

PEJABAT SETIAUSAHA
KERAJAAN NEGERI PERLIS

PKS
2023

POLISI KESELAMATAN SIBER

VERSI 1.0

KERAJAAN
NEGERI PERLIS



SEJARAH DOKUMEN

TARIKH	KELULUSAN	VERSI	TARIKH
7 APRIL 2023	Minit Mesyuarat Jawatankuasa Pemandu Bil.1/2023	1.0	2023

ISI KANDUNGAN

PENGENALAN		11
OBJEKTIF		11
SKOP		12
PRINSIP-PRINSIP		12
PENILAIAN RISIKO KESELAMATAN ICT		14
1.	**BIDANG 01 POLISI KESELAMATAN MAKLUMAT**	15
1.1.	Hala Tuju Pengurusan Untuk Keselamatan Maklumat	15
1.1.1.	Pelaksanaan Polisi	15
1.1.2.	Penyebaran Polisi	15
1.1.3.	Penyelenggaraan Polisi	15
1.1.4.	Pengecualian Polisi	16
2.	**BIDANG 02 PERANCANGAN BAGI KESELAMATAN ORGANISASI**	16
2.1.	Infrastruktur Organisasi Keselamatan	16
2.1.1.	YB Setiausaha Kerajaan Negeri	16
2.1.2.	Ketua Pegawai Digital (CDO)	16
2.1.3.	Pegawai Keselamatan ICT (ICTSO)	17
2.1.4.	Setiausaha Bahagian (SUB) dan Ketua Jabatan Negeri Perlis	17
2.1.5.	Pentadbir Sistem ICT	18
2.1.6.	Jawatankuasa Pemandu ICT (JPICT) Negeri Perlis	18
2.1.7.	Jawatankuasa Pelaksana ISMS Pejabat Setiausaha Kerajaan Negeri Perlis	18
2.1.8.	Pasukan Tindak Balas Insiden Keselamatan ICT (PCERT)	19
2.1.9.	Pengguna	20
2.1.10.	Pengasingan Tugas	20
2.2.	Pihak Ketiga	21
2.2.1.	Hubungan Dengan Pihak Berkuasa	21
2.2.2.	Hubungan Dengan Kumpulan Berkepentingan Yang Khusus	21
2.2.3.	Keselamatan Maklumat dalam Pengurusan Projek	22
2.3.	Peranti Mudah Alih dan Telekerja	22
2.3.1.	Polisi Peranti Mudah Alih	22
2.3.2.	Penggunaan Peralatan Mudah Alih	23
2.3.3.	Telekerja	23
2.3.4.	*Bring Your Own Device* (BYOD)	24
3.	**BIDANG 03 KESELAMATAN SUMBER MANUSIA**	25
3.1.	Sebelum Perkhidmatan	25
3.1.1.	Tapisan Keselamatan	25
3.1.2.	Terma dan Syarat Perkhidmatan	25

3.2.	Dalam Tempoh Perkhidmatan	26
3.2.1.	Tanggungjawab Pengurusan	26
3.2.2.	Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat	26
3.2.3.	Proses Tatatertib	26
3.2.4.	Penamatan atau Pertukaran Tanggungjawab Perkhidmatan	27
4.	**BIDANG 04 PENGURUSAN ASET**	28
4.1.	Tanggungjawab Terhadap Aset	28
4.1.1.	Inventori Aset ICT	28
4.1.2.	Pemilikan Aset	28
4.1.3.	Penggunaan Aset yang Dibenarkan	28
4.1.4.	Pemulangan Aset	29
4.2.	Pengelasan Maklumat	29
4.2.1.	Pengelasan Maklumat	29
4.2.2.	Pelabelan Maklumat	29
4.2.3.	Pengendalian Aset	29
4.3.	Pengendalian Media	30
4.3.1.	Pengurusan Media Boleh Alih	30
4.3.2.	Pemindahan dan Pelupusan Media	30
5.	**BIDANG 05 KAWALAN AKSES**	31
5.1.	Dasar Kawalan Akses	31
5.1.1.	Keperluan Polisi Kawalan Capaian	31
5.1.2.	Capaian kepada Rangkaian dan Perkhidmatan Rangkaian	31
5.2.	Pengurusan Akses Pengguna	32
5.2.1.	Pendaftaran dan Pembatalan Pengguna	32
5.2.2.	Peruntukan Akses Pengguna	32
5.2.3.	Pengurusan Hak Akses Istimewa	32
5.2.4.	Pengurusan Maklumat Pengesahan Rahsia Pengguna	32
5.2.5.	Kajian Semula Hak Akses Pengguna	32
5.2.6.	Pembatalan atau Pelarasan Hak Akses	33
5.3.	Tanggungjawab Pengguna	33
5.3.1.	Penggunaan Maklumat Pengesahan Rahsia (*Secret Authentication*)	33
5.4.	Kawalan Akses Sistem dan Aplikasi	34
5.4.1.	Sekatan Akses Maklumat	34
5.4.2.	Prosedur Log Masuk yang Selamat	34
5.4.3.	Sistem Pengurusan Kata Laluan	34
5.4.4.	Penggunaan Program Utiliti yang Mempunyai Hak Istimewa	35

