi adalah seperti yang berikut:

i. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*).

ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

iii. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

4.31.1 Persekitaran Pembangunan Selamat

Peranan: Pentadbir Sistem ICT, SUB dan Ketua Jabatan

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

Pentadbiran Kerajaan Negeri Perlis perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

i. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;
ii. Terpakai kepada keperluan undangundang dan peraturan dalaman dan luaran;
iii. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;
iv. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;
v. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan
vi. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

4.32 Pengurusan Perubahan

Peranan: SUB, Ketua Jabatan dan Pentadbir Sistem ICT

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkaraperkara berikut:

i. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
ii. Aktivitiaktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini manamana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
iii. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
iv. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak sengaja.

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

vi. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor.

vii. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja.

viii. Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja

ix. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; dan

x. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum

4.33 Maklumat Pengujian

Peranan: ICTSO dan Pentadbir Sistem ICT

Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;

ii. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;

iii. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan

iv. Mengaktifkan *log audit* bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.

4.34 Perlindungan Sistem Maklumat Semasa Ujian Audit

Peranan: ICTSO dan Pentadbir Sistem/Aplikasi

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktivitiaktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumatmaklumat berikut:

i. Rekod setiap aktiviti transaksi;

ii. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

iii. Aktiviti capaian pengguna ke atas sistem ICT samada secara sah atau sebaliknya; dan

iv. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciriciri 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.

Lampiran A

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
(PKS)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan/Bahagian/Syarikat: .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukanperuntukan yang terkandung di dalam Polisi Keselamatan Siber Kerajaan Negeri Perlis; dan

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

Tandatangan : .....

Tarikh : .....

Lampiran B

RUJUKAN

Polisi Keselamatan Siber Kerajaan Negeri Perlis ini hendaklah dibaca bersama dengan akta, warta kerajaan, pekeliling, surat pekeliling, dan peraturan yang berkaitan dan sedang berkuatkuasa sepert berikut:

1. Arahan Keselamatan (Semakan dan Pindaan 2017);
2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
3. Malaysian *Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);
4. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
5. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan PenerimaanTender";
6. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
7. Akta Tandatangan Digital 1997;
8. Akta Rahsia Rasmi 1972;
9. Akta Jenayah Komputer 1997;
10. Akta Hak Cipta (Pindaan) Tahun 1997;
11. Akta Komunikasi dan Multimedia 1998;
12. PerintahPerintah Am;
13. Arahan Perbendaharaan;
14. Arahan Teknologi Maklumat 2007;
15. Surat Akujanji;
16. Myportfolio;
17. Pelan Kesinambungan Perkhidmatan;
18. Surat Arahan MAMPU.7021/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk "Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensiagensi Kerajaan";
19. Surat Arahan MAMPU.BDPICT(S) 7006/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
20. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";
21. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan ISMS Dalam Sektor Awam;

22. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
23. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
24. Garis Panduan GPKI;
25. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 "Langkahlangkah mengenai penggunaan Mel Elektronik Agensi - Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC).
26. Pekeliling AM Bilangan 4 Tahun 2022 “Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam”;
27. Surat Pekeliling AM Bilangan 3 Tahun 2024 “Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam”; dan
28. Surat Pekeliling AM Bilangan 4 Tahun 2024 “Garis Panduan Penilaian Tahap Keselamatan Keselamatan Maklumat Sektor Awam”.
29. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam.
30. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 2 Tahun 2021 Dasar Perkongsian Data Sektor Awam.