5.4.5.	Kawalan Akses Kepada Kod Sumber Program	35
6.	**BIDANG 06 KRIPTOGRAFI**	36
6.1.	Kawalan Kriptografi	36
6.1.1.	Polisi Penggunaan Kawalan Kriptografi	36
6.1.2.	Pengurusan Kunci Awam (*Public Key Management*)	36
7.	**BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN**	37
7.1.	Kawasan Selamat	37
7.1.1.	Perimeter Keselamatan Fizikal	37
7.1.2.	Kawalan Kemasukan Fizikal	37
7.1.3.	Keselamatan Pejabat, Bilik dan Kemudahan	38
7.1.4.	Perlindungan Daripada Ancaman Luar dan Persekitaran	38
7.1.5.	Bekerja di Kawasan Selamat	38
7.1.6.	Kawasan Penyerahan dan Pemunggahan	38
7.2.	Peralatan ICT	39
7.2.1.	Penempatan dan Perlindungan Peralatan ICT	39
7.2.2.	Utiliti Sokongan	40
7.2.3.	Keselamatan Kabel	40
7.2.4.	Penyelenggaraan Peralatan	40
7.2.5.	Pengalihan Aset	41
7.2.6.	Keselamatan Peralatan dan Aset di Luar Premis	41
7.2.7.	Pelupusan yang Selamat atau Penggunaan Semula Peralatan	41
7.2.8.	Dasar Meja Kosong dan Skrin Kosong	43
8.	**BIDANG 08 KESELAMATAN OPERASI**	44
8.1.	Prosedur dan Tanggungjawab Operasi	44
8.1.1.	Prosedur Operasi yang Didokumenkan	44
8.1.2.	Pengurusan Perubahan	44
8.1.3.	Pengurusan Kapasiti	45
8.1.4.	Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi	45
8.1.5.	Kawalan dan Perlindungan Daripada Perisian Hasad	46
8.1.6.	Sandaran Maklumat (*Information Backup)*	46
8.1.7.	Pengelogan Kejadian (*Event Logging*)	47
8.1.8.	Log Pentadbir dan Pengendali	47
8.1.9.	Penyeragaman Waktu	48
8.1.10.	Pemasangan Perisian pada Sistem yang Beroperasi	48
8.1.11.	Sekatan ke atas Pemasangan Perisian	48
8.1.12.	Jejak Audit	49
9.	**BIDANG 09 KESELAMATAN KOMUNIKASI**	50

9.1.	Pengurusan Keselamatan Rangkaian	50
9.1.1.	Kawalan Rangkaian	50
9.1.2.	Keselamatan Perkhidmatan Rangkaian	51
9.1.3.	Pengasingan dalam Rangkaian	51
9.2.	Pemindahan Data dan Maklumat	51
9.2.1.	Polisi dan Prosedur Pemindahan Data dan Maklumat	51
9.2.2.	Perjanjian Mengenai Pemindahan Data dan Maklumat	52
9.2.3.	Pesanan Elektronik	52
9.2.4.	Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality or Non-Disclosure Agreements*)	52
10.	**BIDANG 10 PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM**	53
10.1.	Keperluan Keselamatan Sistem Maklumat	53
10.1.1.	Analisis dan Spesifikasi Keperluan Keselamatan Maklumat	53
10.2.	Keselamatan Dalam Proses Pembangunan dan Sokongan	53
10.2.1.	Dasar Pembangunan Selamat	54
10.2.2.	Prosedur Kawalan Perubahan Sistem	54
10.2.3.	Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi	54
10.2.4.	Persekitaran Pembangunan Selamat	55
10.2.5.	Pembangunan oleh Khidmat Luaran (*Outsource*)	55
10.2.6.	Pengujian Keselamatan Sistem	56
10.2.7.	Pengujian Penerimaan Sistem	56
10.2.8.	Data Ujian	56
10.2.9.	Perlindungan Data Ujian	56
11.	**BIDANG 11 HUBUNGAN DENGAN PEMBEKAL**	57
11.1.	Keselamatan Maklumat Dalam Hubungan Pembekal	57
11.1.1.	Polisi Keselamatan Maklumat Untuk Hubungan Pembekal	57
11.1.2.	Menangani Keselamatan Dalam Perjanjian Pembekal	57
11.1.3.	Rantaian Bekalan Teknologi Maklumat dan Komunikasi	58
11.1.4.	Memantau dan Mengkaji Semula Perkhidmatan Pembekal	58
11.1.5.	Menguruskan Perubahan Kepada Perkhidmatan Pembekal	59
12.	**BIDANG 12 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT**	60
12.1.	Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan	60
12.1.1.	Tanggungjawab dan Prosedur	60
12.1.2.	Pelaporan Kejadian Keselamatan Maklumat	60
12.1.3.	Pelaporan Kelemahan Keselamatan Maklumat	61
12.1.4.	Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat	61
12.1.5.	Tindak Balas Terhadap Insiden Keselamatan Maklumat	61

12.1.6.	Pembelajaran Daripada Insiden Keselamatan Maklumat	62
13.	**BIDANG 13 ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**	63
13.1.	Kesinambungan Keselamatan Maklumat	63
13.1.1.	Pelan Kesinambungan Keselamatan Maklumat	63
13.1.2.	Menentusah, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat	63
13.2.	Lewahan (*Redundancy*)	64
13.2.1.	Ketersediaan Kemudahan Pemprosesan Maklumat	64
14.	**BIDANG 14 PEMATUHAN**	65
14.1.	Pematuhan Terhadap Keperluan Perundangan dan Kontrak	65
14.1.1.	Pematuhan Dasar	65
14.1.2.	Hak Harta Intelek	65
14.1.3.	Perlindungan Rekod	65
14.1.4.	Privasi dan Perlindungan Maklumat Peribadi	65
14.1.5.	Pematuhan Polisi dan Standard Keselamatan	66
14.1.6.	Pelanggaran Dasar	66

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 Closed-Circuit Television System	Sistem TV yang digunakan secara komersil 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 bila-bila 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 kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
CERT MAMPU	Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT MAMPU.
ICT	Information and Communication Technology
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke alas system 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 rangkaian-rangkaian tersebut agar sentiasa berasingan.

Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based JPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
ISMS	*Information Security Management System* (Sistem Pengurusan Keselamatan Maklumat)
MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
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.
LAN Local Area Network	Rangkaian Kawasan Setempat yang menghubungkan komputer.
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 aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan
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	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.
Screen saver	Imej yang akan diaktifkan pada system computer 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.

Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan alasan sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

.



POLISI KESELAMATAN SIBER KERAJAAN NEGERI PERLIS

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.

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 pihak-pihak 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;
vi. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
vii. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

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

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

PRINSIP-PRINSIP

Prinsip-prinsip 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 lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mecorakkan 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 vulnerability yang semakin meningkat hari ini. Justeru, warga Pentadbiran Kerajaan Negeri Perlis perlu mengambil langkah-langkah 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 langkah-langkah 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 sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Kerajaan Negeri Perlis bertanggungjawab melaksanakan dan menguruskan Penilaian Risiko Keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. Kerajaan Negeri Perlis perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

i. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
ii. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
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 pihak-pihak yang berkepentingan.

1. BIDANG 01 POLISI KESELAMATAN MAKLUMAT

1.1. Hala Tuju Pengurusan Untuk 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 lain-lain).

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. Bila mana sesuatu keperluan untuk pengecualian terhadap kepatuhan polisi ini harus dikemukakan kepada ICTSO dan mendapat perakuan JPICT.

2. BIDANG 02 PERANCANGAN BAGI KESELAMATAN ORGANISASI

2.1. Infrastruktur Organisasi Keselamatan

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

2.1.1. 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 peruntukan-peruntukan 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; dan
v. Melantik Chief Digital Officer (CDO) dan ICT Security Officer (ICTSO).

2.1.2. 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 tugas-tugas 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.

2.1.3. 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:

a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan polisi ini;
b) Menjalankan pengurusan risiko;
c) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
d) Menyedia dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
e) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
f) Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP);
g) Menyedia dan merangka program-program kesedaran mengenai keselamatan ICT.

2.1.4. 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 Pegarah 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 berkuat kuasa;
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.

2.1.5. 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 aktiviti-aktiviti 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 maklumat berkenaan secara berkala.

2.1.6. Jawatankuasa Pemandu ICT (JPICT) Negeri Perlis

Peranan: Pentadbir Sistem ICT

Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan siber.

2.1.7. 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 :

1. Pegawai Teknologi Maklumat
Bahagian Pengurusan Teknologi Maklumat

2. 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;
iii. Penetapan kriteria penerimaan risiko, tahap risiko dan risk treatment plan;
iv. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan 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 ISMS yang berterusan.

2.1.8. Pasukan Tindak Balas Insiden Keselamatan ICT (PCERT)

Peranan: PCERT

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

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. 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. Menasihati Pentadbir Sistem/Pelayan untuk mengambil tindakan pemulihan dan pengukuhan; dan
vi. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Pentadbir Sistem ICT.

2.1.9. 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 prinsip-prinsip keselamatan polisi ini dan menjaga kerahsiaan maklumat Kerajaan;
v. Menandatangani Akuan Pematuhan Polisi Keselamatan Siber Kerajaan Negeri Perlis;
vi. Melaksanakan langkah-langkah perlindungan seperti berikut:
    a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
    b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
    c) Menentukan maklumat sedia untuk digunakan;
    d) Menjaga kerahsiaan 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 langkah-langkah keselamatan ICT dari diketahui umum.
vii. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada PCERT dengan segera;
viii. Menghadiri program-program kesedaran mengenai keselamatan siber; dan
ix. Bersetuju dengan terma dan syarat yang terkandung di dalam polisi ini.

2.1.10. 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.

Perkara-perkara 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. Pegasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

2.2. Pihak Ketiga

Objektif: Menjamin keselamatan maklumat dan aset ICT semasa berurusan dengan pihak ketiga.

2.2.1. Hubungan Dengan Pihak Berkuasa

Peranan: Bahagian Khidmat Pengurusan (BKP), Pejabat Setiausaha Kerajaan Negeri Perlis, Pasukan *Emergency Response Team* (ERT) dan Pasukan PCERT

Hubungan dengan pihak berkuasa berkaitan perlulah diwujudkan dan dikekalkan. Perkara-perkara 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/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi dan Multimedia. 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.

2.2.2. Hubungan Dengan Kumpulan Berkepentingan Yang Khusus

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis (Mengikut Bidang Kepakaran)

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Merujuk pertubuhan profesional atau agensi rujukan bagi:

i. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;
ii. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;
iii. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan
iv. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

2.2.3. Keselamatan Maklumat dalam Pengurusan Projek

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis (Pasukan Projek)

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Keselamatan maklumat perlu diterapkan dalam setiap pengurusan projek di pentadbiran Kerajaan Negeri Perlis;
ii. Objektif keselamatan makumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
iii. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan 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.

2.3. Peranti Mudah Alih dan Telekerja

Objektif: Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

2.3.1. Polisi Peranti Mudah Alih

Peranan: BPTM, JPICT, Warga Pentadbiran Kerajaan Negeri Perlis

Membangun serta menyebarkan dasar dan langkah-langkah 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.

Perkara-perkara 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.

2.3.2. Penggunaan Peralatan Mudah Alih

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Capaian sistem maklumat dan aplikasi melalui peralatan mudah alih seperti telefon, tablet, notebook adalah digalakkan. Walau bagaimanapun, penggunaannya perlu mematuhi amalan keselamatan ICT.

i. Pentadbir Sistem hanya menyediakan sokongan terhad (*reasonable endeavors*) kepada pengguna bagi tujuan konfigurasi, tetapan dan penggunaan peralatan mudah alih 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 tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat;
v. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT;
vi. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan;
vii. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan;
viii. Melaporkan kehilangan peralatan mudah alih kepada ICTSO.

2.3.3. Telekerja

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Telekerja meliputi semua bentuk pelaksanaan tugasan yang dilaksanakan di luar tempat kerja. Dasar dan langkah-langkah 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. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;
ii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan
iii. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskini untuk aset ICT.

2.3.4. *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 Wi-Fi jabatan atau data *line* persendirian untuk akses kepada Internet tertakluk kepada PKS Kerajaan Negeri Perlis.

i. Pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut :
   a. Mengelakkan risiko kebocoran maklumat rasmi;
   b. Mengelakkan ancaman risiko keselamatan ICT;
   c. Meningkatkan integriti data; dan
   d. Memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan;

ii. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.

3. BIDANG 03 KESELAMATAN SUMBER MANUSIA

3.1. Sebelum Perkhidmatan

Objektif: Memastikan warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

Peranan: Bahagian Pengurusan Sumber Manusia (BPSM), PSUKPs, Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT.

3.1.1. 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. Perkara-perkara 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.

3.1.2. Terma dan Syarat Perkhidmatan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT

i. 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
ii. Memastikan semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

3.2. Dalam Tempoh Perkhidmatan

Memastikan warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding, dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan asset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

3.2.1. Tanggungjawab Pengurusan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT

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.

3.2.2. Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT

Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara 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 secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;
ii. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber Pentadbiran Kerajaan Negeri Perlis perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; 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.

3.2.3. Proses Tatatertib

Peranan: Unit Pengurusan Korporat dan Integriti (UPKI), PSUKPs

Proses tatatertib yang formal dan disampaikan kepada warga Pentadbiran Kerajaan Negeri Perlis hendaklah tersedia bagi membolehkan tindakan diambil terhadap anggota yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Memastikan adanya proses tindakan disiplin atau undang-undang ke atas warga Pentadbiran Kerajaan Negeri Perlis 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.

3.2.4. Penamatan atau Pertukaran Tanggungjawab Perkhidmatan

Objektif: Melindungi kepentingan pentadbiran Kerajaan Negeri Perlis dari segi proses penamatan dan perubahan pekhidmatan dengan memastikan pengguna dan pihak ketiga yang ditamatkan dari organisasi dan ditukarkan perkhidmatan diurus dengan teratur bagi menjamin keselamatan maklumat terjaga.

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 perkara-perkara 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.

4. BIDANG 04 PENGURUSAN ASET

4.1. Tanggungjawab Terhadap Aset

Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT di bawah Pentadbiran Kerajaan Negeri Perlis.

4.1.1. Inventori Aset ICT

Peranan: Pegawai Aset ICT dan Warga Pentadbiran Kerajaan Negeri Perlis

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT di bawah Pentadbiran Kerajaan Negeri Perlis. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara 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; dan
iii. Pegawai Aset hendaklah mengesahkan penempatan aset ICT.

4.1.2. Pemilikan Aset

Peranan: Pegawai Aset ICT dan Warga Pentadbiran Kerajaan Negeri Perlis

Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. Aset yang diselanggara hendaklah hak milik Kerajaan Negeri Perlis. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah seperti berikut:

i. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;
ii. Memastikan aset telah dikelaskan dan dilindungi;
iii. Kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;
iv. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan
v. Memastikan semua jenis aset dipelihara dengan baik.

4.1.3. Penggunaan Aset yang Dibenarkan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

4.1.4. 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.

4.2. Pengelasan Maklumat

Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

4.2.1. 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 yang berkuatkuasa.

4.2.2. Pelabelan Maklumat

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.

4.2.3. Pengendalian Aset

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan 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 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 langkah-langkah keselamatan siber daripada diketahui umum.

4.3. Pengendalian Media

Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

4.3.1. Pengurusan Media Boleh Alih

Peranan: Pentadbir Sistem ICT dan Pengguna

Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh Pentadbiran Kerajaan Negeri Perlis. Prosedur-prosedur 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
v. Menyimpan semua jenis media di tempat yang selamat.

4.3.2. Pemindahan dan Pelupusan Media

Peranan: Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

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.

5. BIDANG 05 KAWALAN AKSES

5.1. Dasar Kawalan Akses

Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

5.1.1. Keperluan Polisi Kawalan Capaian

Peranan: Pemilik perkhidmatan digital dan Pentadbir Sistem ICT

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. Undang-undang 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*.

5.1.2. Capaian kepada Rangkaian dan Perkhidmatan Rangkaian

Peranan: ICTSO, SUB, Ketua Jabatan dan Pentadbir 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. Mewujud 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.

5.2. Pengurusan Akses Pengguna

Objektif: Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. la perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.

5.2.1. Pendaftaran dan Pembatalan Pengguna

Peranan: Semua pengguna dan warga Pentadbiran Kerajaan Negeri Perlis

Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi:

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. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Pentadbiran Kerajaan Negeri Perlis.

5.2.2. Peruntukan Akses Pengguna

Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.

5.2.3. Pengurusan 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.

5.2.4. Pengurusan Maklumat Pengesahan Rahsia Pengguna

Peranan: ICTSO dan Pentadbir Sistem ICT

Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.

5.2.5. Kajian Semula Hak Akses Pengguna

Peranan: Pemilik aset/projek dan Pentadbir Sistem ICT

Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang diletapkan. Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.

5.2.6. Pembatalan atau Pelarasan Hak Akses

Peranan: Pentadbir Sistem ICT, SUB dan Ketua Jabatan

Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak/perjanjian atau diselaraskan apabila berlaku perubahan dalam pentadbiran Kerajaan Negeri Perlis.

5.3. Tanggungjawab Pengguna

Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

Peranan: Pengguna, Pentadbir Sistem ICT, SUB dan Ketua Jabatan

5.3.1. Penggunaan Maklumat Pengesahan Rahsia (*Secret Authentication*)

Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

i. Membaca, memahami dan mematuhi Polisi Keselamatan Siber Kerajaan Negeri Perlis;
ii. Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;
iii. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat Kerajaan Negeri Perlis;
iv. Melaksanakan langkah-langkah perlindungan seperti yang berikut:
    a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
    b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
    c) Menentukan maklumat sedia untuk digunakan;
    d) Menjaga kerahsiaan kata laluan;
    e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
    f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
    g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.
v. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan
vi. Menghadiri program-program kesedaran mengenai keselamatan siber.

5.4. Kawalan Akses Sistem dan Aplikasi

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.

Peranan: Pengguna, Pentadbir Sistem ICT, ICTSO, SUB dan Ketua Jabatan

5.4.1. Sekatan Akses Maklumat

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.

5.4.2. Prosedur Log Masuk yang Selamat

Peranan: Pentadbir Sistem ICT, ICTSO, SUB dan Ketua Jabatan

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;
vi. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

5.4.3. Sistem Pengurusan Kata Laluan

Peranan: Pengguna, Pentadbir Sistem ICT, ICTSO, SUB dan Ketua Jabatan

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 sekurang-kurangnya 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 atur cara;
vii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan
viii. Mengelakkan penggunaan semula kata laluan yang pernah digunakan sebelum ini.

5.4.4. Penggunaan Program Utiliti yang Mempunyai Hak Istimewa

Peranan: Pentadbir Sistem ICT, SUB dan Ketua Jabatan

Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.

5.4.5. Kawalan Akses Kepada Kod Sumber Program

Peranan: Pengurus Projek dan Pentadbir Sistem ICT

Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara 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.

6. BIDANG 06 KRIPTOGRAFI

6.1. Kawalan Kriptografi

Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.

6.1.1. Polisi Penggunaan Kawalan Kriptografi

Peranan: Pengarah Projek

Kriptografi merangkumi kaedah-kaedah 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.

6.1.2. Pengurusan Kunci Awam (Public Key Management)

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

7. BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN

7.1. Kawasan Selamat

Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh menyebabkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat pentadbiran Kerajaan Negeri Perlis.

7.1.1. Perimeter Keselamatan Fizikal

Peranan: Pemilik Premis, Pentadbir Sistem ICT, Bahagian Khidmat Pengurusan dan Pihak Ketiga

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

a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
c) Mereka bentuk dan melaksanakan perlindungan fizikal di dalam pejabat, bilik dan kemudahan daripada kebakaran, banjir, letupan dan sebarang bencana alam atau perbuatan manusia;
d) Memasang alat penggera atau kamera keselamatan; dan
e) Mewujudkan perkhidmatan kawalan keselamatan.

7.1.2. Kawalan Kemasukan Fizikal

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

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 kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan;
iii. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT Kerajaan Negeri Perlis; dan
iv. Kehilangan pas hendaklah dilaporkan segera.

7.1.3. Keselamatan Pejabat, Bilik dan Kemudahan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT 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.

7.1.4. Perlindungan Daripada Ancaman Luar dan Persekitaran

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

Peranan: Pentadbir Pusat Data dan Bahagian Khidmat Pengurusan

7.1.5. Bekerja di Kawasan Selamat

Objektif: 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 ciri-ciri 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 lain-lain 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; dan
vi. Mengehadkan jalan keluar masuk.

7.1.6. Kawasan Penyerahan dan Pemunggahan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

Titik kemasukan *access point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. Kerajaan Negeri hendaklah memastikan kawasan penghantaran dan pemunggahan dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

7.2. Peralatan ICT

Objektif: Melindungi peralatan ICT Kerajaan Negeri daripada kehilangan, kerosakan, kecurian dan disalahgunakan.

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis.

7.2.1. Penempatan dan Perlindungan Peralatan ICT

Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah 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 masing-masing 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 dikemaskini 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. Peralatan-peralatan 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 ciri-ciri keselamatan;
x. Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan 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 password administrator yang telah ditetapkan oleh pihak ICT; dan
xx. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan Kerajaan Negeri sahaja.

7.2.2. Utiliti Sokongan

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

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 (sekurang-kurangnya setahun sekali).

7.2.3. Keselamatan Kabel

Peranan: Pentadbir Sistem Rangkaian

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. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan
iv. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memaslikan keselamalan kabel daripada kerosakan bencana dan pintasan maklumat.

7.2.4. 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. Langkah-langkah 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.

7.2.5. 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.

7.2.6. Keselamatan Peralatan dan Aset di Luar Premis

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan 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. Peralatan perlu dilindungi dan dikawal sepanjang masa;
ii. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan
iii. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

7.2.7. Pelupusan yang Selamat atau Penggunaan Semula Peralatan

Peranan: Pegawai Aset, Pentadbir Sistem ICT 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. Langkah-langkah seperti yang berikut hendaklah diambil:

i. Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara 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 ciri-ciri 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 perkara-perkara seperti yang berikut:

a) Menyimpan mana-mana 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 mana-mana peralatan yang berkaitan ke mana-mana bahagian di bawah Pentadbiran Kerajaan Negeri Perlis.
d) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan.
e) Melupuskan sendiri peralatan ICT kerana kerja-kerja 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 berkuat kuasa;
ix. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan
x. Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Perakaunan Akruan Kerajaan Negeri (iSPEKS).

7.2.8. Dasar Meja Kosong dan Skrin Kosong

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada alas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:

i. Menggunakan kemudahan *password screensaver* atau *logout* apabila meninggalkan komputer;
ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;
iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimini dan mesin fotostat.
iv. Emel masuk dan keluar hendaklah dikawal; dan
v. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi
vi. penghasilan semula seperti mesin pengimbas dan kamera digital.

8. BIDANG 08 KESELAMATAN OPERASI

8.1. Prosedur dan Tanggungjawab Operasi

Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan baik dan selamat.

Peranan: SUB, Ketua Jabatan dan Pentadbir Sistem ICT

8.1.1. Prosedur Operasi yang Didokumenkan

Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut:

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

8.1.2. Pengurusan Perubahan

Peranan: 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 perkara-perkara 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. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana 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.

8.1.3. Pengurusan Kapasiti

Peranan: Pemilik Sistem dan Pentadbir Sistem

Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara 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 bersesuian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
ii. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

8.1.4. Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi

Peranan: Pentadbir Sistem ICT

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara 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.

8.1.5. Kawalan dan Perlindungan Daripada Perisian Hasad

Peranan: Pentadbir Sistem ICT dan Pengguna

Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh *malware* berbahaya seperti *virus* dan *trojan*. Perkara-perkara 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 mana-mana undang-undang bertulis yang berkuat kuasa;
iii. Megimbas 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 mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
viii. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.

8.1.6. Sandaran Maklumat (*Information Backup*)

Peranan: Pentadbir Sistem ICT

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan sandaran seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
ii. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi;
iii. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan
iv. Salinan hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurangkurangnya tiga (3) generasi.

8.1.7. Pengelogan Kejadian (*Event Logging*)

Peranan: Pentadbir Sistem ICT

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktivitiaktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. 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, e-mel);
iii. Fail log aplikasi (audit *trail*); dan
iv. Fail log rangkaian (contoh: *switch, firewall*, IPS).

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
iii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan PCERT.

8.1.8. Log Pentadbir dan Pengendali

Peranan: Pentadbir Sistem ICT dan PCERT

Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Memantau penggunaan kemudahan memproses maklumat secara berkala;
ii. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;
iii. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;
iv. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan
v. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan PCERT.

8.1.9. Penyeragaman Waktu

Peranan: Pentadbir Pusat Data

Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.

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

8.1.10. Pemasangan Perisian pada Sistem yang Beroperasi

Peranan: SUB, Ketua Jabatan dan Pentadbir Sistem ICT

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah 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.

8.1.11. Sekatan ke atas Pemasangan Perisian

Peranan: Pentadbir Sistem ICT, Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga Pentadbiran Kerajaan Negeri Perlis, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT;
ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan
iii. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

8.1.12. Jejak Audit

Peranan: Pentadbir Sistem ICT

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

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 ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan, dan pengubahsuaian yang tidak dibenarkan.

9. BIDANG 09 KESELAMATAN KOMUNIKASI

9.1. Pengurusan Keselamatan Rangkaian

Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

Peranan: SUB, Ketua Jabatan dan Pentadbir Sistem ICT

9.1.1. Kawalan Rangkaian

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;
ii. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;
iii. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;
iv. Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;
v. Firewall hendaklah dipantau, dikonfigurasi dan diselia oleh Pentadbir Keselamatan (*Admin Firewall*);
vi. Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan pentadbiran Kerajaan Negeri Perlis;
vii. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO);
viii. Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Kerajaan Negeri Perlis;
ix. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;
x. Sebarang penyambungan rangkaian yang bukan di bawah kawalan pentadbiran Kerajaan Negeri Perlis adalah tidak dibenarkan;
xi. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di bawah Pentadbiran Kerajaan Negeri Perlis sahaja dan penggunaan modem dan router persendirian adalah dilarang sama sekali;
xii. Kemudahan bagi wireless LAN hendaklah dipantau dan dikawal penggunaannya;
xiii. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;
xiv. Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian Pentadbiran Kerajaan Negeri Perlis, rangkaian agensi lain dan rangkaian awam;
xv. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;

xvi. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh;
xvii. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan Pentadbiran Kerajaan Negeri Perlis; dan
xviii. Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan Pentadbiran Kerajaan Negeri Perlis.

9.1.2. Keselamatan Perkhidmatan Rangkaian

Peranan: ICTSO, SUB, Ketua Jabatan, Pentadbir Sistem ICT dan Pembekal

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.

9.1.3. Pengasingan dalam Rangkaian

Peranan: ICTSO, SUB, Ketua Jabatan, Pentadbir Sistem ICT

Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian di bawah Pentadbiran Kerajaan Negeri Perlis.

9.2. Pemindahan Data dan Maklumat

Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara Kerajaan Negeri Perlis dan pihak luar terjamin.

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

9.2.1. Polisi dan Prosedur Pemindahan Data dan Maklumat

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 e-mel elektronik hendaklah dilindungi sebaik-baiknya.

9.2.2. Perjanjian Mengenai Pemindahan Data dan Maklumat

Peranan: CDO, SUB dan Ketua Jabatan

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.

9.2.3. Pesanan Elektronik

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis

Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti berikut:

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

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

Peranan: ICTSO, SUB, Ketua Jabatan, pengguna dan pembekal

Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan.

Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.

10. BIDANG 10 PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1. Keperluan Keselamatan Sistem Maklumat

Objektif: Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang seluruh kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan dalam rangkaian awam.

10.1.1. Analisis dan Spesifikasi Keperluan Keselamatan Maklumat

Peranan: Pentadbir Sistem ICT

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut:

i. 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;
ii. 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;
iii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan
iv. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

10.2. Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

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

10.2.2. Prosedur Kawalan Perubahan Sistem

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.

10.2.3. Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi

Peranan: Pentadbir Sistem ICT

Apabila platform operasi berubah, aplikasi penting organisasi hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; dan
ii. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan.

10.2.4. 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 undang-undang 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.

10.2.5. Pembangunan oleh Khidmat Luaran (*Outsource*)

Peranan: Pentadbir Sistem ICT, SUB, Ketua Jabatan dan ICTSO

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 undang-undang dalam melaksanakan pengesahan pengujian.

10.2.6. Pengujian Keselamatan Sistem

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.

10.2.7. 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*).

10.2.8. Data Ujian

Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.

Peranan: Pengguna, Pentadbir Sistem ICT dan ICTSO

10.2.9.Perlindungan Data Ujian

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.

11. BIDANG 11 HUBUNGAN DENGAN PEMBEKAL

11.1. Keselamatan Maklumat Dalam Hubungan Pembekal

Objektif: Memastikan aset ICT Pentadbiran Kerajaan Negeri Perlis yang boleh dicapai oleh pembekal dilindungi.

Peranan: SUB, Ketua Jabatan, Pemilik Projek dan Pembekal

11.1.1. Polisi Keselamatan Maklumat Untuk Hubungan Pembekal

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset di bawah Pentadbiran Kerajaan Negeri Perlis. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Mengawal dan memantau akses pembekal;
ii. Keperluan minimum keselamatan maklumat bagi setiap pembekaldinyatakan dalam perjanjian;
iii. Jenis-jenis obligasi kepada pembekal;
iv. Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;
v. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber Kerajaan Negeri Perlis seperti di LAMPIRAN A; dan
vi. Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.

11.1.2. Menangani Keselamatan Dalam Perjanjian Pembekal

Peranan: Syarikat Pembekal

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.

11.1.3. Rantaian Bekalan Teknologi Maklumat dan 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. Perkara-perkara 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 pembekal-pembekal 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.

11.1.4. Memantau dan Mengkaji Semula Perkhidmatan Pembekal

Peranan: SUB, Ketua Jabatan, Pemilik Projek dan Pembekal

Pentadbiran Kerajaan Negeri Perlis hendaklah sentiasa memantau dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara 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.

11.1.5. Menguruskan Perubahan Kepada Perkhidmatan Pembekal

Peranan: SUB, Ketua Jabatan, Pemilik Projek dan Pembekal

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut:

i. Perubahan dalam perjanjian dengan pembekal;
ii. Perubahan yang dilakukan oleh Pentadbiran Kerajaan Negeri Perlis bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan
iii. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.

12. BIDANG 12 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

12.1. Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan

Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminumkan kesan insiden keselamatan ICT.

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

12.1.1. Tanggungjawab dan Prosedur

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. Perkara-perkara yang perlu dipatuhi adalah sepert berikut:

i. Memberikan kesedaran berkaitan Prosedur Operasi Standard (SOP) Pengendalian Insiden dan hebahan kepada warga Pentadbiran Kerajaan Negeri Perlis sekiranya ada perubahan; dan
ii. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

12.1.2. Pelaporan Kejadian Keselamatan Maklumat

Peranan: ICTSO, SUB, Ketua Jabatan dan PCERT

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

Prosedur pelaporan insiden keselamatan siber berdasarkan:

i. Pekeliling Am Bilangan 1 Tahun 2001 -Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi;
ii. Surat Pekeliling Am Bilangan 4 Tahun 2006 -Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan
iii. Prosedur Operasi Standard: Pengendalian Insiden Kerajaan Negeri Perlis.

12.1.3. Pelaporan Kelemahan Keselamatan Maklumat

Peranan: Warga Pentadbiran Kerajaan Negeri Perlis, pembekal, dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Perlis

Warga Pentadbiran Kerajaan Negeri Perlis dan pembekal yang menggunakan sistem dan perkhidmatan maklumat dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.

12.1.4. Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat

Peranan: ICTSO

Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

12.1.5. 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.

Kawalan-kawalan 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 forensik sekiranya perlu;
ii. Menghubungi pihak yang berkenaan dengan secepat mungkin;
iii. Menyimpan jejak audit, sandaran 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;
vi. Menyediakan tindakan pemulihan segera; dan
vii. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

12.1.6. Pembelajaran Daripada Insiden Keselamatan Maklumat

Peranan: ICTSO, 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.

13. BIDANG 13 ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

13.1. Kesinambungan Keselamatan Maklumat

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

13.1.1. Pelan Kesinambungan Keselamatan Maklumat

Peranan: Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis dan Pasukan Pemulihan Bencana ICT

Pelan kesinambungan perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. PKP perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian:

i. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
ii. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
iii. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
iv. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; dan
v. Melaksanakan penyelenggaraan ke atas pelan tersebut.

13.1.2. Menentusah, Mengkaji Semula dan Menilai Kesinambungan Keselamatan 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.

13.2. Lewahan (*Redundancy*)

Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

13.2.1. Ketersediaan 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 (*failover test*) keberkesanannya dari semasa ke semasa

14. BIDANG 14 PEMATUHAN

14.1. Pematuhan Terhadap Keperluan Perundangan dan Kontrak

Objektif: Meningkatkan tahap keselamatan ICT bagi megelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

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

14.1.1. Pematuhan Dasar

Setiap pengguna di bawah Kerajaan Negeri Perlis hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber Kerajaan Negeri Perlis dan undang-undang 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.

14.1.2. Hak Harta Intelek

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

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak intelektual. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

14.1.3. Perlindungan Rekod

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

Rekod 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.

14.1.4. 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 undang-undang dan peraturan-peraturan Kerajaan Malaysia. kecemasan.

14.1.5. Pematuhan Polisi dan Standard Keselamatan

Peranan: SUB, Pemilik Perkhidmatan dan Ketua Jabatan

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.

14.1.6. Pelanggaran Dasar

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

Pelanggaran Polisi Keselamatan Siber Kerajaan Negeri Perlis boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab "D" - Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib).

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER (PKS)
KERAJAAN NEGERI PERLIS

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 peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Kerajaan Negeri Perlis; dan

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

Tandatangan : .....

Tarikh : .....

LAMPIRAN B

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan dan sedang berkuatkuasa yang perlu dipatuhi oleh warga Pentadbiran Kerajaan Negeri Perlis. Antaranya adalah seperti berikut:

1. Arahan Keselamatan;
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 Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di AgensiAgensi Kerajaan";
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
7. Surat Pekeliling Am Bil. 4 Tahun 2006 - "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";
8. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan PenerimaanTender";
9. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
10. Akta Tandatangan Digital 1997;
11. Akta Rahsia Rasmi 1972;
12. Akta Jenayah Komputer 1997;
13. Akta Hak Cipta (Pindaan) Tahun 1997;
14. Akta Komunikasi dan Multimedia 1998;
15. Perintah-Perintah Am;
16. Arahan Perbendaharaan;
17. Arahan Teknologi Maklumat 2007;
18. Standard Operating Procedure (SOP) ICT MAMPU;
19. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";
20. Etika Penggunaan E-mel dan Internet MAMPU;
21. Surat Akujanji;
22. Myportfolio;
23. Pelan Kesinambungan Perkhidmatan;
24. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk "Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan";
25. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
26. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";
27. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001 :2013 Dalam Sektor Awam;

28. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
29. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT MAMPU;
30. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
31. Garis Panduan GPKI; dan
32. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 "Langkah-langkah mengenai penggunaan Mel Elektronik Agensi - Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC).







KERAJAAN NEGERI PERLIS